2021

Strategies for Integrating the Internet of Things in Educational Institutions

Anthony Kofi Harvey
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Anthony Harvey

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Jodine Burchell, Committee Chairperson, Information Technology Faculty
Dr. Gail Miles, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2021

Abstract

Strategies for Integrating the Internet of Things in Educational Institutions

by

Anthony K. Harvey

MS, Walden University, 2018

MBA, ITT Technical Institute, 2011

BS, ITT Technical Institute, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

January 2021

Abstract

The introduction of the Internet of Things (IoT) into educational institutions has necessitated the integration of IoT devices in the information technology (IT) infrastructural environment of educational institutions. Many IT leaders at educational institutions, however, lack strategies for integrating and deploying IoT devices in their institutions, which has resulted in numerous security breaches. The purpose of this study was to explore security strategies adopted by IT administrators to prevent data breaches resulting from the integration of IoT devices in their educational institutions. The diffusion of innovations theory served as the conceptual framework for this qualitative multiple case study. Eleven IT leaders in 11 public K–12 educational institutions, who had successfully integrated IoT in their educational institutions in the United States Midwest region, were interviewed. Thematic analysis was the data analysis strategy. The 3 major themes that emerged were (a) organizational breach prevention, (b) infrastructure management—external to IT, and (c) policy management—internal to IT. A key recommendation is for IT leaders to develop strategies to harness the efficiencies and stabilities that exist during the integration of IoT devices in their educational institutions. The implications for social change include the potential for securely transforming the delivery of education to students and ensuring the safety of academic personnel by identifying strategies that IT leaders can use to securely integrate IoT devices in educational settings.

Strategies for Integrating the Internet of Things in Educational Institutions

by

Anthony K. Harvey

Doctoral Study Submitted in Partial Fulfillment
of the Requirements for the Degree of
Doctor of Information Technology

Walden University

January 2021

Doctoral Study Submitted in Partial Fulfillment
of the Requirements for the Degree of
Doctor of Information Technology

Dedication

I dedicate this dissertation to my family, friends, and mentors who continued to motivate and support me to keep persevering during hard times. You were on my side through thick and thin and encouraged me to move forward with this project, and for that, I am most grateful. My inspiration was drawn from the adversities I faced during my life journey.

"All our dreams can come true if we have the courage to pursue them."

--WALT DISNEY

Acknowledgment

I will like to acknowledge my committee members formally. I will like to thank my committee chair, Dr. Jodine Burchell, for her patience, scholarly advice, and the attention to detail she provided during the writing of my dissertation. I will like to express similar gratitude to my second commit member, Dr. Gail Miles, for reading and critiquing my paper. I would also like to thank Dr. Steven Case for reviewing my paper and providing feedback during my residencies.

In addition to my formal committee members, I had several cheerleaders and supporters who encouraged me during my doctoral journey. I would like to thank all who advised and encouraged me during this study, and I will like them to know that their support helped me plow through this doctoral study.

I will be remiss if I do not acknowledge that all this would not come to fruition without God's divine grace and my family and friends' support and love.

Table of Contents

List of Tables

Section 1: Foundation of the Study

IT leaders' ability in educational institutions to exploit Internet-connected devices in teaching and learning has accelerated the integration of the Internet of Things (IoT) devices in the educational ecosystem. The IoT refers to a new technology paradigm that remotely connects heterogeneous devices to the internet using sensors and actuators (Meneghello, Calore, Zucchetto, Polese, & Zanella, 2019). The secure integration of these devices in IoT infrastructure can provide educational institutions with data security, business agility, competitive edge, innovation, and increased enrollment. According to Kumar, Rao, Sahoo, and Mahapatra (2017), the IoT's security, reliability, and privacy data have been crucial to the technology's success. Owing to the rush to integrate the IoT phenomenon into their educational ecosystem, some information technology (IT) leaders have chosen to ignore the reliability, security, and privacy issues that arise during innovative technology integration. The lack of strategies for integrating IoT devices into educational institutions' network infrastructure has increased the potential scope of vulnerability, which has led to security attacks, access control breaches, and privacy issues in school districts (Nguyen & Yoo, 2017). At the same time, these risks have occurred that the proliferation of the IoT has led to an era of ubiquitous computing (Mavropoulos, Mouratidis, Fish, Panaousis, & Kalloniatis, 2017).

The purpose of this case study was to explore the security strategies that IT leaders have used to secure the integration of IoT devices in educational institutions. Some IT leaders of educational institutions are integrating IoT devices into their infrastructure ecosystem to facilitate teaching and learning but are they cognizant of the vulnerabilities that exist in the innovative technology they are integrating? The threat of cybersecurity, sophisticated phishing attacks, and distributed denial of service attacks have made IoT devices vulnerable to attacks. In this section of the research study, I present the background, purpose statement, nature of the study, research question, definitions, conceptual framework, and significance of the study.

Background of the Problem

The IoT is a vast network of interconnected devices that helps IT leaders meet developmental goals. The IoT has permeated users' daily lives by collecting and sharing critical data to help IT leaders make rapid decisions (Ren, Pan, Goscinski, & Beyah, 2018). The recent acceleration and automation of industrial processes have led to the proliferation of IoT device integration in educational institutions' ecosystems. The introduction of Internet-connected smart devices in educational institutions has forced IT leaders to maintain secured innovation deployment practices that have ensured the reliability, security, and privacy of IoT devices and data (Cornel, 2015). At the same time, the integration of IoT in educational institutions has led to an increase in security, reliability, and privacy issues among smart devices (Alam & Benaida, 2018). Dyn, an Internet infrastructure company specializing in controlling domain names, was attacked with a distributed denial of service (DDoS) through their IoT devices on October 21, 2016, which disrupted Internet service in the United States and Europe (Riga, 2017). The security, privacy, and reliability issues in IoT device integration have not deterred IT leaders of educational institutions from playing a pioneering role in integrating IoT devices due to the financial and economic benefit derived from the deployment of the IoT technology.

Problem Statement

The number of security breaches in some educational institutions has increased due to the introduction of IoT devices in the networking environment (Aldowah, Ul Rehman, Ghazal, & Naufal Umar, 2017). Lee and Lee (2015) estimated the number of connected devices would reach 26 billion by 2020, and researchers have estimated that 70% of educational institutions deploying new IoT devices may be exposed to vulnerabilities, potentially resulting in security breaches. The general IT problem is that some educational institutions have experienced an increase in security breaches due to the integration of IoT devices. The specific IT problem is that some IT leaders lack security strategies to address potential new security problems resulting from the integration of IoT devices in their educational institutions.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the security strategies that IT leaders had used to secure the integration of IoT devices in educational institutions. The targeted population was IT leaders of 11 educational institutions in the Midwest region of the United States who had developed strategies to integrate IoT devices securely. The study was limited in its geographical setting to five cities in Indiana: Carmel, Fishers, Indianapolis, Muncie, and Wabash. The findings from this study may contribute to positive social change by providing strategies that IT leaders at educational institutions can use to securely transform education delivery to students and safeguard educational personnel's data.

Nature of the Study

The method chosen for this study was qualitative research. Qualitative researchers explore an interpretative phenomenon in its natural setting to gain in-depth knowledge (Khan, 2014). A qualitative method was suitable because an in-depth exploration of the phenomenon took place in its natural setting. A quantitative design is ideal for studies in which there is a need to test hypotheses, examine variables for a causal relationship, and analyze statistical data (Rutberg & Bouikidis, 2018). The quantitative method was not suitable because I did not examine the relationship between variables; consequently, there was no need for inferential statistical analysis. Researchers conducting a mixed-method study employ quantitative and qualitative approaches to provide a more comprehensive understanding of the research study (Palinkas, 2014). The mixed-methods approach was not suitable for this research because the quantitative component of statistical analysis would not have added value to the research. Qualitative research methods were most appropriate for this study due to the potential for in-depth exploration of IT leaders' strategies. By conducting interviews with participants, I was able to identify organizational, security, and technical deficiencies that I would not have realized had I used a quantitative questionnaire or survey. See Appendices A and B for the interview protocol and questions, respectively.

The most appropriate design for this study was a multiple case study. Case studies represent an in-depth investigation and analysis of a collective case, with the intent to understand the philosophy behind the problem within a specific location and time (Cronin, 2014). A case study was the most suitable design because I performed an in-depth investigation and analysis of the problem specific to educational institutions in the Midwest region of the United States. Researchers employ phenomenological designs to explore a population's lived experiences (Eatough & Shaw, 2017). Although a phenomenological study could have been a viable alternative, examining a population's lived experiences was not the aim of this research study. Researchers conduct ethnographic studies to evaluate cultural characteristics by mingling with the population better to understand their behavior (Dunne, 2016). I did not intend to explore a group of people's cultural phenomenon to answer the research question, so ethnography was not a suitable option. Researchers can use a narrative study design to collect stories and analyze artifacts about an individual’s life and experiences (Levitt, Motulsky, Wertz, Morrow, & Ponterotto, 2017). Although an analysis of individual experiences could have contributed to this study, collecting stories and analyzing artifacts was not the focus of this study since I planned to perform an in-depth investigation of various people. Thus, a narrative study was not appropriate. After considering all potential designs, I determined that the case study design, which involved an in-depth investigation and analysis of participants in understanding the philosophy behind a specific problem, was the most suitable because it would comprehensively answer the research question.

Research Question

What security strategies do IT leaders use to prevent data breaches resulting from the integration of IoT devices in their educational institutions?

Interview Questions

1. What is the state of IoT integration in your educational institution?
2. What deployed connected devices in your institution do you classify as belonging to the IoT family?
3. What security strategies did you adopt during the integration of IoT devices?
4. How did your IT staff determine the use of security and reliability strategies during the integration of IoT devices?
5. What strategies did you deploy to control compatibility issues that arose during the deployment of IoT devices?
6. What methods did you use to confirm the viability of your IoT deployment?
7. How did you ensure that stakeholders bought into the security strategies used to integrate IoT devices?
8. How do you remain current regarding the security strategies required to integrate the IoT into your educational institution?
9. How do you ensure the continued security of IoT devices in your educational institution?

Conceptual Framework

I grounded this qualitative study in the diffusion of innovation (DOI) theory, which was first explained by Gabriel Tarde as a conceptual framework in 1902 (Dearing, 2008). Everett Rogers refined the DOI theory in 1962 (Değerli, Aytekin, & Değerli, 2015; Rogers, 1962). Researchers have used the DOI theory to explain innovative technology's adoption in various industries (Sundstrom, 2016). Succinctly, the DOI theory clarifies the reasons why and how new ideas and technologies spread through cultures (Kapoor, Dwivedi, & Williams, 2014). Rogers (2015) theorized the promotion and communication of innovation among members of a social system using appropriate channels within a specific period. The DOI theory comprises four independent but linked components: innovation, communication channels, time, and social system (Rogers, 2015). The integration of technology can be complete when all parts of the concept work in unison (DeGarmo, 2012).

I used the DOI theory to explore IT leaders' strategies to integrate IoT devices in educational institutions securely. The DOI theory requires the existence of innovative ideas or practices, clear communication channels that enhance the proposed innovation, the element of enough time, and a social system that includes the presence of formal and informal hierarchical positions and individual relationships (Rogers, 2015). The DOI theory aligns with the educational environment, including innovations, communication, time, and social system structures. I used the DOI theory to examine social structures and determine communication practices and levels, innovative ideas, and time constraints during the integration of IoT devices. By using the DOI theory, I was able to develop a better understanding of IT leaders’ strategies for securely integrating IoT devices in their educational environments.

The use of IoT in education has been critical to students who have needed the technology to thrive and be successful in school. Furthermore, the DOI theory has played a pivotal role in integrating new technologies across multiple departments and campuses in some public schools in the Midwest region of the United States (Sáenz-Royo, Gracia-

Lázaro, & Moreno, 2015). Students have benefitted from the innovative technology used by teachers to impart knowledge. Students can use the deployed IoT devices to access learning materials at all hours, and they benefit from the availability of data that hitherto were not available without the innovative technologies (Farhan et al., 2018). By using IoT devices, teachers and other school administrators have provided lesson plans and assignments and respond to discussions at all times. The DOI made possible by IoT technology may help IT leaders improve students' grades and enhance effective teaching and learning by teachers and students, respectively.

Definition of Terms

Information technology (IT) administrators are individuals who manage an IT department, such as the chief information officer (CIO), chief technology officer (CTO), IT director, or director of infrastructure (Madakam, Ramaswamy, & Tripathi, 2015).

Innovative technology refers to a strategic asset with the capacity to effect improvement in the tangible and intangible resources of the organization (Son, Kim, Park, & Kim, 2018).

Internet of Things (IoT) is the interconnection of global infrastructure to enable communication between heterogeneous devices (Wortmann & Flüchter, 2015).

Radio frequency identification (RFID) is a key component in the IoT technology that recognizes devices and humans with radio frequencies (Inoue & Nohara, 2009).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions refer to theoretically unproven belief systems that researchers take for granted during a research study (Schoenung & Dikova, 2016). I conducted the interviews for this study in participants' natural setting; doing so is vital to ensuring that participants are comfortable during the interview process (Moerman, 2017). I assumed that the participants would answer the questions accurately, honestly, and to the best of their abilities. I also assumed that the participants would understand the meaning and interpret the questions accurately. The final assumption was that I would conduct a thorough literature review before performing the analysis.

Limitations

Ellis and Levy (2009) described research limitations as uncontrollable threats to a research study's internal validity. The convenience sampling of participants from 11 educational institutions in the U.S. Midwest is likely a limitation that will impede the findings' generalization. This case study's other limitation was the small sample size; only 11 IT leaders from 11 school districts in the Midwest responded to the interview questions. Limiting the interview to the education sector precluded consideration of the broad spectrum of other industries, and this limitation might have harmed the case study. Last, the interview participants were drawn from IT leadership, and as a result, the case study does not reflect the perceptions of non-IT leaders.

Delimitations

Delimitations are boundaries imposed by researchers to ensure that the research scope stays intact (Dunne, 2016). The study participants were school districts’ IT leaders with knowledge and experience in the secured IoT integration. The data collection method used was interviews with IT leaders of school districts and participants’ review of documents. The interview questions were semi-structured and open-ended and designed to enable the population to provide their perception and experiences on the security strategies deployed when integrating IoT devices in the school district. I selected the participants based on the population sample and ensured that they met the eligibility criteria. All participants were interviewed for this study.

Significance of the Study

Contribution to Information Technology Practice

Insecurely configuring and integrating IoT devices in education has the potential to lead to the disruption of services. The interruption of services leading to systems stoppage in educational institutions can be inconvenient and counterproductive (Hsu & Lin, 2018). Furthermore, in the event of an ill-designed integration of IoT devices in education, user data could be susceptible to attack and unauthorized access. The results of this study shed light on some of the strategies required to successfully integrate IoT devices in educational institutions in a secured manner. IT leaders can potentially use these integration strategies in their educational institutions to secure IoT devices. Ideally, IoT devices can provide improved productivity by enhancing teaching and learning in educational institutions. The study can contribute significantly to a positive social change by promoting continuous teaching and learning; grooming an academic community; and providing improved social amenities to employees, students, and the community. Having an educated community can lead to economic stability and peaceful coexistence.

Implications for Social Change

The implication for social change is the contribution that IT leaders in an organization may make to increasing the awareness of the security vulnerabilities in IoT devices used domestically and industrially. Understanding IoT security can lead to the development of tools needed to detect, monitor, and prevent security issues related to IoT device deployment. This study may contribute to positive social change by securely transforming education delivery to students and improving the safety of educational personnel’s data by identifying strategies aimed at securely integrating IoT devices in educational settings. The knowledge gleaned from IoT deployment in some school districts can make faculty more productive and efficient while improving students’ lives and society due to their ability to access data and information in real-time. The IoT may enable researchers to acquire the information and knowledge necessary to develop a data bank of awareness while helping society understand diseases, crime, and ways to improve health that could enhance families’ lives.

A Review of the Professional and Academic Literature

IT leaders have been late to integrate innovative technologies, including the IoT, into their educational ecosystem due to concerns about security breaches. The number of security breaches in educational institutions has increased due to the introduction of IoT devices in their networking environment (Aldowah et al., 2017). According to Khan and Salah (2018), Cisco Inc. predicted that there would be about 50 billion connected devices by 2020, and most o IT leaders integrating new IoT devices may be exposed to vulnerabilities that could potentially result in security breaches.

This literature review represents a synthesis and analysis of professional literature and other data sources to establish the potentially new security problems experienced by IT leaders resulting from IoT devices' integration in their educational ecosystem. The IoT has permeated every facet of human life, and concepts such as smart cities, smart schools, and smart homes rely on the IoT technology to thrive (Pinka, Kampars, & Minkevičs, 2017). Some IT leaders have embraced the integration of IoT devices to disseminate learning materials and access to the network infrastructure in schools. The use of actuators and wireless sensors in IoT, for instance, has enabled IT leaders to collect and share data using students' everyday devices connected to the Internet. The interconnection of these heterogeneous IoT devices can increase data sharing and accelerate the acquisition of knowledge. Yet, the integration of IoT devices in educational institutions has introduced vulnerabilities, and many IT administrators lack strategies to address the subsequently introduced security, reliability, and privacy issues. The prevalence of security risks resulting from the increased use of everyday devices has affected educational institutions and users, and the security challenges are immense and varied.

In this qualitative case study, I explored potentially new security problems experienced by IT leaders resulting from the successful integration of IoT devices in their educational institutions. The overarching research question was as follows: What security strategies do IT leaders use to prevent data breaches from integrating IoT devices in their educational institutions? I reviewed numerous IoT integration security-related issues in educational institutions and examined strategies that researchers had considered to address security, privacy, and reliability integration problems. I used the five characteristics of the DOI theory (Rogers, 1962) as a framework for my investigation.

Specifically, I used Rogers's (1962) DOI theory to describe the level at which security, reliability, and privacy concerns have influenced the integration of technology in educational institutions. In the literature review, I discuss the purpose of the study and analyze other innovative technologies such as the technology acceptance model (TAM); disruptive innovation; the theory of reasoned actions (TRA); the theory of technology, organization, and environment (TOE); the unified theory of acceptance and use of technology (UTAUT); and the theory of planned behavior (TPB). The articles and journals I used were current and concerned IT leaders' lack of strategies to address potential new security problems resulting from the integration of IoT devices in their educational institutions.

The literature I reviewed included 417 references from articles and journals. I derived the literature materials from sources such as Computers and Applied Sciences Complete; ProQuest Dissertations and Theses Global; Dissertations and Theses @ Walden University; Academic Search Complete; AARP State Data Center; ABI/INFORM Collection; IBISWorld; IBM Technical Paper Search; IEEE Xplore Digital Library; International Security and Counter-Terrorism Reference Center; Thoreau

Multi-Database Search; Computing Database; Directory of Open Access Journals; ERIC; and Library, Information Science and Technology Abstracts. I used the following keywords to conduct the searches: *diffusion of innovations, IoT integration*, *reliability of IoT, security of IoT, privacy of IoT, innovative technology, sensors, RFID, characteristics of DOI*, *vulnerabilities in IoT*, *technology acceptance model*, *unified theory of acceptance and use of technology*, and *technology-organization-environmental framework*. I confirmed the veracity of the articles using Ulrichweb's database of peer-reviewed articles. Most (98%) of the 417 articles I read were peer-reviewed, and 90% were published within five years of my anticipated graduation in 2020.

Application to the Applied IT Problem

The purpose of this qualitative multiple case study was to explore the strategies that IT leaders had used to secure the integration of IoT devices in educational institutions. IT administrators have integrated the IoT in their ecosystems due to the benefits derived from its implementation. Singh, Millard, Reed, Cobbe, and Crowcroft (2018) noted that the IoT's integration had enabled some educational leaders to harness the efficiencies and stability in the devices and their accompanying infrastructure. Students and faculty have been able to collaborate, and teaching and learning have been enhanced because of the use of IoT technology. The IoT has supported the sharing of high-volume data and knowledge between users of the infrastructure to facilitate the profitability, growth, and success of most educational institutions (Aldowah et al., 2017). The early integrators of the IoT accrued many advantages, and those benefits propelled educational leaders to develop strategies that made their institutions lucrative and successful (Kiryakova, Yordanova, & Angelova, 2017). The use of sensors and radio frequency identification (RFID) in the IoT has enabled IT leaders to collect and share data via users' everyday devices connected to the Internet (Cornel, 2015). IT leaders have used the IoT in U.S. public educational institutions to measure, monitor, and determine students' knowledge levels (Cornel, 2015).

Beyond educational institutions, corporate leaders of industries, including health and agriculture, have used IoT-based sensors to enhance patients' lives and livestock profitability, respectively. The increased benefits of the IoT can be observed in the use of IoT in educational and residential environments, which has led to the development of smart factories and smart cities (Choi, Yang, & Kwak, 2018). The use of remote functions embedded in IoT devices has made it possible for educational stakeholders to measure students' activities and performance and access to materials that would otherwise be out of their reach (Verma & Sood, 2018). Stakeholders in education have realized improved teaching, learning, and administration due to the interconnectivity with users provided by IoT devices (Kiryakova et al., 2017). The desire to acquire knowledge and the need for lifelong learning at all levels have necessitated the development and enhancement of IoT device integration in education and have contributed to e-learning and distance learning (Pinka et al., 2017). The interconnection of devices has improved the speed of sharing data and, as a result, saved time that could be used for higher-end pursuits. The sensors present in IoT devices have been used to measure students' cognitive abilities, have helped teachers better explain the content of courses, and have increased students' concentration and management of learning stress in education (Iftene

& Trandabăț, 2018). Educators have used IoT technology to develop an intuitive understanding of student behavior and manage the dynamic educational environment. The evolution of the IoT has affected smart campuses, physical devices, and virtual learning environments (Elsaadany & Soliman, 2017).

The many sensors, including RFID and wireless radio sensors, embedded in IoT devices that communicate with institutions' network infrastructure demonstrate IoT devices' potential in education (Tan, Wu, Li, & Xu, 2018). These RFID and wireless radio sensor technologies are embedded in IoT devices and used in educational institutions to foster faster connectivity and remote data access. Educational institutions whose infrastructure does not support IoT devices have experienced challenges ranging from ethical constraints, including privacy and confidentiality, to technical limitations, including data source and transmission (Kassab, Defranco, & Voas, 2018). Experts contend that the use of IoT devices in educational institutions needs to increase to match smart devices' adoption by considering these devices with data on-demand as standard or routine devices (Elsaadany et al., 2017).

The introduction of IoT in educational institutions has increased the dissemination of instructional materials exponentially. The use of the Internet has evolved over time, and the IoT has become a new technological phenomenon that relies on the availability, security, stability, and adaptivity of interconnected wireless devices via the use of the Transmission Control Protocol and the Internet Protocol (IP; Riahi Sfar, Natalizio, Challal, & Chtourou, 2018). The IoT has enabled smart devices' interweaving with actuators and sensors (Ahmed, Yaqoob, Gani, Imran, & Guizani, 2016). The explosion of the IoT was fueled by the introduction of RFID and wireless sensor network (WSN) technologies (Chen, Wu, Huang, Wu, & Xiong, 2018). The technologies used in the IoT include sensors, RFID tags, actuators, and WSNs, and these technologies work in a host of heterogeneous smart devices (Lee & Lee, 2015). These technologies try to connect anything with anyone, anytime, and anywhere (Riahi Sfar et al., 2018). The IoT engages things or objects to enable interaction between devices and users. The inner workings of the IoT ensure that objects or devices are connected to a more extensive computer network, and data are shared through servers at the back end (Kamin, 2017). Smart devices are interconnected using IP addresses on a subnet.

The IoT is a heterogeneous set of technologies that can interface with multiple networks and frameworks. Technology innovators built the IoT’s foundation on the interworking of multiple network infrastructures connected to day-to-day personal and industrial devices (Thibaud, Chi, Zhou, & Piramuthu, 2018). The devices that make up the IoT include objects that can connect to the Internet and are used in users’ day-to-day lives. According to Ahmed et al. (2016), IoT devices may include smart devices, heating, ventilation, air-conditioning (HVAC) systems, and science probes. The rapid progression of communication technologies, coupled with the Internet’s growth, has accelerated the IoT's acceptability and use. At its core, the IoT combines physical and digital characteristics to provide seamless services used by educational institutions (Wortmann & Flüchter, 2015). Researchers have described the use of ubiquitous communication, ambient intelligence, and pervasive computing as characteristics of IoT (Thibaud, Chi, Zhou, & Piramuthu, 2018). The platform upon which IoT devices operate comprises sensor hardware platforms, sensor operating systems, software operating systems and development, and data integration systems (Mourtzis, Vlachou, & Milas, 2016). Educational institutions IT leaders who seek to integrate IoT may benefit from the flexibility that the technology's framework provides.

Yet, the rush by vendors to build IoT technology has led to an assortment of platforms that have made the management of IoT cumbersome in educational settings. Simultaneously, introducing various proprietary versions of advanced protocol stacks used for intercommunication has exacerbated IoT's security, reliability, and privacy vulnerabilities (Mishra, Verma, Srivastava, & Gupta, 2018). The lack of a standardized protocol has confused school district leaders trying to determine whether it is worth integrating the technology (Sicari, Rizzardi, Grieco, & Porisini, 2015). IoT devices' heterogeneous nature is the principal reason for the many communication problems between IoT devices and infrastructure (Li, Xu, & Zhao, 2015). Galembeck and Galembeck (2017) referred to the use of devices by science students in the interaction of models, access to learning data, and the possibility of simulating complex systems as some of the protocol complexities that have plagued IoT devices. The assumption was that there had to be a standard platform for these devices to communicate among themselves. Simultaneously, there must be an acceptable set of protocols implemented by standardization bodies if the IoT is widely accepted by organizations (Hsu & Lin, 2018). The acceptance and integration of the IoT may be beyond the reach of institutions if IT administrators do not implement strategies that will use standards that have been set up to ensure effective interplatform communications. The heterogeneous nature of the

IoT devices enrolled in educational institutions' ecosystem requires that IT administrators develop and implement practical and pragmatic security integration strategies to ensure the reliability, security, and privacy of IoT devices and data.

Conceptual Foundation

The conceptual foundation for this study was the DOI theory. The DOI theory comprises compatibility, relative advantage, trialability, observability, and complexity (Rogers, 2015). The literature review focuses on the characteristics of DOI theory, the IoT's security and privacy, and the reliability of IoT strategies. The characteristics of DOI can relate to the security and reliability issues affecting the strategies needed for integrating IoT devices. The review of reliability, security, and privacy-related issues during the integration of IoT involves modern problems, consequences, and ways to curtail the challenges. In reviewing IoT devices' security, reliability, and stability, I considered contemporary problems, related technologies, inherent vulnerabilities, and mechanisms that mitigate the adverse effects.

Diffusion of innovation. Rogers (1962) defined the DOI as the process through which innovative technologies are communicated over a specific time span to a community made up of social networks. The DOI theory emphasizes how social networks, communication channels, and time influence innovation (Kendall, 2014). The innovative technology being communicated could be a new idea, technology, process flow, or application that the IT leader is integrating. The DOI refers to an idea, product, or practice deemed new and worthy of integration by an institution or individual (Keller, Aguilar, & Hanss, 2018). Five distinct characteristics from Rogers’s (1995) DOI theory have contributed to technological growth. The DOI characteristics and their definitions, according to Rogers (1962), are (a) relative advantage (knowledge that the proposed innovation trumped the current one), (b) complexity (the innovation's usability), (c) compatibility (how the new technological innovation fits into the current system and ways of achieving the same goal), (d) trialability (the ability to test-run the technology in phases until found acceptable and ready for deployment into the mainstream of the organization), and (e) observability (the extent to which results can be realized).

The five characteristics of the DOI theory played critical roles in this study as I used them to explore the lack of security strategies to prevent data breaches resulting from the integration of IoT devices in educational institutions. I used the DOI theory's five characteristics to remind the integrators of privacy concerns, security implications, and reliability issues that can derail an innovation's integration. During this study, the knowledge gathered may assist IT administrators considering the integration of IoT in educational institutions. This study's finding may provide IT administrators of educational institutions with the foundation needed to comprehend IoT integration by using the examples and scenarios from previous research.

Diffusion of innovation characteristics: compatibility. As defined in the DOI theory, comprehensibility is the level at which an innovation matches the perceived current values, previous experience, and integrators' needs (Rogers, 1995). The current value in the definition represents the strategies, techniques, behaviors, objectives, and goals deployed by the educational leaders to integrate innovative technology in their environment (Cheng, 2015). An organization's current state may include its techniques, which the integration of innovation could enhance. An organization's past experiences may be the body of knowledge accrued over the years due to innovation (Rogers, 1962). A positive or negative response to innovation depends on users' prior success or failure in educational institutions within which the IT administrators intend to integrate IoT. A user's perception of innovation is an essential factor in successfully integrating the IoT in educational institutions (Cheng, 2015). IT leaders tend to have a positive attitude toward integration if prior innovations are successful, while conversely, they are numb to innovation if their previous attempts failed. As previously described in the definition of DOI characteristic of compatibility, needs must align with an institution's requirements to integrate the innovative technology, and IT administrators need to consider the adaptability, motivation, and encouragement of users to embrace IoT device integration in education during the integration process (Cheng, 2015).

The integration of IoT devices requires the perceived innovative technology to be compatible with the existing values. Therefore, compatibility is an essential component of the successful integration of IoT as it permeates the integration process's security, privacy, and reliability strategies (Rahimi, Timpka, Vimarlund, Uppugunduri, & Svensson, 2009). There is limited knowledge of the conflict between integrators' characteristics and innovations' characteristics (Ax & Greve, 2017). Late and early IoT technology integrators may be willing to adopt an innovation after weighing the possible economic and social benefits and losses. According to Jwaifell and Gasaymeh (2013), compatibility is the degree to which IT leaders perceive an innovation consistent with existing values, past experiences, and integrators' needs. The benefit of compatibility is the increase in behavioral change and intentions associated with technology integration and user experience (Nehme, Pérez, Ranjit, Amick, & Kohl, 2016). The successful integration of innovation requires the compatibility of existing technology with the perceived innovation.

The successful integration of IoT devices in network infrastructure within educational institutions requires compatibility between the systems and the applications that run on the systems. The IoT comprises numerous devices, and those devices have many technologies embedded in them that can fail during interaction (Rjab & Mellouli, 2018). For the IoT infrastructure to perform efficiently, the different devices must be compatible. In contrast, there must be compatibility between organizational culture and the values and beliefs embedded in the innovation under integration (Ax & Greve, 2017). During the integration of IoT technology, the devices and infrastructure should allow for backward compatibility and interoperability, as all the devices will have to interact in the same ecosystem (Rjab & Mellouli, 2018). IoT devices' heterogeneous nature requires an in-depth understanding of the security, privacy, and reliability ramification of introducing and integrating the innovation into existing architecture. The low-powered and memory-deficient RFIDs and sensors used in IoT integration require the right data transmission and communication protocols, such as the Institute of Electrical and Electronics Engineers Standard 802.15.4 (Rjab & Mellouli, 2018). Therefore, it is imperative to have consistent communication lines between existing structures and innovation during IoT integration. IT leaders see value in legacy systems, and therefore, innovative technologies are necessary to enhance the current system and provide rich user experiences instead of introducing bottlenecks.

Understanding DOI compatibility and security of the IoT. The DOI theory espouses compatibility as a needed part of the total innovation package. Researchers use the theory to apply past experiences to current values and determine reasonable considerations during the adoption and integration of innovations (Rogers, 1962). According to Rogers (2015), the integration of innovations occurred slowly in educational institutions, even though the advantages were apparent. The reluctance in educational institutions to speedily integrate the IoT directly impacted the experiences of users. As posited by Pinka et al. (2017), users have positive opinions about innovation when it is compatible with current organizational values. IoT security must not be sacrificed for innovation's compatibility during the IoT integration (Oliveira, Thomas, Baptista, & Campos, 2016). IT leaders must use innovation to accelerate the achievement of organizational goals, and the compatibility of the innovative technology is vital to the organization’s success.

The security of IoT devices is still an issue. A report released by Hewlett Packard revealed that 70% of IoT devices are likely to be attacked, thereby putting users at risk (Rauti et al., 2018). The vulnerabilities in the devices enrolled in the IoT architecture make them susceptible to security attacks, especially in the lower network layer that harbors the devices (Rjab & Mellouli, 2018). Educational IT leaders can use layering and limit the access of IoT devices to mitigate security vulnerabilities in the devices (Jwaifell & Gasaymeh, 2013). Securing IoT devices at the physical layer is a problematic measure to take, as it is typically challenging to police most devices, including cameras and other indoor IoT devices (Jang, Lee, Choi, & Son, 2019). The multiple layers, combined with the many sensors and actuators, make it complex to secure and support the devices as they require significantly different configurations. One of the users' concerns during integrating innovative technology was the new technology's compatibility with the current technology (Cheng, 2015). It was easier for users to use their innovation skills than to learn new skills owing to the introduction of an innovation. Users preferred to be part of the solution, and therefore, it was desirable to understand users' knowledge and skill when planning to integrate an innovation (Baldini, Botterman, Neisse, & Tallacchini, 2018). After all, users with relevant knowledge and skills will help deal with security and compatibility issues related to IoT integration.

Understanding DOI compatibility and privacy of the IoT. The DOI characteristics span several areas, and compatibility is one of the essential theories. IT leaders used compatibility to determine the level at which innovation was perceived to be consistent with past beliefs and preferences to influence current values (Rogers, 1962). Jwaifell and Gasaymeh (2013) conducted a qualitative study in which they examined the use of interactive whiteboards by female teachers in Jordan and concluded that compatibility, among other characteristics, influenced their preferences. The study concluded that users welcome innovations first, based on their perceptions, and then need the training to help integrate the innovation into the educational process. Users' privacy must be enshrined in an organization's IoT policies, and IT administrators must clearly define the procedures used to grant access to data (Garg, 2018). IoT privacy is a critical aspect of the integration process, and the compatibility of the IoT should not undermine the confidentiality of IoT systems and data. One way to ensure the privacy of the IoT ecosystem is to promulgate an effectual and resolute privacy policy (Aldowah et al., 2017). Efforts are necessary to protect IoT devices at each network infrastructure, software, and file storage layer. The IoT is a new phenomenon, and as such, there has not been extensive research into privacy-enhancing sensors (Bennati & Pournaras, 2018). IoT technology requires further research into the protection of users and corporate data. The privacy of corporate data is a fundamental requirement for the security of IoT integration and a prerequisite to building confidence in the organization's infrastructure (Sicari et al., 2015). The compatibility of innovation and existing infrastructure needs close attention when integrating the IoT in an educational institution.

Understanding DOI compatibility and reliability of the IoT. As discussed in DOI characteristics, comprehensibility can distinguish between integrators' experiences and the impact innovative technology has on existing values during the integration of IoT (Rogers, 1962). The extent of alignment between an innovation and the integrators' social norms and values affects compatibility (Ruth, Lamm, Rumble, & Ellis, 2018). Shiau, Huang, Yang, and Juang (2018) posited that compatibility has a positive relationship with an innovation's perceived usefulness (PU). An innovation being introduced must be highly available for the innovation's compatibility to be highly beneficial. The concept of IoT reliability is vital to educational institutions, and this research study involved exploring opportunities to ensure the continuous availability of IoT systems to users.

Developers of innovative technology must rely on common factors to ensure stability, reliability, security, and technology availability. One such common standard is the wireless 802.11 family of networks. The Institute of Electrical and Electronics Engineers' wireless standards ensure that IoT devices, sensors, wearables, and smartphones maintain a high level of availability and dependability (Rjab & Mellouli, 2018). Innovation can create setbacks for educational institutions if IoT devices cannot function in the IoT infrastructure due to service unavailability. The reliability of IoT devices during integration hinges on the compatibility of the innovation and users' positive perception (Li, Tryfonas, & Li, 2016). Thus, IoT reliability is critical to integrating IoT devices in an educational institution if they have to overcome compatibility issues.

Diffusion of innovation characteristics: relative advantage. The other characteristic of the DOI theory is relative advantage. Rogers (1962) described relative advantage as the degree to which an innovation is deemed better than the existing technology. The relative advantage of innovation can be measured using the benefit of economic profitability and the social prestige matrix (Rogers, 1995). The introduction of innovation must provide value to an institution while at the same time, propelling it ahead of its competitors (Prescott, 1995). Relative advantage provides institutions with cost-efficient and improved technological services. The process of reducing the risk associated with vulnerabilities enhances the adoption rate of innovation and increases the usage rate of the innovation since the IoT innovation is perceived to be better than the technology it is replacing (Shiau et al., 2018). One of the IT administrators' considerations when contemplating integration is to ensure that mistakes are minimized and that technology integration benefits are maximized. IT leaders must embark on technology innovations if they want to place themselves ahead of the competition.

Organizations embarking on IoT integration must review the DOI characteristic of relative advantage since it raises and answers comparativeness (Shiau et al., 2018). Relative advantage refers to replacing an idea or technology with a better one (Rahimi et al., 2009). The idea or phenomenon, therefore, needs to bring improvements and benefits to an educational institution. The integration of IoT in educational institutions should positively influence the existing technology (Davis, LeBeau, Brooks, & Brown, 2014). The use of heterogeneous devices to access data and lessons in educational institutions can be problematic, and the introduction of appropriate innovation to ensure secure and smooth access to the network infrastructure can be a prime example of an innovation having a relative advantage over the previous technology (Kasperavičiūtė-Černiauskienė & Serafinas, 2018). The integration of the IoT in educational institutions serves as an example of an innovation having a relative advantage over existing technology in a classroom or lab. A study conducted by Ashrafzadeh and Sayadian (2015) indicated that instructors perceived integrating technology in their instructions better than the previous ideas. The use of sensors and RFIDs in IoT devices helps with the integration process, as IT leaders collect and analyze a large amount of pertinent data such as the usage pattern that cannot be collected from using standard labs (Bahrami, Khan, & Singhal, 2016). Therefore, relative advantage is significant when an educational IT leader is considering the integration of IoT innovation.

Relative advantage is often mentioned as the essential characteristic in the DOI theory when compared to the other characteristics (Rogers, 1962). The relative advantage concept was used by staff members of the U.S. Agency for International Development to implement growth in babies in developing countries such as Ghana through exclusive breastfeeding, as an example of the usefulness of these DOI characteristics in fields apart from education (Moseley, 2004). The likelihood of integrating technology increases when faculty face new technology demands (Sahin, 2006). Ashrafzadeh and Sayadian (2015) indicated that when faculty determine that a particular technology has value in delivering instructional materials, they can integrate that technology into their classroom setup. An educational institution's goals must be to determine the perception of innovation, and that must drive the level of relative advantage to the educational institution (Rogers, 2015). There are security risks associated with the non-vetting of IoT innovation, as that could create loopholes or backdoors for an attack on the system; therefore, efforts must be made to ensure an innovation does not introduce any vulnerabilities (Li et al., 2016).

The heterogeneous nature of devices enrolled in IoT integration makes it difficult for IT administrators to enjoy the full benefits of relative advantage, as security, privacy, and reliability vulnerabilities inherent in the technological innovation. One of IT administrators' main concerns is the vulnerabilities associated with IoT due to the enrollment of everyday usage devices in the IoT ecosystem (Radisavljevic-Gajic, Park, & Chasaki, 2018). Failing to configure these numerous devices securely could open them up to unauthorized access. Solangi et al. (2018) concluded that privacy concerns in the

IoT environment and unauthorized users and competitors strive to access users' confidential and personal data. According to Assiri and Almagwashi (2018), privacy issues are detrimental to integrating the IoT in educational institutions, as users are skeptical about enrolling their devices in the IoT system. According to Granjal, Monteiro, and Sa Silva (2015), the IoT has reliability issues because low-energy wireless sensing applications and devices have varying demands on IoT infrastructure, as resource allocation to devices is not the same across the board. Relative advantage in IoT can help IT leaders strategize the integration of IoT to prevent IoT security and privacy concerns while at the same time providing a relative advantage over competitors.

Understanding DOI relative advantage and the security of IoT. As stipulated in the DOI characteristics, relative advantage is the concept of a novel technology upstaging the previous technology (Rogers, 1962). This DOI characteristic enables users to be creative as they have room to test the technology, which can be measured by an enhancement in productivity, social prestige, and efficiency (Kasperavičiūtė-Černiauskienė & Serafinas, 2018). IT leaders who prevent IoT design flaws from posing as security vulnerabilities gain a competitive advantage over their adversaries as they can identify and fix most of the security and privacy vulnerabilities (Neshenko, Bou-harb, Crichigno, Kaddoum, & Ghani, 2019). Dorri, Kanhere, Jurdak, and Gauravaram (2017) discovered that IoT security remains a significant challenge due to its large scale and diverse nature. Iles et al. (2017) concluded that a new technological infusion or integration offers effective communication regarding new security technology that motivates users and enhances safety. The process of integrating innovation has the potential to bring to light security vulnerabilities and can provide a relative advantage and social value to educational institutions (Vojtovič, Navickas, & Gruzauskas, 2016). Security vulnerabilities are detrimental to IoT innovations, and documenting security fixes and creating a privacy policy aids IoT integration in educational institutions (Liu & Liu, 2019; Villari et al., 2017). The security of the IoT infrastructure and devices enrolled in them is necessary to the success of innovation. To gain a relative advantage over competitors, educational institutions need to create reliability and security policies.

Understanding DOI r*elative advantage and privacy of IoT*. Educational IT leaders mostly adopt relative advantage as a DOI characteristic to improve their operations through innovation (Rogers, 1962). Ahanger and Aljumah (2019) revealed that privacy and security threats are some of the IoT challenges. There are privacy concerns during the integration of IoT innovations in educational institutions, and one must be mindful of that limitation and take steps to reduce or eliminate them while at the same time taking advantage of the inherent relative advantage. To take advantage of the relative advantage inherent in integrating the IoT in an educational institution, there must be an IoT privacy policy to curtail users' infringement (Ahanger & Aljumah, 2019). Byun (2011) conducted a study that indicated that the relative advantage of IoT innovation outweighs information privacy risk, and therefore, users tend to benefit from the high availability of data. Educational IT leaders must not overlook the harm caused by the invasion of users' privacy and, therefore, must assiduously protect their organization's information through privacy policies and data protection (Torre, Sanchez, Koceva, & Adorni, 2018).

Educational IT leaders should create an environment where users know that privacy vulnerabilities are being addressed through regulatory and educational means.

Understanding DOI r*elative advantage and reliability of IoT*. Relative advantage is a significant characteristic of DOI theory that can exploit the perceived economic value, idea, or practice of innovation to an educational institution (Rogers, 1962). According to Ntemana and Olatokun (2012), relative advantage significantly influences the devices and applications used to integrate innovation in educational institutions. The motivating factor is that this improved technology influences IoT reliability during the integration process. The integration of the IoT provides educational institutions with faster, cost-effective, and reliable access to the Internet and user data (Boit, 2017). The adoption and integration of the IoT in educational institutions will be a cost-savings to the institutions as the efficient harnessing of data can be extended to other business operations spheres (Menon, 2017). The use of cloud storage space also provides reliability and relative advantage owing to the high availability of data at all locations to educational institutions. Storing IoT systems data in the cloud provides IoT integrators with low cost, high resource utilization, and flexible extendibility (Xu, Yang, Mu, & Liu, 2019). The relationship between IoT devices and the server infrastructure has provided a level of reliability, and this has been an essential catalyst in the sustenance of the technology (Sadique, Rahmani, & Johannesson, 2019). The heterogeneous nature of the devices enrolled in educational institutions' IoT infrastructure makes it cheaper, faster, and reliable for users to access their data in a distributed application environment using secured authentication and encryption mechanisms (Sicari et al., 2015). IT leaders have expressed dissatisfaction with the reliability and the speed at which data are accessed using IoT devices, which requires unprecedented collaboration and coordination between all the systems (Rifi, Rachkidi, Agoulmine, & Taher, 2018). IT leaders planning the integration of IoT should consider the development of IoT reliability standards as a guiding principle during the integration of IoT (Nikoukar, Raza, Poole, Gunes, & Dezfouli, 2018). The purpose of relative advantage is to provide high levels of availability, reliability, privacy, and security of IoT devices.

Diffusion of innovation characteristics: trialability. Another characteristic of DOI theory is the element of trialability. According to Rogers (1962), trialability is the level to which the prototype innovation can be experimented with on a limited basis to ensure its viability for being fully integrated. Experimentation is an essential characteristic of DOI and software development (Dutta & Omolayole, 2016). The testing of new ideas and products in segments has higher success rates than holistically introduced innovations (Rogers, 1995). Developers in the software industry mostly use trials to determine the effectiveness of their applications. The introduction of innovation has similar characteristics to the software development process due to continuous tweaking until attaining the right level. Therefore, IoT innovation in educational institutions must offer the opportunity for experimentation (Iles et al., 2017). Testing involves examining firmware, operating systems, and services for design flaws in the innovative technology, as improving input validation and trialability is essential to the IoT ecosystem (Chen, Zhang, Lee, & Shieh, 2018). In the educational environment, the trialability of innovation involves testing and redesigning an application or idea based on stakeholders' feedback, which ultimately helps reduce the degree of uncertainty before integrating the innovation into the educational environment (Mamun, 2018). Trialability is critical to providing integrators with a quick look into innovation prior to its integration. Trialability provides a solution to potential issues, such as oversubscription of licenses, overburdening the infrastructure, and ensuring high availability of users' data (Strömberg, Rexfelt, Karlsson, & Sochor, 2016). Though trialability is a poor predictor of successful innovation integration, it is worth proceeding with the process (Banerjee, Wei, & Ma, 2012). According to Johnson, Kiser, Washington, and Torres (2018), trialability is the extent to which integrators perceive that they have the chance to experiment with innovation before deploying the technology into the production environment.

The lack of research on IoT technology makes trialability an essential element of integrating innovation. The integration of IoT into an education institution's environment alters education delivery to students (He, Lo, Xie, & Lartigue, 2016). Therefore, it behooves integrators to ensure the trial of technologies is successful before being introduced into the mainstream IoT environment. The trialability of innovation must include the compatibility and flexibility of the innovation being integrated since it can predict IoT devices (Pashaeypoor, Ashktorab, Rassouli, & Alavi-Majd, 2008). One constraint of integrating innovation in educational institutions is the oversight that rules and regulations provide. Rules and regulations hinder educational IT leaders from integrating innovation because they do not want to be saddled with regulatory standards that will bog down their innovation (Li & Palanisamy, 2019). Therefore, experimenting with innovative technology allows the educational IT leader to work through innovation kinks before integrating. Experimentation will provide integrators with the opportunity to decide whether the perceived benefit of integrating the innovation outweighs the vulnerabilities (Karahoca, Karahoca, & Aksöz, 2018). According to Stephenson, Phelps, and Colburn (2018), trialability helps reduce flaws and integration errors due to the slow integration of innovation. To depict trialability's success in introducing innovation, the IT leader must consider trialability as culturally useful and adding to the institution’s social values (Aldowah et al., 2017). One of the main elements of integrating innovation is to reduce risk, as trialability has become one of the essential tools in determining the efficacy of technological innovation (Safa et al., 2015). Trialability, therefore, has become a mechanism for IT administrators when integrating IoT innovation in educational institutions.

Educational IT leaders introduce IoT innovation into the educational environment due to the perceived benefits technology is expected to bring. To ensure the success of integrating innovation in an educational institution, the challenges of security, privacy, and reliability have to be tackled and fixed (Nouri-Mahdavi, 2016). Based on the challenges of security, privacy, and reliability, trialability provides IT administrators with the chance to experiment and correct the privacy, security, and reliability challenges in the innovation before its integration (Johnson et al., 2018). The opportunity to experiment with the innovation before its integration enables IT administrators to identify and eliminate the potential privacy, security, and reliability risks associated with the innovation. The value of innovation is most appreciated by educational IT leaders when trialability is enforced and used during IoT innovation.

Understanding DOI trialability and security of IoT. The DOI theory explains trialability as the ability to experiment with innovation for a limited period before integrating the innovation (Rogers, 1962). The trialability of innovation enables IT leaders to quell uncertainty associated with introducing the innovation (Tanye, 2017). It is common for innovation to be accepted by the user community if the technology has gone through an experimentation process and found to be acceptable. Experimenting with the innovation before it goes into production depends on the geographic location and the technology's inter-organizational cooperation strategies (Le Roy, Robert, & Lasch, 2016). The introduction of IoT in third-world countries may involve purchasing off-the-shelf technology compared to industrialized countries that may test and retest before outdooring the innovation (Tanye, 2017). According to Johnson et al. (2018), ubiquity and trialability are positively perceived by users when security concerns are considered. Banerjee and Sheth (2017) noted that a trialability process is an essential tool for introducing innovation to actual integration. Therefore, IT administrators should ensure that IoT security vulnerabilities are unearthed and overcome during the trialability of innovation integration.

Understanding DOI trialability and privacy of IoT. Trialability has been described as the number of times innovation is tested before integrating the technology (Rogers, 1962). The concept of trialability is vital at the decision-making phase, as commitments must be made before the integration (Strömberg et al., 2016). Johnson et al. (2018) concluded that privacy in IoT is attitudinal and, therefore, a malleable hindrance compared to infrastructure, a structural problem. When one can influence a user, the benefits permeate through other concerns, including security and increased productivity. The gradual introduction of innovation due to the experimentation of ideas or products enables the innovation to be fine-tuned to an acceptable level by users (Stephenson et al., 2018). User privacy is a consideration when encouraging the integration of innovation in educational institutions (Iles et al., 2017). Trialability, therefore, plays a pivotal role in ensuring users' privacy and devices are not undermined during the integration of IoT innovation integration.

Understanding DOI trialability and reliability of IoT. The concept of trialability as a characteristic of DOI theory describes the extent to which IT leaders can evaluate an innovation before its integration into the infrastructure of an educational institution (Rogers, 1962). One way to ensure the reliability of innovation is to pilot the technology before releasing it to the entire educational institution (Safari, Safari, & Hasanzadeh, 2015). Piloting an innovation will provide IT leaders with the assurance that innovative technology is reliable and, as a result, ready to use in the infrastructural environment of the educational institution. During the adoption of technology, trialability plays a significant role in reducing technology's uncertainty (Safari et al., 2015). Therefore, the reliability of innovation provides IT administrators with the conviction that the innovation has passed the various rigorous testing phases and is ready for the production environment. IT leaders prefer to integrate innovations that allow trialability in phases until the entire technology integration process is complete (Waheed, Kaur, Ain, & Sanni, 2015).

Conversely, users become comfortable when they are involved in a phased introduction and experimenting with innovative technology. The involvement of users in the integration of innovation provides a level of reliability as the users understand the technology and its inner workings and know how to handle the sensors and nuances that come with it (Billet & Erie, 2017). Additionally, Jwaifell and Gasaymeh (2013) indicated that IT administrators have a responsibility to ensure an innovation is well configured during the phased experimentation to provide stability, consistency, and accuracy, which are all tenets of reliability.

Diffusion of innovation characteristics: observability. Observability is another characteristic of DOI theory. Observability is the ability to determine innovation's performance and explain its intricacies to stakeholders (Rogers, 1962). According to Ax and Greve (2017), observability is the level at which the output of innovation is available to users. Users play a role in the successful implementation of innovation, as the decision to integrate innovation is a gateway to either integrate or abort the innovation (Kasperavičiūtė-Černiauskienė & Serafinas, 2018). Observability stimulates the discussion of an innovation and promotes a positive vibe about the innovation. It is in the institution’s interest for users to engage with the innovation and be conversant with its performance to advocate for its integration (Hart & Sutcliffe, 2019). The perceived benefit of an innovation by stakeholders will increase if they can experiment and observe the innovation’s output during its integration into an educational institution (Hayes, Eljiz, Dadich, Fitzgerald, & Sloan, 2015). Jwaifell and Gasaymeh (2013) concluded that it is easier for users to accept an innovation if they see the positive results of innovation. In an investigative study, Ntemana and Olatokun (2012) surveyed 213 lecturers, who concluded that observability had the most positive influence on innovation's viability, mainly if influential people process the innovation. Pashaeypoor, Ashktorab, Rassouli, and Alavi-Majd (2016) indicated that observability has high integrability and adoptability rates than the other DOI characteristics.

Observability is essential to the success of IoT integration, as it provides IT administrators the opportunity to determine the efficacy and benefits of the innovation. The opportunity to observe the integration process from initiation to the final delivery of the technology makes it easier for user assimilation and beneficial to the institution (Stephenson et al., 2018). Cheng (2017) observed in research that observability positively affects creativity, as stakeholders find themselves knee deep in integrating the innovation. According to Abdullah, Karim, Sanni, Ngah, and Waheed (2014), one of the best ways to confirm the success of integrating an innovation is for employees to demonstrate results. The input by users during the initiation, building, and testing of an IoT innovation is a potential area that could provide visibility, as they would be aware of the systems' configuration. IT leaders integrating the IoT in educational institutions could use the DOI characteristic of observability to provide visibility into the innovative technology.

Security, privacy, and reliability are areas of observability that can be useful to IT administrators during the integration of IoT innovation. The level to which the results of innovations are visible to the user ensures increased acceptability of a technology (Hayes et al., 2015). IT administrators of educational institutions can use observability to provide technological innovation processes, either through a clean bill of health or failure (Hsu & Lin, 2016). The creation of security and privacy requirements is fundamental to ensuring confidence in integrating the IoT, and ensuring strong authentication and access control mechanisms to protect the privacy, security, and reliability of the IoT infrastructure is necessary to safeguard measures (Sicari et al., 2015). The essence of integrating the IoT in an educational institution is to provide fast, reliable, and easy-to-use technology for teaching and learning, including the storage and retrieval of data and unimpeded access to learning materials (Sathiyanarayanan, Govindraj, & Jahagirdar, 2018). It may be challenging to attain all the three IoT integration elements of fast, reliable, and easy-to-use technology simultaneously, as the integration process reflects a cyber-physical-human-system (Nakamura, 2018). IT administrators of educational institutions need to develop policies that will promote observability to increase the acceptability of the innovative technology being integrated.

Understanding DOI observability and security of IoT. Observability is another characteristic of DOI theory. Observability is the ability to determine innovation's performance and explain the intricacies to stakeholders (Rogers, 1962). The unauthorized access to the physical IoT infrastructure and institutional data's cyber content can be deemed a security breach (Ammari, 2018). The process of observability has the potential to build barriers to ward off intruders who plan to access the IoT network infrastructure and its associated data. The flexibility required to build a resilient

IoT infrastructure can put the network and data security at risk due to the observability characteristic, which is one of the DOI theory components. Therefore, the process's transparency should not derail the objective of enhancing the final results of integrating IoT in educational institutions (Ilie-Zudor, Kemény, & Preuveneers, 2016). One observable security threat during the integration of IoT in educational institutions is the threat of obtaining unauthorized access to data due to either the misuse of elevated privilege or bypassing access-control mechanisms through spoofing the network (Ilie-Zudor et al., 2016). Observability during IoT integration requires continuously checking systems for faults and unauthorized access in applications engaged in the IoT ecosystem (Miranda, Vaskova, Portela-Garcia, Garcia-Valderas, & Lopez-Ongil, 2017).

Understanding DOI observability and privacy of IoT. Observability is a DOI characteristic that demonstrates technological innovations to stakeholders and reduces uncertainty (Rogers, 1995). The degree to which an innovation is observable strongly correlates with whether the technology will be integrated (Keller et al., 2018). IT leaders are unlikely to integrate innovations if ambiguities are surrounding the technology. The privacy and security of IoT systems are vital to their successful integration, and according to Safari et al. (2015), 50% of organizations integrating cloud computing, which is a component of the IoT, consider privacy and security as a top concern. The risk of RFIDs linked to users leaking data is a considerable privacy concern that IT leaders need to understand when integrating the IoT into their network environment (Inoue & Nohara, 2009). Wang, Yuen, Wong, and Teo (2018) concluded that users' privacy, such as protecting confidential data, is likely to be accessed during innovation integration because visibility promotes users’ involvement. The privacy of the application data that traverses the network due to the use of WSN-embedded devices might be as important as the privacy of the storage location of the devices and their associated data (Abuzneid, Sobh, Faezipour, Mahmood, & James, 2015). According to Alaeddini, Morgansen, and Mesbahi (2017), network observability exposes IoT network data to unauthorized and undeserving users; subsequently, promoting integration mechanisms to minimize the exposure will ensure the privacy of enterprise data.

Understanding DOI observability and reliability of IoT. Observability is the characteristic of DOI theory that refers to how innovation integration is visible to users (Rogers, 1962). Observability is the level to which the results of innovations are made visible to interested parties (Taib, De Coster, & Nyamu, 2017). Reliability in IoT can lead to the heterogeneous remote-controlled devices' stability and efficiency connected to their digital counterparts, which eases observability during the integration process (Li, Shahidehpour, & Liu, 2018). Observability promotes faster integration and provides reliable, robust, and secured innovative technology (Radisavljevic-Gajic et al., 2018). Mamun (2018) concluded that the degree of reliability in an innovation is dependent on the level of observability and strategic orientation. The level to which an innovation is noticeable to others confirms that observability is at work (Al-Rahmi et al., 2019). The development of an effective and fault-tolerant innovative technology is necessary to increase system availability and performance of an educational institution (Bregon, Alonso-González, & Pulido, 2014).

Diffusion of innovation characteristics: complexity. Complexity is the final DOI characteristic. According to Rogers (1962), complexity is the perceived difficulty of the innovation being integrated. The extent to which the innovation is difficult to understand makes it less likely to be integrated than a technology that is easier to comprehend (Ruth, Rumble, Lamm, & Ellis, 2018). Complexity can sway the user's mind if the innovation has a steep learning curve, and therefore reducing the complexity of innovation can increase the adoption of the technology being integrated (Dan, Osterheider, & Raupp, 2019). Gibson et al. (2018) identified scenarios where the characteristics of complexity can increase adaptability and integrability while at the same time enabling educational institutions to reap maximum benefits from the integration process. Understanding complexity intricacies will enable educational institutions to enjoy the benefits of simplicity, efficiency, and effective management of the IoT ecosystem (Makovhololo, 2018). Mapande, Zuva, and Appiah (2018) mentioned that, because complexity is the extent to which an innovation can be challenging to comprehend, it has the potential to lower the rate of integration into the working environment. In a study on cloud enterprise resource planning, while there are technical and economic benefits to integration, the technical complexity and legal issues posed critical challenges and barriers to the successful integration of the IoT (Choi, Nazareth, & Ngo-Ye, 2018).

The multiplicity of Internet-connected devices and sensors has exacerbated the IoT complexities (Drira, 2017). The previously mentioned complexities in the IoT confirm the position taken by Rogers (1962) that users of the IoT require a high level of knowledge and understanding during innovation integration. IoT systems have many embedded smart objects, and the presence of these various objects increases the complexities of the computing environment made up of humans, objects, applications, and sensors (Riahi Sfar et al., 2018). IoT problems are multiscaled, as sensors, RFIDs, actuators, and servers need to work together to ensure IoT innovation's smooth performance (Drira, 2017). The complexities in IoT innovations are enormous, and integrating the systems into an educational system requires a good grasp of the innovative technology’s various parts.

The DOI characteristic of complexity has an influential role in the security, reliability, and privacy of integrating the IoT into an educational organization’s IoT architecture. IT administrators need to overcome security, interoperability, and communications challenges before integrating the IoT into an educational institution’s networking environment (Lennvall, Gidlund, & Akerberg, 2017). There are no cookie-cutter methods to fix the challenges that IoT integration generates, but the inclusion of artificial intelligence into data collection and dissemination leads to efficient decision making using the enormous amount of data accrued by IoT devices (Javaid, Sher, Nasir, & Guizani, 2018). The interconnection of massive heterogeneous devices in the IoT makes it complicated to integrate communication protocols, routing problems, and resource allocation related to an innovation into an organization’s ecosystem (Javaid et al., 2018). Educational institutions have a role to play to ensure IoT systems incorporate the right packages that include sensors, connectivity mechanisms, and memory utilization while maintaining the IoT devices' reliability, privacy, and security (Martins et al., 2018).

Understanding DOI complexity and security of IoT. According to Rogers (1962), DOI's complexity characteristic refers to the degree of understanding and innovation by potential integrators. The definition of complexity in the context of DOI is that it is difficult for users to understand innovation and how easy it is to use, which affects the rate of adoption and integration (Al-Rahmi et al., 2019). Al-Rahmi et al. (2019) concluded that students' perceived level of complexity of e-learning systems might affect students' learning performance, as they would have low intention to use the system. Complexity is one of two DOI constructs that can be used to predict the acceptance and final integration of IoT systems (Mokwena & Hlebela, 2018). Mapande et al. (2018) concluded that innovation's complexity is challenging to comprehend, and adding security measures into the mix makes it difficult to integrate. The perceived uncertainty in the innovation directly affects whether users are willing to integrate technology, as they are not sure of the security implications of introducing the technology (Coursaris, Van Osch, & Sung, 2013). IT administrators have been concerned about the significant security risk associated with innovation, and that concern has an exponential effect on the rate of integrating technology into an educational institution's IoT environment (Coursaris et al., 2013). Coursaris et al. (2013) described how the level of difficulty of innovation dictates technology's integration into the production environment. AlBar and Hoque (2019) observed that one of the reasons IT leaders may defer the integration of innovation is the risk of data security and the lack of a skilled workforce.

Understanding DOI complexity and privacy of IoT. Complexity refers to the level to which advancement is difficult to understand and use (Mapande et al., 2018).

Innovation is complex when users have difficulty integrating and assimilating it (Corneille, Carter, Hall-Byers, Clark, & Younge, 2014). Safari et al. (2015) found that privacy was the concern of 50% of IT integrators deciding on integrating innovation into cloud computing, which IoT technology relied upon to provide efficiency in data storage. The use of devices in the health industry in South Africa came under scrutiny as technological challenges made its interoperability challenging to integrate and challenging to secure the privacy of the data in motion and at rest (Leon, Scheneider, & Daviaud, 2012). With the introduction of IoT and big data, the collection, storage, manipulation, and data storage have become a privacy concern, and hackers have exploited these vulnerabilities with malicious intent (Pathak, Vyas, & Joshi, 2017).

Understanding DOI complexity and reliability of IoT. Complexity refers to an innovation that is difficult to understand and, as a result, negatively affects its adoption and, by extension, integration (Rogers, 1962). According to Ganglmair-Wooliscroft and Wooliscroft (2016), the increased complexity of an innovation relating to technology's usability reduces the adoption rate. The level of understanding of the technology being integrated determines the users' involvement in determining the innovation's suitability for the organization's environment (Irani, Weerakkody, Dwivedi, Sivarajah, & Kapoor, 2016). Rogers (1995) posited that the less complicated a service is, the more likely it will be adopted and integrated. IoT devices' reliability in the educational infrastructure is part of a complex network of interconnected infrastructure that needs to be improved to enhance the growth of the technology (Kamyod, 2018). Galinina, Andreev, Komarov, and Maltseva (2017) mentioned that the IoT-based 5G ecosystem's rapid growth is posing reliability and performance problems for researchers, especially with the ultra-low latency of IoT devices and the availability and secure wireless connectivity to the ubiquitous IoT devices. The reliable performance of IoT devices must therefore be of concern to users of the technology.

There have been numerous studies on the effects of integrating the IoT in educational institutions using theories and known methods, including the DOI theory, TAM, disruptive innovation, productivity, strategic alignment of technology and user retraining, and coaching (Sundstrom, 2016). I reviewed literature related to the security implication of integrating the IoT into educational environments and the measures that could be put in place to ensure the successful integration of the IoT. I examined scholarly research on lessons derived from negligently integrating the IoT in educational institutions, and I reviewed current scholarly literature on methods that IT administrators used to integrate the IoT in educational institutions in the Midwestern United States.

Analysis of Supporting Security Theories

Researchers have propounded numerous theories to support the integration of IoT in educational institutions. IT leaders integrate the IoT for various reasons, but the primary motivating factor is the advancement of the effective sharing of knowledge (Zhang, Duong, Woods, & Marshall, 2017). The integration of the IoT by IT leaders is preempted by their desire to improve upon their current technology status. The requirements of innovation must be creative to meet the goal of improving upon the delivery of teaching, the consumption of knowledge by students, and the success of educational institutions (Horkoff, Maiden, & Asboth, 2019). The technological needs of educational institutions have been spurred on by advances made in automation, RFID, and sensor domains, which have influenced the software and infrastructure required to enhance the delivery of knowledge to students (Xu, Qu, & Yang, 2016). Some of the factors that can affect innovative technology deployment by IT leaders include external considerations, market conditions, availability of technology vendors, human resources, and progressive regulations (Hagen, 2014). In this study, I used the five characteristics of DOI theory to map the technological elements to the educational institution's objectives to address the lack of knowledge when integrating IoT security strategies (Scott & Mcguire, 2017). To prevent data breaches resulting from the integration of IoT devices in educational institutions, the knowledge gathered from this research will provide IT administrators with the tools needed to securely and successfully integrate the IoT.

Technology acceptance model (TAM). Researchers have used the TAM to explain the theoretical model's prolific use in information systems (Lee, Kozar, & Larsen, 2018). TAM was derived from the theory of reasoned action and used the PU and perceived ease of use (PEU) of technology to describe an individual’s acceptance of information systems (Arvie & Tanaamah, 2018). According to Davis (1989), PU and PEU of innovation are the determinants of user behavior, and this is the core theoretical foundation of TAM. The focus of this study was IoT integrating strategies imbuing DOI characteristics. DOI and TAM have similarities, as both include an interest in the rate of acceptance of an innovation by users (Alam, Omar, Mohd Ariffin, & Nik Hashim, 2018). The other similar variable between DOI and TAM is the concept of relative advantage and PU, as they both determine users’ positive attitude toward the usage of innovation

(Natarajan, Balasubramanian, & Kasilingam, 2017). The differences lie in DOI emphasizing the five characteristics to influence a user’s perception and TAM’s focus on the PU and PEU of the individual user on the one hand and the effect of DOI and TAM on the attitude of users on the other hand when coping with the complexity (ease of use) and trialability of the innovative technology (Shiau et al., 2018). After considering the differences and similarities of DOI and TAM, I selected DOI because I planned to use the five characteristics of DOI to understand the reliability, security, and privacy strategies used by IT administrators of educational institutions during the integration of IoT devices.

Theory of technology, organization, and environment (TOE). The TOE theory is the other framework that I considered. IT leaders adopting information systems innovation have used the TOE theory to investigate its efficacy (Wang, Li, Li, & Zhang, 2016). The TOE framework uses four constructs (PEU, PU, actual behavior, and attitude toward usage) to explain why users choose to accept the adoption of technological innovations (Deslonde & Becerra, 2019). DOI factors of acceptance of technology are affected by an individual’s perception of the innovation's characteristics (Rogers, 1995). Some similarities exist between TOE and DOI regarding identifying antecedents of adoption and diffusion, respectively. The TOE framework was developed to determine, among other things, the external factors affecting the adoption of innovation, and DOI uses technological characteristics to determine the rate of adoption, diffusion, and acceptability of innovation (Kim, Hebeler, Yoon, & Davis, 2018). The differences between TOE and DOI include emphasizing the theory's environmental aspect rather than on the five characteristics. The reason for developing the research question was to understand the security, reliability, and privacy strategies that IT administrators of educational institutions deploy during the integration of the IoT. Therefore, the DOI theory aligned well with the overarching research question and, as a result, was the most suitable theory for the study.

Disruptive technology. One of the prominent models within the innovative theoretical framework considered during this research study was the concept of disruptive technology. Disruptive technology involves the radical use of technology to reform products and services by simplifying the product or services and rigorously moving the product up through the marketing process until major competitors are displaced (Nawaz, 2018). Disruptive innovation denotes the improvement of performance superseding users’ needs and requirements (Montoya & Kita, 2018). Disruptive innovation involves expanding and simplifying a previously complex product or service that served a limited market (Al-Imarah, & Shields, 2018). Disruptive innovation and DOI have simplified the innovation process and the ease of use of technological innovations in common. The differences in the DOI and disruptive innovation lie in the methodologies employed by the innovation process. Although the disruptive innovation framework could fail an institution by overrating a product and misapplying a concept, DOI stresses improving user engagement during the innovation's introduction. I chose DOI because it closely aligned with the research question and was suitable for exploring the strategies used in educational institutions during the IoT integration.

Analysis of Contrasting Theories

Researchers have developed many theories to describe the integration of IoT in institutions. This literature review shows that researchers have employed the UTAUT and TPB theories to explore the possibility of integrating the IoT into organizations. I reviewed these two alternative theories and provided contrasting views from DOI. Reviewing UTAUT and TPB provided a .perspective on the integration behavior of IT leaders.

Unified theory of acceptance and use of technology. The UTAUT concept aims to help IT administrators determine the success factors that influence the acceptance and intent to integrate technology (Venkatesh, Morris, Davis, & Davis, 2003). Integrating a technology hinges on users' positive continuance behavior rather than the innovation's viability (Verma & Sood, 2018). The UTAUT was created based on multiple theories, including the theory of reasoned action, the TAM, the motivational model, and the TPB (Høyland, Hollund, & Olsen, 2015). Persada, Miraja, and Nadlifatin (2019) theorized that the UTAUT has four constructs that help IT administrators determine information systems' usage: performance expectations, effort expectations, social influence, and facilitating conditions. The UTAUT construct helps determine a user's behavioral intentions regarding the integration of technology. Although the UTAUT has multiple useful constructs and has been used to support numerous research positions, it has some limitations that will adversely negate the DOI's positive effect (Thongsri, Shen, Bao, & Alharbi, 2018). In a research study conducted to determine the factors that affect the yearning of IT leaders to implement information management systems, using UTAUT provided insight into the rate of adoption and integration of technology, especially in the context of developing countries (Mukred, Yusof, Alotaibi, Mokhtar, & Fauzi, 2019). The UTAUT is a combination of numerous theories and used to assess behavioral intention's effectiveness toward integrating technology. I did not use UTAUT because I was not assessing only the behavioral intentions of users adopting technology; instead, I explored the security strategies that IT administrators had used to secure the integration of IoT devices in educational institutions.

Theory of planned behavior. Researchers use the TPB to determine the correlation between a user’s intention and actions on the one hand and plans that influence behavior, on the other hand. The TPB indicates that human behavior is goal-driven and, as a result, requires a well-developed plan of action to be successful (Ajzen, 1985). Chipidza, Green, and Riemenschneider (2019) conducted a study to determine why IT leaders cannot fill IT positions, and they used TPB to identify the salient behavioral, normative, and control beliefs attributable to IT adoption and acceptance. Researchers have used the TPB to determine students’ and entrepreneurs’ intentions to adopt a particular trade (Sieger & Monsen, 2015). Moore and Burrus (2019) used TPB’s core tenet of participants’ intention to perform a behavior to investigate the potential for ACT-tested 11th and 12th graders to choose science, technology, engineering, and mathematics (STEM) related college majors and STEM careers. Moore and Burrus concluded that using the best predictors of behavior as the intention to perform a particular behavior was a good predictor of students choosing a STEM career later in life. I did not use TPB because this theory is not testable in all empirical settings to explore the security strategies that IT administrators deploy when integrating IoT devices in their schools (Kolvereid & Isaksen, 2006).

Analysis of Potential Themes and Phenomena

The theme of the security, reliability, and privacy of the IoT permeated throughout the literature review, and Fawaz and Shin (2016) noted the lack of it could have a potentially harmful consequence on the IoT infrastructure and users' data. The security of IoT devices deployed in an educational setting underwent extensive exploration during the literature review, and I highlighted the vulnerabilities that attackers could exploit. The development of strategies and policies to control the infringement on the security, reliability, and privacy of users' data was a constant theme throughout this literature review. Understanding privacy concerns in IoT is a broad and complicated concept, and organizations have different procedures to manage IoT privacy issues (Li & Palanisamy, 2019). The lack of strategies in integrating and managing IoT devices can become an attractive target for hackers who can circumvent security and privacy vulnerabilities in the IoT ecosystem (George & Thampi, 2019).

Essence of securing IoT in education. The continuous advancement of the Internet has spurred the growth of auxiliary technologies and applications. The IoT has been considered one of the disruptive technologies that have transformed humans' lifestyle and uplifted standards in education and living (Ullah, Ahmad, & Kim, 2018). Associated with the increase in technology and improvement in living standards introduces security vulnerabilities that have permeated all technologies, including the IoT (Alam & Benaida, 2018). The IoT has stimulated innovative applications in various IT domains, and cyber-physical systems security has become a frequently discussed topic (Rajamaki, 2018). The IoT's heterogeneous nature has led to the introduction of security vulnerabilities for adopters of the technology (Ge, Hong, Guttmann, & Kim, 2017). The sensors in the IoT have made devices locatable, reachable, and addressable. IoT devices' remote capability attributes that have made the technology accessible have also enabled unauthorized users (Metz, 2016). The IoT has presented challenges to protecting enterprise data privacy due to the enrollment of organizational devices in this new phenomenon (Weber, 2015).

The sensors embedded in enrolled IoT devices pose the most significant risk to the security of users’ data and privacy. Over 1 billion sensors that have been deployed in IoT technology lacked the necessary protections against manipulations by attackers (Fu & Xu, 2018). There is a lack of specificity in the design of sensors for different devices, which has created potential problems for securing the devices that participate in the IoT technology platform (Girma, 2018). Sensors were designed to catch up with the new technology paradigm shift before the technology designing community considered the risk factors involved in the enrollment of IoT devices in the technology (Fu & Xu, 2018). The danger of adversaries causing a distributed denial-of-service (DDoS) in the sensors or causing them to malfunction has grown tremendously over the years (Tankard, 2015). One of the significant challenges facing most educational institutions is determining the causes of security vulnerabilities during the integration of IoT strategies in their educational institutions (Menon, 2017). Some IT leaders do not consider the ethical and security implications when integrating the IoT until a breach occurs. The complexity of

IoT technology makes it difficult to isolate the devices involved in the innovation process (Georgescu & Popescu, 2015). The IoT includes objects and the coordination and relations between user devices that are interconnected (Menon, 2017). The IoT devices connected to the Internet are sometimes personal and unattended, their securities cannot be guaranteed, and they are sometimes managed remotely by unknown administrators.

Strategies required to secure IoT in education. The IoT encompasses millions of sensors and interconnected devices that are continuously exchanging data and, as a result, producing a large volume of data moving through complex networks. Therefore, there is a need to develop security strategies to mitigate escalation in resource congestion and oversaturation (Ren, Li, Dai, Yang, & Lin, 2018). The traffic derived from the billions of wireless devices connected to the Internet and the authentication process's full autonomy can cause IP traffic congestion and pose severe challenges through eavesdropping and data theft (Hammi, Hammi, Bellot, & Serhrouchni, 2018). A decongestion strategy is necessary to ensure communication between all devices is smooth. The IoT requires a resolute security requirement and solution based on a four-layer framework made up of sensing, network, service, and application layers (Li et al., 2016). There is a need for new IoT security designs that will incorporate new standards capable of managing the physical devices connected to the Internet and the services that run on the devices (Laplante, Voas, & Laplante, 2016). For IoT integration to be sustainable, holistic security strategies need to be developed to thwart the exploitation of the reliability, privacy, and security vulnerabilities in the trusted architecture and identity management of the IoT devices.

Policies required to secure IoT in education. IT administrators’ role is to either reduce or eliminate the vulnerabilities introduced due to integrating the IoT into an institution’s networking environment. IT administrators have a responsibility to ensure that users understand the importance of policies geared toward improving the performance and security of the IoT (Garg, 2018). IT executives’ decisions to limit IoT technology's vulnerabilities should align with the organization’s security policy. The security policies must be well written, well thought out, and fully supported by the users (Flowerday & Tuyikeze, 2016). Organizations’ security policies expatiate on the need and importance of organizational security practices. The security of pervasively connected smart devices autonomously interacting using the Internet has been a significant source of concern for most proponents of the IoT (Conti, Dehghantanha, Franke, & Watson, 2018). The security of the IoT encompasses a diverse range of devices and tasks, including the embedding of critical components during the manufacturing process, provisioning of key management, and establishing access control in the devices manufactured to participate in the IoT technology (Keoh, Kumar, & Tschofenig, 2014). Security policies are intended to promote a safe and secure working environment and should therefore not be so technical that the users will not perform fundamental functions such as using their credentials and authorization of access (Sadeeq, Zeebaree, Qashi, Ahmed, & Jacksi, 2018). IoT security policies will provide users with authentication and authorization access to ensure the security of devices that operate on the IoT platform.

Securing IoT in education. Researchers have underestimated the IoT's ability to play a significant role in transforming education over the years. Although the IoT can provide advanced data to support the teaching and learning that occurs every day in classrooms, the support provided via IoT systems also brings some security problems (Asraf, Dalila, Zakiah, Amar Faiz, & Nooritawati, 2018). In a survey conducted by the Information Systems Audit and Control Association (ISACA), three-quarters of the IT professionals who responded indicated that their institutions are likely to experience security breaches due to IoT connectivity (Salierno, 2015). According to Manky (2017), the weakest link in cloud technology is not the architecture but the over 3.2 billion devices connected to the infrastructure. The increased size of the attacking surface, coupled with the shortage of security experts, has made the threat to IoT connected devices critical and urgent. The prevalence of security risk facing the increased use of the everyday product in the IoT concept will affect businesses and household users as the security challenges are immense and varied (Syal & Gupta, 2018). IoT devices have defined the way consumers, and therefore, IT leaders use devices with sensors and wireless technologies such as Bluetooth with its host of associated security vulnerabilities (Sadeeq et al., 2018). The impact of a data breach on an educational institution's database as a result of IoT device integration will be devastating to the security and privacy of users and the institution (Maras, 2015). Therefore, it is incumbent on IT administrators to ensure steps are taken to harden the firewall and other security loopholes created by IoT device integration (Siegel & Sarma, 2019). Creating a security policy that is well thought out and easy to digest can help safeguard the IoT infrastructure and assets of institutions (Garg, 2018). The stakes are even higher when one considers that IT leaders must adhere to the Family Educational Rights and Privacy Act and other federal regulations or face steep penalties (Stahl & Karger, 2016).

IT administrators have a responsibility to ensure security policies have the backing of senior management. IT administrators' role is to enforce security practices, and policies need support from managers who will provide the platform for users to be trained and educated (Almeida, Carvalho, & Cruz, 2018). Investing in IT security does not guarantee that an institution will reduce the risk posed by security vulnerabilities. For IT leaders to ensure the security of an institution's data and user accounts, attention must be paid to the nontechnical human-related issues such as information security education training (Safa et al., 2015). It is imperative for IT administrators considering the integration of the IoT in their institutions to create a security policy that can be efficiently enforced throughout the institution (Wang, Shi, Xiang, & Li, 2016). IoT devices' susceptibility to security attacks was demonstrated in the 2017 WannaCry cyberattack that was unleashed on IoT devices (Kirtley & Memmel, 2018). One devastating effect of a security attack is the theft of an institution's confidential data and user's data. A security breach in education can be devastating, socially, and economically (Yang, Huang, Wang, Chen, & Wang, n.d.). IT administrators need to ensure that devices and sensors used in IoT communication securely support multi-things involved in innovative technology (Hwang, 2015).

Essence of privacy of IoT in education. Privacy is another factor that IT administrators must consider when adopting IoT in their educational institutions.

According to Li, Yan, and Chang (2018), the new IoT paradigm created privacy challenges related to authentication, authorization, confidentiality, and computation. The IoT integrates many smart objects by adopting intelligent data processing mechanisms, communication techniques, and management strategies while seamlessly coordinating the protocols needed to transfer data (Sethi & Sarangi, 2017). The emergence of IoT sensors and other technologies in the devices that engage in IoT technology has created new privacy issues for educational institutions (Qu et al., 2018). According to Andrea, Chrysostomou, and Hadjichristofi (2016), the volume and speed of the processed and transmitted data between devices on the IoT platform have led to privacy concerns. The growth in computing ubiquity has caused some confidentiality and privacy concerns and increased the incidence of malware attacks, data theft, and DDoS attacks in educational institutions (Sahmim & Gharsellaoui, 2017). One of the concerns of IoT proponents is that users are not aware of the violation of their privacy and that devices could be involved in a DDoS attack without the administrators being aware (Bertino & Islam, 2017). Some IT administrators are reluctant to integrate IoT technology in their educational institutions due to their lack of understanding of the vulnerabilities that exist during the integration process (Samanta, Kelly, Bashir, & Debroy, 2018). According to Samanta et al. (2018), although security experts have explored defense against vulnerabilities, IT administrators lack an intelligent understanding of the IoT and its associated collaborative privacy vulnerabilities to provide a platform that will enhance user productivity.

Privacy issues in the IoT can be caused by numerous issues, including lack of any of the following: policies, end-user training, and protection of confidential and an institution’s trade secrets. The existence of sensitive data on IoT devices or networks is a source of concern for IT administrators that could have enormous consequences and implications if the data fall into the wrong hands (Rifi et al., 2018). Due to new privacy and novel attacks emerging with the IoT's proliferation, intruders are now looking for loopholes and other weaknesses in institutions’ IoT architecture to exploit (Jesus, Chicarino, De Albuquerque, & Rocha, 2018). Attackers aim to alter or steal confidential data using Trojan horses, viruses, and worms. In addition to the problems caused by intrusion due to unauthorized access, the advancement in technology and the IoT platform's heterogeneity has increased the attack surface on IoT technology (Rana, Halim, & Kabir, 2018). Criminals use numerous techniques, including social engineering, phishing, hacking, and man-in-the-middle attacks, to access IoT users' data (Khan et al., 2018). The enrollment of physically connected objects with sensors and everyday usage devices in the IoT has extended IoT technology’s attack surface. Therefore, each IoT device could become a vulnerability source, as users' privacy could be infringed upon due to data mining and unauthorized access (Mangaya, Issa, & Chapter, 2018). Therefore, it is incumbent on IT administrators to develop privacy policies that will create awareness among IoT users and prevent attacks on users' privacy.

A privacy breach may expose an organization to information, identity, and trade secret theft. To reduce the level of invasion into IoT users’ privacy, IT leaders must promote awareness by creating policies that will help them determine when their data are being compromised (Kim & Lee, 2017). An informed user group is likely to secure its data privacy, often pervasively and seamlessly collected and connected to the user experience (Im, Kim, Oommen, Kim, & Ko, 2012). As a result of poor data management habits by employees, 85% of security breaches occur during the use of IoT devices. Employees' data are rich targets for attacks, exemplified in the two breaches that occurred to Anthem in 2015 and the U.S. Office of Personnel Management in 2015 (Riga, 2017). The mishandling of data can be deduced to be one of the greatest vulnerabilities posed to educational institutions. The breach at the U.S. Office of Personnel Management in 2015 affected over 22 million individuals and cost the organization over $10 million in cybersecurity preparations. IT leaders tend to reduce their investment in security training anytime there is pressure on their budget (Chpa, 2015). An investment in other sectors of educational institutions' infrastructure takes precedence over users' training, as the lack of understanding in the security implication of not protecting the data and devices enrolled in an IoT program to prevent breaches is sometimes misconstrued (Ko, Wagner, & Spetz, 2018).

Privacy concerns should not deter IT leaders from making available and sharing the institution's data with employees. The extensive use of modern devices that have access to the Internet requires data availability; therefore, investing in data security enables the full utilization of the technology (Panagiotou, Sklavos, & Zaharakis, 2018). It is common for IT leaders to share data to facilitate teaching and learning, using smart devices usually with limited computing power, and this presents users with privacy issues (Zheng, Wu, Zhang, & Zhao, 2018). During the sharing of data in the digital era, the privacy of users has been a fertile ground for attackers, which has led to significant complexities in integrating the IoT in educational institutions' infrastructure (Soultatos et al., 2018). To improve upon the IoT's use and effectiveness, increased collaboration is necessary for the data collection using sensors and other objects (Wu, Zhai, & Zhao, 2018). According to Wu et al. (2018), a traffic monitoring sensor network will require the exchange of data from driving direction computation, traffic characterization, congestion prediction, vehicle fleet management, and an urban management tool to create an efficient and coordinated data-sharing mechanism in the transportation sector. Accurate data make it possible for IT administrators to make informed and quality decisions that reflect positively on the security and privacy of users' data; therefore, there must exist a balance between protecting the privacy of user data and sharing the same data (Kalyani, Rao, & Janakiramaiah, 2018). It can be counterproductive to overprotect data, which explains why some IT leaders freely share data during IoT technology integration (Lee & Lee, 2015). Institutions whose IT leaders take advantage of information sharing need to develop policies to secure users' data privacy. Therefore, IT administrators of educational institutions need to develop policies that will balance IoT data privacy and effective data sharing.

Strategies required to ensure the privacy of IoT in education. Educational institutions' IT leaders must create strategies that will provide users of IoT devices with a clear path to navigate the challenges associated with the integration and usage of IoT devices. To this end, privacy strategies are necessary to help break down and reduce the complexities of protecting IoT users (Bennati & Pournaras, 2018). The simplification of

IoT strategies will enable IoT integrators to monitor users' data, collect accurate data, and support users as part of their attempts to protect user and company data (Yin, Xi, Sun, & Wang, 2018). The successful integration of the IoT requires a user base with knowledge and understanding of privacy strategies (Pacheco, Alchieri, & Barreto, 2018). It is imperative to establish and enforce a user privacy strategy to protect sensitive information between integration and the cloud. The provision of unfettered data and privacy concerns are at the opposite ends of the spectrum, and narrowing the gap has been the challenge for IT administrators. Using various encryption frameworks has helped bridge the privacy gap between device users and cloud vendors (Zhou et al., 2018). It has been a daunting task for most IT leaders integrating IoT technologies to avoid inside attacks due to the sharing of data gathered during the usage of the IoT (Zhang, Chu, Sankar, & Kosut, 2018). The benefits associated with the integration of the IoT can be increased substantially if privacy issues are enshrined and addressed in a grouped strategy document (Bennati & Pournaras, 2018). The volume of data shared in IoT adoption and implementation requires data privacy and confidentiality that traverse the network infrastructure.

The integration of the IoT requires the knowledge of potential pitfalls, and as a result, IT administrators need to identify and strategize on how to prevent the privacy vulnerabilities that are well-known in the adoption of IoT device technology. IoT technology requires new privacy strategies; therefore, IT leaders must not attempt to recycle policies designed for other IoT technologies (Subahi & Theodorakopoulos, 2018). The privacy strategies developed by IT leaders adopting the IoT need to be holistic and must address all technology facets, including data at rest and in motion (Barga, 2016). To preserve sensitive intellectual property and financial data, IT administrators are responsible for enshrining monitoring and measuring matrices in privacy policies (Yu, Tian, Qiu, & Jiang, 2018). One way to ensure data safety is to encrypt the data packets that traverse the network to avoid leakage, conspiracy, and data theft (Chervyakov et al., 2017). Yu, Wang, Liu, and Niu (2018) concluded that attacks could be attributed to external intruders, and insiders also have the potential to cause vulnerabilities to the privacy of data through the accidental leakage or theft of intellectual properties during IoT integration. IT leaders can use various techniques to minimize the effect of this mishap, which include lightweight authentication schemes and authorization methods (Chen, López, Martínez, & Castillejo, 2018). Man-in-the-middle attacks and access to the physical infrastructure of the institution are prime targets for privacy infringement, and as a result, IT leaders need to develop privacy strategies to preserve the confidentiality of users' data through the use of an encrypted virtual private network/IP Security tunnel (Condry & Nelson, 2016). Adopting prudent privacy strategies can ensure the privacy of an institution's confidential data and intellectual property.

Policies required to ensure the privacy of the IoT in education. The IoT ecosystem comprises users, various sensors, devices, data collectors, an institution's legal minds, and other stakeholders, and as a result, needs formidable strategies to provide a coherent business model. Any effective strategy must be enshrined in policies. IT leaders interested in preserving their institutions' data need to develop policies that clearly state the method needed to secure the data (Yang et al., 2017). The inclusion of access-control mechanisms and encryption methods to protect institutions’ data privacy is vital to an organization's security and viability (Condry & Nelson, 2016). The satisfaction of privacy requirements plays a fundamental role in building confidence in the IoT ecosystem (Sicari et al., 2015). One way to propagate the privacy policies developed is the internal training of staff and uploading policies to an institution’s internal website. The dissemination of information on the importance of protecting users’ privacy and their data is paramount, and that is the main reason any privacy policy that is created needs to have as its core the protection of data (Nandan et al., 2020). Such a policy should highlight some of the techniques attackers have used to access the confidential data of users and institutions (Mini & Viji, 2017). Using methods such as social engineering, man-in-the-middle, and Trojans by intruders to access the institution’s data must be stressed in any privacy policies developed by the institutions (Baagyere, Qin, Xiong, & Zhiguang, 2016). The massive amount of data shared by IoT devices makes them susceptible to attacks, and as a result, an institution’s IT leaders must reinforce the importance of protecting data through training models and other methods (Fu, Wang, Xu, Mi, & Wang, 2019). The IT administrators of educational institutions must create and refine policies, including acceptable-use policies and access-control mechanisms, to prevent unauthorized access to confidential documents (Hernández-Ramos et al., 2018). The interoperability and data access level by vendors and other external users is critical to the integrity, confidentiality, and privacy of IoT-embellished systems (Raza, Helgason, Papadimitratos, & Voigt, 2017). To prevent the tainting of stolen data, IT leaders need to consider privacy concerns with all seriousness and reprimand violators for deterring all attempts to abuse users' privacy.

The result of a privacy policy weakness could be a data breach, and a data breach could be damaging to the organization's reputation. The lifeblood of any institution is the security and privacy of its users' data. Therefore, a breach could have a devastating effect on an institution's image, profitability, pedigree, and clientele base. According to Solangi et al. (2018), researchers have focused on privacy and trust concerns inherent in the optimal performance of the IoT in an educational setting. Real-time monitoring of data is a method to ensure an institution's data privacy, confidentiality, integrity, and availability (Triantafyllou, Sarigiannidis, & Lagkas, 2018). Integrating the IoT in an educational institution requires the security and privacy of all data generated during the technology usage. IoT technology promises tremendous benefits, but it is incumbent on IT administrators to ensure the risk of compromising the generated data does not outweigh the benefits (Haddud, DeSouza, Khare, & Lee, 2017). There is no risk-free proprietary or confidential data, so IT leaders must prioritize which data to protect with the limited set of resources available (Freund, Fritts, & Marius, 2016). IT leaders must ensure the grades, personal data of users, financial documents, and business strategies are not compromised during IoT integration and usage.

It is cost-effective to bundle the messaging of reliability, security, and privacy issues, as these three domains go together. IT leaders may craft policies with reliability, privacy, and security concerns in mind, but IT administrators must also invest in creating secured encryption and authentication methods to protect the privacy of data (Andrea et al., 2016). When integrating the IoT in an educational institution, the IT administrators and their teams need to ensure the infrastructure is hardened to prevent recalcitrant users from compromising the organization's data's reliability, security, and privacy (Li et al., 2016). Users must be imbued with all the required knowledge to enable them to make an informed decision that will affect the security of the network infrastructure and the data that traverse it (Hou, Qu, & Shi, 2018). Institutions implement different privacy levels, and therefore, the tightening of access to data must be commensurate with the business needs, policy, and design. The interaction with data needs to be regulated, and the privacy of the owners of the data needs to be respected, whether individuals or institutions are harvesting the data (Miloslavskaya, Nikiforov, & Budzko, 2018). Vendors of IoT devices continue to introduce features into their devices but fail to patch those devices for privacy vulnerabilities. Vendors typically have one device that fits all operations without considering the devices' heterogeneity and organizations that use the devices (Villari et al., 2017). As part of the efforts to protect users' privacy and their data, IT leaders must be cognizant of the rules and regulations that govern their industry (Sullivan, 2018). Violators of state and federal laws face substantial punitive measures, which could cripple an institution's performance and its profitability (Li & Palanisamy, 2019). Therefore, the integration of the IoT by institutions must consider the privacy of data and state, federal, and international laws and balance them with the need to share data freely (Pasquier et al., 2018). The level of privacy protection and financial or security risk associated with IoT data management is a decision that needs to be made by the IT leaders during the integration phase.

Privacy of the IoT in education. The introduction of the IoT in an educational institution has tremendous benefits, but many institutions lack the knowledge to integrate technology into their educational environment security. The collection, storage, and sharing of a large volume of data have outpaced the privacy expectation of some institutions and, as a result, have halted the integration of IoT (Adams, 2017). The use of the IoT in educational environments requires access to geographically restricted systems, cloud and biometric datastores, and the network infrastructure of the educational institution (Lee, Chen, Li, Cheng, & Lai, 2019). The effective performance of IoT devices in educational institutions also requires access to low-cost design and stable virtual objects by students when off-site (Gokceli, Zhmurov, Kurt, & Ors, 2017). The primary aim of integrating the IoT in educational institutions is the easy access to data to increase the efficiency of the teaching and learning process (Guo, 2018). User data management has become a shared burden between users, institutions, and private Internet providers. Devices that share data on multiple platforms have potential privacy issues such as leakage and access authorization (Mollah, Azad, & Vasilakos, 2017). IT leaders should create policies that will protect users' data privacy while on the institution's network and external storage devices in the shared storage infrastructure. In a world of unfettered and instant access to online education, users have to be informed of the state of their data and of policies that have been put in place to protect them from unauthorized access (Li et al., 2016). At the same time, users may experience specific privacy infringements if they require data on a whim, trusting that the IT administrators will institute IoT technologies and potential regulations to ensure the application of IoT data management techniques to protect privacy (Perera, Ranjan, Wang, Khan, & Zomaya, 2015).

Educational institutions do not perform in isolation. They are required to abide by state and federal regulations, as well as internal ethical conventions. Some rules, laws, and regulations protect the handling of IoT data, and institutions that wish to adopt the IoT need to adhere to the General Data Protection Regulation (GDPR; Singh et al., 2018). One of the tenets of GDPR is data protection, depending on whether the data are personal or belong to an institution. Educational institutions can use GDPR as the foundation of the privacy policy while identifying the institution’s core business function's conflicts if the user’s data conflict with the institution’s data (Subahi & Theodorakopoulos, 2018). While federal authorities may sanction educational institutions that do not follow GDPR, the irreparable damage caused to the data owners could also damage the institution (Singh et al., 2018). The least that institutions integrating the IoT can do is to enshrine GDPR and other federal laws in their privacy policies and train their users to be aware of the ramification of violating these policies (Varkonyi, Kertesz, & Varadi, 2019). The IoT has been touted as part of the information superhighway, and as with any technology, rules of engagement have to be respected and refined. Educational institutions need to safeguard their reputation and the privacy of their user’s data by adopting privacy policies that will protect both an institution’s confidential and its users’ data.

Essence of reliability of the IoT in education. The reliability of data being transported using IoT devices is critical to the success of an educational institution. Reliability has been classified as one of the essential concepts used to measure information protection. One of the most essential IoT device integration characteristics is the systems' reliability; therefore, the integration process needs to receive special attention (Safaei, Mahdi, Monazzah, Bafroei, & Ejlali, 2017). The successful integration of IoT in educational institutions depends on how reliably the large volume of data generated by the IoT devices is managed and protected (Najjar-Ghabel, Yousefi, & Farzinvash, 2018). Reliability establishes confidence in an organization, as users of IoT devices will be comfortable that their data will not be altered due to the maintenance of performance standards and protocols (Pokorni, 2019). The concept of reliability refers to the expectation that IoT systems will perform optimally under prescribed conditions (Deif & Gadallah, 2017). IT leaders must ensure that no one or nothing compromises data quality and productivity (Georgakopoulos, Jayaraman, Fazia, Villari, & Ranjan, 2016). Ubiquitous smart devices enrolled in IoT technology acquire and distribute a massive amount of data. IT leaders have to define the means to validate the authenticity of data that are both at rest and in motion (Lennvall et al., 2017). IoT sensors' performance and the reliability of data gathered need to be efficient and accurate, respectively (Zhang, Szabo, & Sheng, 2016). For data to stay accurate, they must not have been altered through systems error, and accidental errors must be minimized (Banerjee & Sheth, 2017). In research by Jia, Zhu, Li, Zhu, and Zhou (2019), it was determined that, for systems to be considered reliable, the packet loss rate must not be lower than 1%, and the average packet correct rate should exceed 98.5%. Attaining IoT systems reliability and data availability could be difficult for IoT devices to achieve because they perform at numerous and different layers that depend on each other.

According to Jiang, Shen, Chen, Li, and Jeong (2015), IoT devices achieve reliability when storage and data are available are at a highly secured, stable, scalable, and synchronized level. There are multiple reliability failure points, including bugs in operating systems, the Internet, defective hardware, lack of data availability, and user error. IT leaders can track and attend to the points of failure, but one of the first areas that need testing is the devices and their ability to connect to the Internet using various wireless protocols. The ability of IoT devices to reliably connect to the Internet is not negotiable, as that is the primary benefit of IoT devices (Mcleod, 1994). Reliability issues must, therefore, be factored into the process of IoT integration by educational institutions.

Educational institutions are massive consumers of data and, as a result, require IoT technology to continue the trend of ensuring their data and related systems are reliable. The probability that the system and data do not fail but perform under the right condition and functions, as required, makes the IoT reliable (Guan, 2018). Skewed data can negatively affect institutions' performance, so the development of multiple layers of system checks that will ensure the reliability of the data being harnessed is necessary (Mataloto, Ferreira, & Cruz, 2019). IoT devices interact with the network architecture at numerous layers, and therefore, reliability is a critical factor in building confidence in the system (Safaei et al., 2017). The reliability of data depends on the integrity, availability, and confidentiality of the systems that process the data. Reliability refers to the stability of base data through redundancy to reduce downtime, corruption, and inefficiency in data transmission while maintaining data integrity and fault tolerance (Xing, Tannous, Vokkarane, Wang, & Guo, 2017). The lack of an IoT reliability strategy can lead to integrity issues as the failures in governance and employees' erroneous actions can put an institution's systems at risk (De Cremer, Nguyen, & Simkin, 2017). Most IT leaders prefer to maintain their data's original state, as final computation and analysis will not be accurate if the data keep changing. Trusting data in the cloud is one of the most challenging integrity sustenance dilemmas since users rely on cloud service providers to protect and securely deliver data on time to institutions (He et al., 2018). The change in data integrity has security implications, as institutions have to wonder who is tampering with the data and what percentage of the data is unreliable (Tian et al., 2019). Ideally, institutions will prefer 100% integrity of their data, but this is achievable only if authentication mechanisms are put in place to check the data at every stage of storage (Koo, Shin, Yun, & Hur, 2018). IoT data integrity and trustworthiness are essential reliability concerns, especially when constrained storage and processing (Hameed, Khan, Ahmed, Reddy, & Rathore, 2018). Apart from human factors, multiple other factors could impede the achievement of full integrity, and they include inadequate support systems, poorly written algorithms, defective backup systems, physical and cyber-attacks, system inaccuracies, and hardware and software failures (Nurunnabi & Hossain, 2019). Therefore, IT leaders of educational institutions must implement a system that will continuously check the data to ensure that the data conforms to set parameters so that the data's integrity can be guaranteed.

One other indicator of reliability is systems performance. Devices have to perform at different network infrastructure layers to enable data generated by IoT devices to be trusted and reliable (Guan, 2018). IoT device users expect the data, both in motion and at rest, to be intact when retrieved and transmitted. Users expect the infrastructure to guarantee that the data will not be altered, skewed, or degraded (Farhan et al., 2018). The reliability in an institution’s infrastructure's performance is the probability that the system can complete the operation by managing traffic volume within the prescriptive time (Xing et al., 2017). The system should be available 99% of the time, and the data produced must be accurate (Lennvall et al., 2017). Because the network could be overloaded due to the infrastructure's excessive tasking, a throttling mechanism must be instituted to prioritize processing tasks for accuracy reasons. Therefore, IT leaders must make sure that user confidence is not diminished due to performance and reliability issues.

Strategies required to ensure the reliability of IoT in education. Most educational institutions do not consider reliability issues until after an IoT infrastructure has been set up, and users experience poor performance and instability. The IoT is a new technology, and there has not been enough research and history on reliability-related issues. A typical IoT sensor or RFID has little to no storage and processing power, and therefore, computation and network support have to be provided at the infrastructure level (Ali et al., 2015). Institutions integrating this technological paradigm shift need to develop strategies geared toward ensuring the devices' reliability and transferring data to and from the devices (Castaño, Beruvides, Villalonga, & Haber, 2018). It is worthy of note that the reliability of IoT devices is typically not one of the core aims of the manufacturers of IoT devices. IT administrators have a responsibility to seamlessly integrate sensor-embedded devices into the IoT network infrastructure from a reliability perspective (Jiang et al., 2015). Strategies need to be deployed to ensure smooth communication between remote sites and heterogeneous sensors (Ali et al., 2015). With the heterogeneous nature of devices enrolled in IoT adoption and integration, it will be beneficial for institutions to address reliability using a coherent strategy. The development of a strategy that confirms the reliability of devices and data engaged in IoT technology is imperative. The instructions that tie access to IoT resources must be adhered to if the reliability, availability, integrity, and performance of devices are synchronized (Sicari, Rizzardi, Miorandi, & Coen-Porisini, 2017). Many factors help make IoT systems reliable, and key among them is the hardware of the devices, the software that runs on the devices, and the institution's infrastructure. The development of a reliability strategy by educational institutions may require reducing possible multi-points of failure in IoT interconnected devices (Singh et al., 2018). A single point of failure could cripple the entire IoT technology installation and affect the educational institution's effective teaching and learning, especially during an IoT system attack. Reliability strategies must ensure servers that intercept and transfer IoT communication are configured to have the ability to upload data to cloud platforms to act as fault-tolerant and high availability (Pacheco et al., 2018). IoT servers must have the ability to retain and transfer data when called upon in the event of catastrophic damage to the main servers. Therefore, it is a good business plan for institutions to have an implementable reliability strategy that needs to be refined yearly, considering technological advancement.

The performance of the IoT network backbone is one area that could affect the reliability of IoT. IT administrators of educational institutions need to simplify network design and remove bottlenecks to improve the data's transportation and security that traverse the network. The processing of data into meaningful information will be enhanced if IT administrators correctly configure the IoT infrastructure to facilitate optimal and stable performance (Roldán, Real, & Ceballos, 2018). Institutions need to eliminate compatibility and interoperability issues in IoT to ensure devices interact with the infrastructure at a high level for IoT devices to take advantage of IoT server infrastructure (Triantafyllou et al., 2018). The role of IT administrators during the IoT integration is to preserve the integrity of IoT data. Data loss could be detrimental to the confidence posed by users in the IoT. Educational institutions need to ensure safeguards have been put in place to prevent the loss of data. Performance issues could result from poor network architecture design and configuration, theft of data, and the lack of an integration policy (Sicari et al., 2017).

Identifying issues that affect the performance of the IoT has to be a continuous effort on the part of IT administrators if their reliability strategy in IoT is to be successful. Congestion is another factor that could potentially affect the performance of IoT integration and implementation. According to Mishra et al. (2018), network congestion is one of the fundamental problems of computer networks, and the inclusion of the IoT in the mix provides fertile ground for reliability issues. The protocols and modernness of applications that run on devices enrolled in the IoT could cause some congestion and, as a result, hamper the performance of the IoT. It is the expectation that the devices used in

IoT address flow control, congestion control, and the segmentation and reassembling of data packets (Mishra et al., 2018). The design of the operating systems running on the network infrastructure, the version and security of the software installed on the IoT devices, and the Internet bandwidth size can affect the IoT's performance during integration (Bonafini et al., 2019). The system should be designed to withstand multiple fault-tolerant provisions as the continuous uptime of the infrastructure is essential to the performance of the IoT during the integration process.

Policies required to ensure the reliability of the IoT in education. The integration of the IoT in educational institutions requires the prior development of reliability policies. Well-developed reliability policies can provide performance standards, set benchmarks in data protection, stabilize the network, manage the heterogeneity of devices operating in the IoT ecosystem, and ensure the security of both infrastructure and devices (Moghaddam, Wieder, & Yahyapour, 2016). Reliability in the integrated system, including IoT infrastructure, ensures users have confidence in the technology's performance. One way to measure the performance of the IoT is to have a policy that ensures consistency and high availability (Hwang, Lee, Park, & Chang, 2017). Though it has been difficult for IT Leaders to capture real-time data to depict real situations, the IoT-based performance measurement consisting of ISA-59 and ISO-22400 standards have served as a performance indicator (Hwang et al., 2017). IT administrators of most educational institutions desire a resolute and robust IoT network infrastructure that can support all the IoT devices used daily by students and staff. Educational institutions can use IoT reliability policies to enhance learning outcomes by collecting real-time and actionable insight into students' performance (Aldowah et al., 2017).

The reliability policies of an educational institution need to include a base threshold that the IoT infrastructure must meet to be considered satisfactory, and the threshold must include the assurance that students' and faculty's data will be available and the Internet will be stable (Moghaddam et al., 2016). The use of the IoT permeates industries, and while IT leaders of educational institutions use the IoT to share knowledge, the IT leaders of environmental institutions use the IoT to predict the weather and environmental hazards. IT administrators in educational institutions need to place a high value on the IoT infrastructure's performance to preserve user data integrity (Aldowah et al., 2017). It is nearly impossible to sustain and maintain the performance baseline of the IoT infrastructure; thus, IT administrators of educational institutions need to create and sustain reliability policies geared toward efficient resource allocation and enhanced performance of IoT devices (Shah & De Veciana, 2015). The establishment of IoT infrastructure baseline policies will help IT administrators measure the infrastructure's minimum performance standards.

An unstable and poorly written software application could profoundly affect the performance and stability of the IoT infrastructure. Software on devices regularly interacts with the IoT infrastructure and, as a result, needs to be bug-free (Siboni et al., 2019). The discovery of software vulnerabilities can increase through testing and retesting the applications installed on devices (Wang et al., 2019). IT administrators need to ensure that software on user devices and applications accessed globally by users are patched and tested in a timely fashion, as there are over 100,000 well-documented vulnerabilities (Cristian, Grigorescu, Deaconescu, & Mihnea, 2018). Updating software and testing could either discover systems vulnerabilities or confirm the IoT technology infrastructure's stability. Testing software has the benefit of reducing the possibility of attacks on the IoT infrastructure, as IT administrators will determine the extent of the vulnerabilities of the software being deployed into the production environment (Munea, Lim, & Shon, 2017). IT administrators establish an elaborate software reliability test using real-time scenarios to check the reliability and ensure trouble-free and full utilization of the devices (Tyagi, Kumar, & Kumar, 2017).

Reliability of the IoT in education. IT leaders are used to virtualization in one form or the other, but the integration of the IoT has faced some resistance, as IT administrators are unsure of the role that IoT can play in the teaching and learning paradigm. Reliability and security are some of the reasons IT administrators have been hesitant to integrate the IoT into their production environment, and the enrollment of personal devices in the network environment is another reason IT leaders are late integrators of the IoT (Boit, 2017). IoT technology requires the uptime of critical infrastructure to be a prerequisite to device authentication and reliability (Lennvall et al., 2017). Current IoT devices and infrastructure need to have 99.9999% reliability and uptime, and attaining 99.9999% reliability is challenging, especially in an environment where heterogeneous devices transmit data in real-time (Lennvall et al., 2017). The efficient, reliable, and speedy delivery of data should be the primary goal of IT administrators, and content-centric networking can be deployed to assist significantly in making the IoT reliable (Bosunia, Hasan, Nasir, Kwon, & Jeong, 2016). It is incumbent on IT administrators in educational institutions to develop an IoT strategic policy that makes systems highly available while at the same time secure from unauthorized external access because the negligence of cloud data storage vendors could jeopardize the reliability and availability of data (Bahrami et al., 2016). Students and faculty need to have access to their data and the infrastructure at all times, regardless of the storage location.

One way to achieve sustainable reliability is to attend to every issue, regardless of size, and keep users informed of every policy and strategy change. IoT users are typically unaware of policies that govern technology (Das, Degeling, Smullen, & Sadeh, 2018). For example, users do not know the mechanism to opt-in or out of data collection processes. Educating users on reliability policies will become part of the solutions as they will make informed decisions that will make the IoT reliable. Other ways to achieve reliability in the IoT include creating excellent cross-domain IoT integration policies, strategies, procedures, and user training (Das et al., 2018). To successfully integrate the IoT, IT leaders can develop strategies geared toward the high reliability of the IoT infrastructure and the enrolled devices. This research study outlined some strategies that IT leaders could deploy to enhance their IoT infrastructure reliability.

The characteristics of the DOI theory influenced this study. These characteristics served as an outline to understand reliability, privacy, and security strategies during IoT integration in educational institutions. IT leaders ensure the concurrent attainment of reliability, privacy, and security during IoT integration. An educational institution’s IoT infrastructure's demise could come to fruition if IT administrators do not establish a careful balance between security, privacy, and reliability to create trustworthiness (Das et al., 2018). It is the IT leaders' responsibility to integrate their current infrastructure into the IoT technology and ensure the systems jell to the benefit of IoT users. The raw data collected by the IoT sensors from multiple heterogeneous IoT networks have the propensity to present noise, outliers, and redundancy in the IoT ecosystem (Sanyal & Zhang, 2018). The constant monitoring of the IoT systems, data traffic, and the packets traversing the IoT network infrastructure will likely ensure the reliability of IoT users' data and the architecture's stability. The characteristics of DOI should influence the strategies used by IT administrators when creating IoT security and reliability policies. For the integration of IoT to be successful, IT administrators must consider student and staff usage patterns to determine peak and low network use trends (Casoni, Grazia, & Klapez, 2017). The security and reliability vacuum created in the IoT infrastructure resulting from integrating the IoT in educational institutions has raised challenges and opportunities for further research to resolidify the solutions to IoT security and reliability issues (Granjal et al., 2015). Identifying standards in IoT integration is long overdue, and IT leaders must keep testing and documenting results to develop strategies that will ensure the successful integration of the IoT. Further study is necessary to find a standardized system geared toward the integration of the IoT.

IT leaders used the DOI theory to explore characteristics exhibited during integrating innovative technologies by educational institutions. The DOI theory, aimed at spreading new ideas or products, comprises four independent but linked components:

innovation, communication channels used, time component, and social system; Scott and Mcguire (2017) used all these components to examine the strategies deployed by IT administrators to integrate IoT devices into educational institutions securely. IT administrators of educational institutions will be the ultimate beneficiaries of the strategies identified in this study, as they will become well informed of the security strategies that could be deployed during the integration of the IoT in their educational institutions.

Relationship of This Study to Previous Research

Researchers have used the DOI theory to support technology deployment in multiple organizations, including educational institutions (Rogers, 1995). Researchers have also applied the DOI theory to the adoption of bicycling as a means of transportation by determining the correlation between the DOI's perceived compatibility and the stage of adoption (Nehme et al., 2016). IoT integration decisions are mostly made by IT leaders at the corporate levels of educational institutions, and DOI has been the framework that researchers have used most often to explore the effectiveness of integrating technology in an educational institution for teaching and learning purposes (Hsu, 2016). Morrison, Reilly, and Ross (2019) showed that educational institutions' integration challenges were consistent with previous DOI research results. The IT leaders of the British Columbia Institute of Technology integrated numerous technologies using the DOI framework with considerable success to support student-centered learning and the adoption of new teaching techniques (Doyle & Budz, 2016). Dintoe (2018) contended that DOI influences the use of accessible and available innovative technology.

At the individual level, some studies have confirmed that the integration of the IoT using Rogers's (2015) DOI theory can be successful if users' preferences are met and usage motivation is high. Though the private sector has experienced the frequent use of DOI in integrating IoT devices, there are substantially high geographical, socioeconomic, and legal subsystems barriers that impede this innovative concept's acceleration into the private sector (Zanello, Fu, Mohnen, & Ventresca, 2016). Thomas, Costa, and Oliveira (2016) investigated the integration of innovative technology in IT-enabled process virtualization, and they proposed a conceptual model that combines various theories, including DOI, TOE, and process virtualization theories.

Rakic, Novakovic, Stevic, and Niskanovic (2018) used a mixed-methods approach in a study and found that the integration of mandatory health standards in the Republic of Srpska, Bosnia, and Herzegovina, produced varying results due to the extent of adverse financial repercussions, availability of information, availability of support, and vendors' perception of the newly integrated standards. Nieuwenhuijsen, Correia, Milakis, van Arem, and van Daalen (2018) used a novel quantitative research model to evaluate the effect of a dynamic and complex innovative automation system. The use of a systematic-quantitative research framework to investigate innovative technological systems led to the conclusion that integrating technologies in developed countries requires disseminating DOI processes, which can be complex and slow (Aslani & Naaranoja, 2015).

Transition and Summary

The purpose of this multiple case study was to examine strategies adopted by IT administrators when integrating the IoT in educational institutions. Section 1 included examining the concept of the IoT through the lens of DOI theory, with reliability, security, and privacy strategies by IT administrators being the focus. This section included the study's background and a review of the literature with strategies designed for the reliability, security, and privacy of IoT devices in mind. I reviewed the concept of the IoT and determined that the subject lacks extensive research, and IT leaders are still exploring the security, reliability, and privacy issues associated with integrating the technology into their educational ecosystem. I explored the use of DOI theory in institutions during the integration of the IoT and observed that the process is efficient if effectively communicated, and users understand and accept the integration process. During the literature review, I examined the application of DOI theory, coupled with TOE, TAM, and TRA frameworks in various instances, to implement or investigate the efficacy of integrating the IoT into educational institutions. It became apparent during the literature review that the continuous efforts to find ways to integrate the heterogeneous IoT phenomenon efficiently have provided opportunities for further research into leveraging DOI theory with TOE, TAM, or TRA frameworks in the education industry. Therefore, an opportunity existed for research into the strategies used by IT administrators during the integration of the IoT into educational institutions.

In Section 1, I aligned the five characteristics of Rogers’s DOI theory with IoT device integration in education institutions. I was able to derive some benefits attributable to the characteristics of DOI and the compatibility of IoT, and existing technology is one of those benefits. I gleaned from this section that educational institutions can also benefit immensely from the relative advantage of introducing innovation into the existing infrastructure. Based on the reviewed literature, I developed an understanding that the concept of trialability enables IT leaders to pilot test innovations to ensure they fit into the perceived innovation. Observability is the next DOI characteristic I examined, and it relates to scrutinizing the technology and determining its accrued benefit to an educational institution. Finally, I analyzed the DOI characteristic of complexity and determined that it allows IT leaders to understand the innovation's intricacies, enabling them to fully understand the level at which the technology is useful to the institution. By combining the heterogeneous nature of the IoT with the lack of strategies that lend themselves to vulnerabilities, I was able to deduce that IT leaders strive to enhance education delivery to their clientele and need to take advantage of the new paradigm shift enrolling day-to-day devices in their network infrastructure. I was also able to deduce that IT administrators of educational institutions have a responsibility to modernize their systems to take advantage of the devices owned by the users and be conscious of security, reliability, and privacy concerns. Innovation leads to growth and, subsequently, profitability.

Section 2 includes the research design, population sample, and methods used in this study on the integration of the IoT. Section 3 includes an overview of the study and the presentation of findings based on the analysis of the data collected. Section 3 includes a discussion on applying the research to professional bodies and presenting the recommendations, reflections, and conclusions from the study.

Section 2: The Project

In this section, I provide information about the research method, design, and methodologies used in this study. As the researcher, I describe my role, the criteria used for selecting research participants, the population sample, and ethical research considerations for the study. In addition to explaining the data collection method, I clarify the processes used to perform the analysis.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the security strategies that IT administrators had used to secure the integration of IoT devices in educational institutions. The targeted population was IT administrators of 11 educational institutions in the Midwest region of the United States who had developed strategies to integrate IoT devices securely. The study was limited in its geographical setting to five cities in Indiana: Carmel, Fishers, Indianapolis, Muncie, and Wabash. This study's findings may contribute to positive social change by providing strategies that IT leaders at educational institutions can use to securely transform education delivery to students and safeguard educational personnel’s data.

Role of the Researcher

I was the primary data collector for this research study. A researcher’s role is to direct the research to the desired goals and interpret the research findings (Karagiozis, 2018). The qualitative researcher subjectively applies human intentions during a research study to inform and reshape the methodology, interpretation, analysis, and treatment of the gathered data related to the phenomenon under study (LeCroix, Goodrum, Hufstetler,

& Armistead, 2017). My role as the researcher mainly consisted of being the primary instrument for interviewing the participants and collecting other data and interpreting, analyzing, and presenting the study findings. Cronin (2014) indicated that a researcher's role is to provide a good description of the study that accurately portrays the entire experience, including the design of the study, the interview questions, and the selection of participants using best practices, in addition to ensuring researchers are not disruptive and do not inject themselves into their research. My role in this qualitative multiple case study included analyzing the data gathered from the participants. According to Nilson (2017), the researcher's role is to be a facilitator, coordinator, and participant-observer who participates in direct observation and interviews. I used my role as the main instrument to ensure that the research was objective and unbiased and portrayed the participants' viewpoint.

I have been in the IT profession for 20 years, specializing in server infrastructure and virtualization. I have spent the past four years working in a school district where IoT device usage has increased. Though I had some preexisting knowledge about the IoT, I lacked experience with the security, reliability, and privacy of the technology, and as a result, I had limited bias on the topic during the study. I have worked in educational institutions for over 15 years, and although the use of IoT devices has increased exponentially, not many educational leaders have considered the security, reliability, and privacy of the devices and their integration in the IoT infrastructure. The lack of security strategies to prevent data breaches that result from the integration of IoT devices in educational institutions compelled me to research the topic of the IoT in education.

The safety of students’ data and the reliability of an educational institution’s network infrastructure were the main reasons this research study was essential. I had some conversations with my peer IT administrators on the topic to justify the need for a research study into the security, reliability, and privacy of IoT in educational institutions. However, there was no relationship or coordination with the members of the potential institutions I studied. I approached the selected IT leaders for approval to study after the Walden Institutional Review Board (IRB) approved my research study. To foster a meaningful research study and obtain accurate data, I sought trust and openness with my participants. According to Guillemin et al. (2018), the trust relationship between the researcher and participants is paramount to the research's success.

I employed appropriate ethical considerations during the research and data collection phases of the study. Ethical data collection requires informed consent, data ownership, quality data, and participants' opportunity to back out of a study (Roberts, 2015). I emphasized respect for participants and the quality of the participants' data and avoided analyzing the participants' personal attributes. Informed consent, transparency, and control over the interviews are essential ingredients to successful data collection (Nebeker, Linares-Orozco, & Crist, 2015). As part of my preparation for this research study, I completed the National Institutes of Health, Office of Extramural Research, a course on research ethics, which prepared me to understand the participants’ role and how to protect them (see Appendix A). I also adhered to the *Belmont Report*’s on ethical guidelines for handling human participants (Koro-Ljungberg, Gemignani, Brodeur, & Kmiec, 2007)I used the *Belmont Report*’s tenet of creating an ethical judgment and generating a boundary between the participant and the process of developing ethical research. My understanding of the *Belmont Report* protocol improved my ability to act ethically during the study.

I avoided bias by gathering data using semi-structured interviews and observing ethical considerations. Researchers use semi-structured interviews, peer review, investigative responsiveness, and ethical obligation to mitigate biases during research (Wadams & Park, 2018). Because researchers can influence research findings, they should take steps to avoid doing so (Segev et al., 2016l; Shepperd, Hall, & Bowes, 2018). I strove to avoid bias by making the participants comfortable and not allowing their responses to my interview questions to influence the study findings. I used open-ended and semi-structured questions to interview my participants, and I avoided injecting my thoughts and personal beliefs in the interview process.

I conducted interviews using an interview protocol. An interview protocol enables a researcher to briefly introduce the interview in lay terms, explain the interview procedures, and provide the participants with the opportunity to inquire about the research study (Liao & Hitchcock, 2018). The interview protocol provided me with a broad outline of my interview, areas to explore, possible questions, and methods to transition between questions (see Appendix B). Yeong, Ismail, Ismail, and Hamzah (2018) noted that a reliable interview protocol is one reason researchers can obtain quality interview data. Additionally, using an interview protocol ensures alignment between interview questions and the research question. I was able to ask tailored interview questions to the participants using the carefully crafted interview protocol.

Castillo-Montoya (2016) laid out a four-phase interview protocol refinement process consisting of the following phases: aligning interview questions, constructing an inquiry-based discussion, getting feedback, and testing the interview protocol. This four-step process was my guiding principle during the interview process, as it enabled me to produce balanced interview data.

I provided the participants with the opportunity to ask questions, and as a result, they enriched my research study by providing quality responses to the interview questions. The interview questions' informed responses served to provide the participants' viewpoint on the privacy, reliability, and security of integrating IoT devices into educational institutions. I chose the semi-structured interview method because it was essential for the participants to be free to provide uncensored answers geared toward the secured integration of the IoT in educational institutions and ask follow-up questions.

Participants

Selecting the right participants for the research study was a necessary impetus for the research study's success. The improvement of participants' literacy is essential to full and informed participation in a research study (Kiernan, Oppezzo, Resnicow, & Alexander, 2018). Ensuring that participants were eligible to participate in the research study was essential to meeting the research study's requirements. The process of selecting the participants for the research study was a critical activity, as the accuracy and richness of a study's finding is a direct reflection of the data collected from the participants (Ross, Iguchi, & Panicker, 2018). Although familiarity with the phenomenon under study can breed bias in a research study, researchers must have enough sample data from participants to ensure the research is credible (Liao & Hitchcock, 2018). The research study comprised a semi-structured interview with IT leaders of educational institutions in the Midwest region of the United States who had successfully integrated the IoT into their educational institutions. IT leaders of educational institutions include CIOs and IT directors. IT leaders are decision-makers and subject matter experts with knowledge in security strategies in their respective institutions. The IT leaders who participated in an interview had developed and used strategies to prevent data breaches resulting from the integration of IoT devices in their educational institutions.

I also recruited individuals in the institutions to act as gatekeepers. An essential component of successful access to research participants in an institution is the gatekeeper who can either support or hinder the research based on how they value and view the research to the institution (Høyland et al., 2015). The IT leaders of institutions who participated in the research study were selected based on their successful integration of IoT devices in their educational institutions. I interviewed participants after receiving approval from Walden University’s IRB.

An effective way to contact participants is to ask a gatekeeper who works in an institution to provide a list of individuals who potentially qualify to participate in the study. Researchers use gatekeepers to obtain a list of possibly qualified participants who meet the selection criteria and bridge the gap between the researcher and the institution (Shaw, 2018). The role of a gatekeeper is to facilitate the selection of potential participants for a research study, as the gatekeeper may have initial direct access to the participants, and the gatekeeper's role ends after the gatekeeper provides a researcher with a list of potential participants (Goduscheit & Knudsen, 2015). I emailed invitations to all potential participants. Based on the invitation responses received, I e-mailed all respondents who voluntarily agreed to participate in the study to schedule interview dates and times. I ensured all participants completed and signed the consent form before the interview.

To ensure I adhered to the IRB requirements, I checked and confirmed that all interviewees signed the consent form and received all relevant documentation regarding the research study. The IRB process required adherence to all requirements, including writing the research proposal, obtaining signed consent forms, applying the Belmont principles of beneficence, and maintaining oversight over the research (Kawar, Pugh, & Scruth, 2016). I adhered to all the IRB requirements. The consent form helped participants understand the reason for the study and be comfortable with my assurance that I would respect and protect their privacy during the interview process and the study's entirety. Researchers have a responsibility to protect participants' privacy by following national ethical standards as prescribed by their respective IRBs and, as a result, build a cordial relationship with the participant (Barkhordari-Sharifabad, Ashktorab, & Atashzadeh-Shoorideh, 2018). Researchers must ensure the informed consent form discussing protecting participants' confidentiality and anonymity as an effort to build trust with the participant (Leyva-Moral & Feijoo-Cid, 2017). According to Leyva-Moral and Feijoo-Cid (2017), the *Belmont Report* supports researchers' need to explain that they will limit access to their research participants' data and not share participants' information with anyone. I followed the process of requiring participants to sign the consent form before interviewing the participants and assured all participants that the dissemination of their data would be limited to my research.

The participants' voluntary commitment to participate in the research study enabled me to schedule the participants' interviews. I began by informing the participants to contact me if they had questions about the study or felt uncomfortable. Also, I sent second reminders to the participants who had not completed the appropriate consent documentation and asked them to agree to participate in the interview. The reminder e-mail to the participants included some information regarding the study's background and importance, the anonymity of the interview, and the study's potential benefits to the community. Participants were able to communicate their questions or express their concerns about the interview process through e-mail or fax until the day before the research interview. Turcotte-Tremblay and Mc Sween-Cadieux (2018) noted that researchers must develop strategies to build respect and trust for privacy between researchers and participants. I provided participants with a synopsis of the interview before interviewing them and maintained frequent contact with the participants to ensure their current contact information. Researchers should provide participants a synopsis of the interview to inform them of the possible questions before the start of the interview and to build rapport so that the participants will be comfortable (Mcinnis & Rodriguez, 2016). I provided the participants with opportunities to withdraw from the interview if they felt uncomfortable or vulnerable, and I assured them that only a summary of their interview with no identifiable personal information would make its way into the research study.

The participants opening up during the interview process was vital to the success of the research. As a result, I kept in touch with the participants by updating them on the research status and providing the interview details, including the expected duration and information about their anonymity. My assurances to participants that I would protect their privacy and the fact that I provided them with the interview questions helped the participants feel comfortable and enabled them to provide quality answers to the interview questions.

Research Method and Design

The process of selecting the research method was exhaustive and deliberate. Researchers generally use one of the three most common research methods: qualitative, quantitative, or mixed methods (Taguchi, 2018). I reviewed the three research methodologies and selected the qualitative research method, as it allows exploring an interpretative phenomenon in its natural setting to obtain in-depth knowledge of the phenomenon. I chose a qualitative method and a multiple case study design to explore in an in-depth manner the security strategies employed by IT administrators to prevent data breaches resulting from the integration of IoT devices in their educational institutions. Qualitative research provides researchers with opportunities to allow participants to articulate their ideas (Wadams & Park, 2018). Case studies represent an in-depth investigation and analysis of a collective case, with the intent to understand the philosophy behind the problem within a specific location and time (Cronin, 2014). The qualitative research method was most suitable for this study because it could explore in-depth the strategies that identify organizational, security, and technical deficiencies that a questionnaire or short survey could not identify.

Method

I answered the primary research question by performing an in-depth investigation and analysis of IT administrators’ security strategies during the IoT integration in their educational institutions. Qualitative research involves using rigorous data collection mechanisms, including interviewing and observation (Moerman, 2017). I used a qualitative research method to investigate the experiences of each participant. In qualitative research, researchers emphasize exploring, understanding, and contextualizing participants’ perspectives (Park & Park, 2016). The selection of a qualitative research method allowed me to ask open-ended questions and append follow-up questions, including engaging the participants using open-ended questions that generated data that enhanced and enriched the findings. Researchers who have a genuine and deep interest in the phenomenon can use interview questions to extract the meaning of participants' experiences (Moerman, 2017). I also respectfully asked follow-up questions when a participant’s response to a question required further probing. Asking follow-up questions required me to respect the fact that the participants were sharing their lived experiences with me. I expressed genuine interest in what the participants were sharing with me, even if I did not share the participants' views. Researchers interview participants and ask follow-up questions to gain insight into their experiences (Stahlke, 2018). I used inductive reasoning to investigate participants’ experiences regarding the reliability, security, and privacy of integrating IoT devices in educational institutions.

I considered a quantitative research method. Quantitative research is suitable for studies where there is a need to test hypotheses, examine variables for a causal relationship, and conduct statistical analysis (Rutberg & Bouikidis, 2018). According to Park and Park (2016), quantitative research methods' objectives are forecasting and controlling social phenomena. My research study involved exploring reliability, security, and privacy concerns in the participants’ IoT devices in an in-depth manner in their natural setting. Conversely, quantitative research focuses on static objective data and empirical data (Boeren, 2018). Researchers use quantitative methods to assess conceptual models to establish connections between variables and treatments while, at the same time, quantifying the thoughts of participants using statistical analysis (Christenson & Gutierrez, 2016). I did not use statistical numerical data to explore the strategies used to integrate IoT devices in educational institutions. The quantitative method was not suitable because I did not plan to examine the relationship between variables, and there was no need for inferential statistical analysis.

I also considered the use of mixed methods. A mixed-method study includes both quantitative and qualitative data collection methods, and researchers employ elements of both approaches to provide a more comprehensive understanding of the research study (Palinkas, 2014). Mixed-method studies involve using a quantitative research approach to emphasize objective measurement and qualitative research to explore a phenomenon in its natural settings in the same study (Thiele, Pope, Singleton, & Stanistreet, 2018).

Researchers use mixed methods to capitalize on the quantitative method's benefits, including the presentation of data in an objective form and the qualitative method, which is subjective (Newman & Houchins, 2018). The mixed-methods approach was not suitable for this research because it is time-consuming, and the statistical analysis ascribed to quantitative methods would not add value to the research. According to Stahl, Lampi, and King (2019), mixed methods combine quantitative and qualitative methods to provide researchers with the interpretation of numerical values and explore individuals' lived experiences, respectively. The focus of this research was the lived experiences of the participants. Therefore, the qualitative research method was most suitable because it offered an in-depth exploration of the strategies required to enhance the security, reliability, and privacy of integrating IoT devices in educational institutions.

Research Design

The design selected for this qualitative research study was a multiple case study. Case studies represent an in-depth investigation and analysis of a collective case, with the intent to understand the philosophy behind the problem within a specific location and time (Cronin, 2014). A case study was the most suitable design as I conducted an in-depth investigation of the security, reliability, and privacy strategies used by IT administrators to prevent data breaches resulting from the integration of IoT devices in their educational institutions in the Midwest. Ntemana and Olatokun (2012) described a case study as exploring a time and space-bound phenomenon to explain a problem's complexity. A way to extract information from each participant in the case study regarding the reliability, stability and privacy of IoT devices was to interview each participant. This multiple case study involved exploring in-depth the strategies used by IT administrators to integrate IoT devices into the education institutions' ecosystem.

The case study involved asking questions that solicited explanatory answers from the participants to understand them and their surroundings. Case studies represent an in-depth investigation and analysis of a collective case, with the intent to understand the philosophy behind the problem within a specific location and time (Cronin, 2014). Conducting interviews and supporting the answers with documents provides verification and confirmation of the participants' answers (Suharta & Suarjan, 2018). Supporting the interviews with documentation increased corroboration and knowledge gathered to explore the experiences and strategies used to integrate IoT in educational institutions. According to Dintoe (2018), interviews are the most common methods of gathering and validating qualitative research data. I selected a case study design because it would enable me to thoroughly gather and analyze data to support the strategies used by IT administrators to integrate IoT devices while ensuring the reliability, privacy, and security of the educational institutions’ IoT infrastructure. The multiple case studies included interviews and document analysis to examine in depth the strategies used by IT administrators at multiple educational institutions to integrate IoT devices into their IoT infrastructure.

I considered a phenomenological research design. Researchers employ phenomenological designs when they seek to examine a population’s lived experiences (Eatough & Shaw, 2017). According to Thompson (2019), the phenomenological design involves the rudimentary meaning, background, and cultural beliefs of several or one individuals ’ lived experiences of a phenomenon. Even though the participants’ experiences might have been useful to my study, a phenomenological study would not have enabled me to gather pertinent documentation to corroborate the interviews conducted with the participants on the institution’s perspective on interview questions. Researchers use a phenomenological design to uncover the essence of participants’ lived experiences through approaches such as in-depth semi-structured interviews, focus groups, and artifact collection (Flynn & Korcuska, 2018). I focused on the strategies used by IT administrators to integrate IoT devices into educational institutions’ infrastructure and did not explore the participants' individual lived experiences. The phenomenological study would not have addressed the privacy, security, and reliability strategies used to integrate IoT devices in multiple educational institutions. Thus, a phenomenological study was not suitable for this study.

I also considered an ethnographic research design. The ethnographic design seeks to understand participants’ daily activities by cutting through complex structures using rapport building and in-depth interviews (Brooks & Alam, 2015). The use of ethnographic interviews and participants' observation enables researchers to gain insight into a phenomenon's inner workings (Tomko, Linsey, Nagel, & Alemán, 2017). I used the participants’ interviews to gather data for my research, but observation to understand their daily lives was unnecessary. Researchers conduct ethnographic studies to evaluate the cultural characteristics by mingling with the population better to understand their behavior (Dunne, 2016). An ethnographic study is an approach that researchers can use to observe and understand a phenomenon's culture (Greig, Renaud, & Flowerday, 2015).

Understanding the culture of the phenomenon was not part of this study, and the focus of asking the research question was not to explore the cultural phenomenon of a group of people; thus, ethnography was not a suitable option.

A narrative study is the other design that I considered for this study. Researchers can conduct a narrative study to collect stories and analyze artifacts about an individual's lived and told experiences (Levitt et al., 2017). Although individuals' experiences contributed to this study, collecting stories and analyzing artifacts were not the focus of this study. Narrative inquiry allows people to shape their daily lives using stories of their interactions with others and to interpret them (Clandinin, Cave, & Berendonk, 2017). I used stories about individuals, but stories were not necessary to explore educational institutions' strategies to integrate the IoT. Thompson Long and Hall (2018) posited that researchers who select a narrative inquiry design use storytelling as the foundation and as the primary method to engage and form unions about others around them. I focused on the strategies used by IT administrators to integrate IoT devices in educational institutions and not on the formation of unions and identity, so the narrative study would not have enhanced the data collection to support my research question. A narrative study was, therefore not appropriate. After considering all potential designs, I opted for a case study as the most suitable design for this study, and I was able to answer my research question comprehensively.

During the study, I relied on data from multiple sources to achieve data saturation. To achieve data saturation, researchers must rely on open-ended surveys' sample size (Tran, Porcher, Tran, & Ravaud, 2017). Data become saturated when they stop providing meaningful information to a research study (Constantinou, Georgiou, & Perdikogianni, 2017). One way to achieve data saturation is to triangulate quality and in-depth data from multiple sources that enhance the findings' reliability and validity (Ness & Fusch, 2015). For this research study, I used multiple case studies as the research design and collected data from various IT administrators from numerous educational institutions in the Midwest region of the United States using open-ended semi-structured interviews. I conducted interviews with the participants until the data generated no longer added value to the research findings. I supplemented the semi-structured interviews with the institutions' documents to support educational institutions' reliability, privacy, and security strategies. While interviewing and gathering data from multiple sources to achieve triangulation, I noted the stage at which data saturation occurred. The point at which new information produces no change to the research findings can be classified as data saturation (Tran, Porcher, Falissard, & Ravaud, 2016). I stopped collecting data when I reached data saturation.

Population and Sampling

One of the initial steps in research sampling is the process of defining the population. The research population is the entire selected group of people in a research study (Haegele & Hodge, 2015). This study's targeted population was IT leaders of 11 educational institutions in the Midwest region of the United States, who had developed strategies to integrate IoT devices securely and reliably. The IT administrator interviewed at each educational institution met the qualifications of being a CIO or an IT director who had developed strategies that had been successfully used to integrate IoT devices in their institutions. I selected institutions that had recently integrated IoT devices in their network infrastructure. According to Wirtz et al. (2016), researchers purposively choose a targeted group population representing a set of characteristics that meet the criteria to participate in the research. I selected my population based on the members' expertise on IoT devices' reliability, security, and privacy during their integration into an educational institution's ecosystem. The population's composition, IT administrators who had experience integrating the IoT in educational institutions' network infrastructure with security, reliability, and privacy in mind, aligned with the overarching research question.

I prescribed a set of criteria that the sample population needed to meet to qualify to participate in the research study. Setting up criteria helps ensure participants can provide sufficient and reliable data before data saturation is achieved and ensure that the research budget is not overstretched (Wang et al., 2018). Researchers can determine the most suitable sample size by thinking of the population that needs to be studied (Krause, 2016). Participants' position, level of knowledge, and profession make it imperative for researchers to develop standards to achieve consistency (Derrick, Eliseo-Arras, Hanny, Britton, & Haddad, 2017). I selected participants using purposive criterion sampling. To be eligible to participate, participants needed to meet the following criteria: (a) were willing to share experience, (b) worked for an educational institution participating in the study, (c) met the leadership requirements of a CIO or IT director, (d) had experience integrating IoT devices in school infrastructure, and (e) were at least 18 years old. A sample of 11 IT leaders with decision-making capabilities from public educational institutions participated in this study. I defined the eligibility criteria to determine the sample. Therefore, the sample consisted of participants who understood the successful deployment of IoT devices in educational institutions.

In this study, I used purposive criterion sampling. The concept of selecting participants with relevant characteristics, such as those experienced and knowledgeable in the field of study, is purposive criterion sampling (Byrne, 2015). McCarthy et al. (2018) used the purposive criterion to find participants for a study on the role of using qualitative research in an emergency. According to Arnold (2016), purposive sampling, coupled with participant stratification, allowed him to interview enough participants to attain data saturation during a study on strategies to reduce high turnover among information technology professionals. Ames, Glenton, and Lewin (2019) used purposive sampling in a qualitative research study to perform a thorough analysis. I used purposive sampling to choose participants from institutions that met the criteria and had integrated IoT devices in their network infrastructure.

The use of sample size enables a researcher to determine the desired level of the population value the researcher needed to interview for the research study (Anderson, Kelley, & Maxwell, 2017). Either CIOs or IT directors of participating institutions who met the eligibility criteria of integrating the IoT in their educational institutions qualified to become part of the research study's sample. An appropriate sample size ensures the validity of a research study (Aburahma & Mohamed, 2017). According to Vasileiou, Barnett, Thorpe, and Young (2018), a qualitative research study typically reaches data saturation with at least 12 interviews; therefore, data collection must continue until there is nothing more to discover. This multiple case study had a sample of 11 IT leaders from 11 public K–12 educational institutions in the Midwest region of the United States, who had successfully integrated IoT in their educational institutions. Sampling conducted based on the selection criteria were participants' knowledge and experience in IoT integration, while non-completion of the consent form and questionnaire served as the disqualifying criterion. A sample size must be sufficiently large to explain the findings of the phenomenon under study; therefore, the more knowledgeable and experienced the participants are, the smaller the sample size needed to reach data saturation (Malterud, Siersma, & Gusaturationassora, 2016). This research study included 11 IT leaders in educational institutions. I performed member checking after interviewing and transcribing the interview data. I kept an eye on the data saturation level during the participants' interviews to ensure that the data being collected was not a repetition of previous interview responses. I was the primary instrument throughout the data collection process, and I selected the participants who qualified for the study and sought their permission to participate in interviews. For the overarching research question to be answered, I interviewed all participants using open-ended semi-structured questions until I reached the saturation point.

I interviewed the participants in their natural setting, and the interview locations were safe and convenient. According to Moerman (2017), researchers choose interview locations based on their natural settings and convenience, and the participants and the researcher's safety. To avoid disrupting the daily duties of the participants, I allowed the participants to decide on the location of the interview. Still, I recommended a closed office space or area with Internet and devices with web conferencing capabilities. I informed the participants that the interview had to be a semi-structured face-to-face interview regardless of the location. I turned on the recording equipment before starting the interviews. The interviews took place behind closed doors and were one-to-one. I thanked the participants after the interviews and turned off the recording equipment.

Ethical Research

Walden University's IRB stipulates that researchers must receive permission before embarking on research. One of the requirements of a research study is that the researcher must ensure participants' privacy and confidentiality, and the attainment of this assurance can be through informed consent (Zahle, 2017). I applied to the IRB for permission to contact potential participants, and upon approval, I e-mailed participants and asked them to consent voluntarily to participate in the research interview. All participants voluntarily completed the consent form as prescribed by Walden University's IRB. The consent form had a checkbox that all participants checked to acknowledge that they understood and voluntarily agreed to participate. To meet the Walden University research protocol and IRB ethical research requirements, I explained to potential participants the purpose, procedures, risks, benefits, and voluntary nature of the research study. I explained the benefits and associated risks, compensation, and confidentiality of the study to the participant to know the research's situation. Participants were aware that their participation was voluntary and that they could withdraw from the research study at any time before the interview date. Participants received the consent form through e-mail.

I informed the participants of the research study through e-mail to have documented proof of our communication. According to Allen and Foulkes (2011), an examination of 30 research studies revealed common themes such as (a) reason for collecting the samples, (b) details of consent request, (c) methods of sharing data, (d) ways the participant can withdraw, (e) risks, (f) possibility of recontacting, and (g) plans to protect the privacy of participants. Providing a full explanation of the participants' consent form ensured they knew their rights and the research study’s benefits.

Participation in the research was voluntary. Kılınç and Fırat (2017) defined research voluntariness as the choice or action performed by individuals who are not coerced, influenced, or subjected to external pressure. According to Kılınç and Fırat, interviewees provide fewer misleading answers when they voluntarily agree to participate in research studies. The consent form had provisions that stipulated that participation in the research study was voluntary, and individuals could withdraw from the study before the interview should they not feel comfortable or willing to continue to participate. The interview participants were aware of the inability to withdraw from the research study after the interview since their identities were masked at that point, and it would be difficult to exclude their portion of the interview.

I ensured the protection of participants and institutions by masking their identities. Participant protection is essential during data collection; therefore, masking participants’ identities is critical to their privacy, security, and confidentiality (Teixeira da Silva, 2017). I used pseudonyms to represent participants’ identity to avoid divulging the names of individuals who shared information on their experiences. The participants’ names were shielded from unauthorized access and, therefore, are not included in the final research study. In all, I interviewed 11 IT leaders in educational institutions.

The data collected will remain stored in an encrypted and password-protected file in the cloud for at least five years to ensure access to the data is controlled and secured from unauthorized access. The Walden University IRB approval number is 02-27-20-0632354. I informed participants that the interview invitation link would become inactive after the interview, and they would not be able to access the link after the interview date. The stored encrypted data will be safely destroyed when the 5-year period for safe storage elapses.

Researchers sometimes offer incentives to participants for participating in a research study. Using incentives in research can potentially influence responses (Crane & Broome, 2017), and providing participants with financial incentives may have unintended consequences as the researcher has to decide whether it falls within ethical guidelines (Zutlevics, 2016). I did not offer incentives to participants because I did not want the participant's responses to be influenced by financial or other incentives. I also wanted participants to withdraw from the study freely and not feel obliged to continue due to the incentive.

Data Collection

Instrument

Data collection is one of the main catalysts toward completing a research study. I was the principal data collection instrument for this qualitative research study. Researchers need to focus and act as critical interpretative thinkers when they are the primary data collection instrument (Kevin & Vealé, 2018). According to Wiseman, Rossmann, and Harris (2019), researchers use data collection techniques to gather and accurately measure variables of a phenomenon during a research study. During the semi-structured interviews, I used open-ended questions to extract data from the participants to address the research question and understand their experiences using the interview protocol provided in Appendix A. A researcher's responsibility is to ensure that a study's findings reflect the participants' experiences and thoughts, not the researcher's ideas and values (Constantinou et al., 2017). Researchers are responsible for gathering and analyzing rich data to arrive at interesting and informative findings (Moser & Korstjens, 2018). As the primary data collection instrument, I gathered, organized, and analyzed the data to answer the overarching research question.

I used a semi-structured interview as the primary data collection technique and relied on a review of institutional documents as my secondary data collection technique. Researchers use in-depth interviews, literature studies, and reviews of organizations' documents as data collection techniques (Sinaga, 2018). Researchers also use secondary data collection techniques to confirm the participants' information during the interviews (Pliakas et al., 2017). To confirm the validity and accuracy of the interviews with the participants, I used member checking to ensure the interview data was accurately transcribed. Through member checking, researchers try to confirm that their transcribed interview responses can be confirmed as accurate by the participants (Naidu & Prose, 2018). As part of the member-checking process, I invited the participants to scrutinize my interview interpretation. Member checking involved conducting either a follow-up telephone interview or a WebEx meeting with the participants to verify the interpreted interview data. The participants reviewed and confirmed my interpretation of their interview, not the raw data, to provide the research's external validity. Researchers traditionally use member checking to confirm the interview transcripts' internal and external validity (Brear, 2019). I allowed participants to perform member checking individually to enhance the accuracy and transferability of the findings.

Though researchers must trust the data from interviews with participants, it is imperative to collect secondary data as evidence to support the participants' assertions without distorting the responses to the interviews (Dierickx et al., 2019). Collecting secondary data enabled me to validate the interview data gathered from the participants. I used data from more than one source to achieve data triangulation during the research study. In addition to using the interviews as the primary data collection tool, I also used the institution's documents to buttress the interviews' information to solidify the findings and attain triangulation.

I gathered and used the educational institutions' documents as part of the data collected through the participants. Researchers commonly use various types of data, including minutes of meetings, strategic documents, and archived and secondary data to augment the data gathered from participants (Oteng-Ababio, Sarfo, & Owusu-Sekyere, 2015). I used innovative, strategic, proprietary, and archived documents from the educational institutions to supplement the data gathered during interviews. Researchers can simultaneously collect existing institutions' records with interviews during the data collection process (Rimando et al., 2015). The institutions' documents on devices, Internet bandwidth, security policies, responsible-use policies, network infrastructure, board minutes, and student populations enabled further exploration of the security, reliability, and privacy involved in integrating the IoT into the institution's infrastructure. Researchers' use of internal secondary data to augment the data collected during interviews and the member-checking process has increased (Ellram & Tate, 2016). Using the institution's records and other internal documents, I established trends and strategies used by IT leaders to integrate IoT devices into the infrastructure ecosystem.

Data Collection Techniques

Researchers use data collection techniques to measure variables to ensure accurate data collection, and it is vital to select the right data collection technique to match the characteristics of the data (Wiseman et al., 2019). Collecting accurate data has become one of the researchers' primary functions (Fuchs, Haldimann, Vuckovac, & Ilic, 2018). Researchers have used observation, interviews with open-ended questions, questionnaires, and document reviews as data collection techniques to achieve triangulation (Fuchs et al., 2018). Ways to elicit information from participants include open-ended interview questions, as they enable researchers to ask follow-up questions (Mekonnen, Ambaw, & Neri, 2018). The primary data collection technique I used to gain information into the participants' experiences on the security, reliability, and privacy of integrating IoT devices in their educational institution was a face-to-face semi-structured web interview using the interview protocol provided as Appendix B. In the face-to-face semi-structured interviews, I asked a list of prepared questions, and the questions elicited open responses on the participants' experiences. I was also able to ask follow-up questions when I found that the responses required further inquiry. Face-to-face semi-structured interviews contribute to a qualitative research study's trustworthiness and objectivity and enhance the study (Kallio, Pietilä, Johnson, & Kangasniemi, 2016). During the interview, I used open-ended questions based on the interview protocol (see Appendix C) to explore the participants' experiences. I asked follow-up questions to enhance the trustworthiness and objectivity of the findings of the research study.

I went through a checklist of the interview rules of engagement with each participant, including an audiotape recording the interview, taking notes, and interpreting the responses. I explained to each participant that note-taking, interpretation, and audiotape recording of the interview were part of the data collection process. All ethical issues were taken into consideration, including the participants' privacy and confidentiality. I provided each participant with a pseudonym before starting the recording of the interviews. I made sure that I asked each question as clearly as possible so the participants would understand my question, as this enabled me to gather quality and accurate data from the participants.

The interviews included nine short open-ended questions, starting with a broad starter question (see Appendix C). To make the interview process comfortable for the participants, each participant decided the location for the interview. Before the interview, I ensured that I established relationships with the participants through dialogue and communication to feel comfortable sharing their experiences with me. I used the participants' experiences to determine their participation in the interviews. I began the interviews by introducing myself and expressing my appreciation to the participant for agreeing to participate in an interview for the research study. I discussed the essence of the research and the consent documents they signed, as prescribed in the interview protocol in Appendix B. With the participants’ permission, I recorded the interview, and I also took notes, as recommended by Strickland, Pirret, and Takerei (2019), in case the recording equipment failed. I provided the participants with an opportunity to withdraw from the interview if they felt uncomfortable, in line with the guidelines for protecting participants. I was diligent with the participants to ensure I could explore the participants’ experiences in integrating IoT devices in their educational institution. I reminded participants that they would be able to contact me after the interview, and, if at any time before I published the findings of this study, they wished to alter or add relevant materials, they were free to do, as this would be fulfilling the member-checking requirements. At the end of the interview, I informed the participant that the interview was over, thanked the participant, and turned off the audio recording device.

Accurately transcribing and interpreting the information from participants was essential to the validity and reliability of the study’s findings, so I endeavored to transcribe the interviews as soon as the interviews were over so that I could accurately and diligently capture the information gathered from the participants. To ensure the participants’ privacy and confidentiality, I removed the participants' pertinent personal information during the transcription process by using unique identifiers to denote their identities. Audio taping the interviews of participants has a threefold benefit: (a) participants have the opportunity to review the tapes for accurate interpretation, (b) save storage of interview tapes for future review, and (c) future review of tapes for the integrity of interview interpretation (Evangelinou-Yiannakis, 2017). I interpreted the recordings using best practices and followed up with additional questions when I found ambiguity in a participant’s responses.

I used member checking to augment the validity and reliability of the responses from the participants. Iivari (2018) concluded that the member-checking technique allows participants to check the facts of, comment on, and approve the researcher’s interpretation before submitting a research study's findings. Before member checking, I reviewed and interpreted all interview recordings and categorized them into reoccurring ideas and subjects. Researchers conduct member checking to explore the credibility of the responses provided by the participants of a research study by reconfirming the accuracy and resonance of their experiences as portrayed in their responses and interpreted by the researcher (Birt, Scott, Cavers, Campbell, & Walter, 2016). I worked with the participants to review the interpretation of their responses to ensure the accuracy of the interviews. This process also enabled participants to add or subtract information from the interpreted interview or provide additional documents to corroborate their responses. I repeated the member-checking process until participants did not have any more information discovered, and then I moved on to analyze the data.

I used the institutions’ documents, which included policies, procedures, and practices, to support information provided by participants to ensure the findings of my research were not deficient or inaccurate, and they accurately reflected the reliability, security, and privacy strategies used in the organizations during the integration of the IoT. Researchers use an organization’s documents to acquire knowledge and information on an organization’s practices and policies during and after research projects (Curran, Kekewich, & Foreman, 2019). According to Siegner, Hagerman, and Kozak (2018), documents are sourced to support other forms of data collection, such as interviews, to corroborate themes and perspectives generated to attain triangulation during a study. Research participants should be allowed to freely review an organization’s documents and other secondary data sources to enable them to refresh their memory (Chu & Ke, 2017). I ensured the documents provided and reviewed were legally obtained and reflected each institution’s policies and practices.

Data Organization Techniques

Data organization was an essential aspect of this study, as I needed to analyze the data efficiently and interpret the interviews into accurate quality findings. Researchers need to develop strategies to enhance stored data's speed and retrieval efficiency (Guo, Huang, Guan, Xie, & Wu, 2017). The process of organizing research data involved note-taking, abstracting, indexing, and classification of the data gathered (Given & Olson, 2003). Williams and Moser (2019) noted that the data organization must be repeatable, robust, precise, and analyzable for research findings not to be skewed. According to Lai, Zhang, Tong, Li, and Ding (2018), researchers use data organization techniques to improve the data storage and retrieval process while maintaining the data's security and accuracy and a well-organized coding system. I used NVivo 12 and Microsoft Excel to organize my data, including the consent forms, tape recordings, and participant list. The data were encrypted and stored on Microsoft OneDrive for security and easy access. Storing the data in the cloud provided secure and quick access. I generated the forms and transcribed the interviews from the participants using Microsoft Word and stored the documents on Microsoft OneDrive. I created separate folders and subfolders for member-checking data, audio recordings, e-mails, consent forms, and artifacts.

To ensure the confidentiality of the participants, I used pseudonyms to mask their identities. Institutions use masking to preserve participants' anonymity, which is an essential characteristic of using a consent form (Journot et al., 2013). I masked the identities of the participants, as indicated in Appendix B. Masking participants' identities ensure their anonymity and prevent them from being identified in the findings of a research study (Allen & Wiles, 2016). I masked participants' identities with pseudonyms and carefully tagged them in an encrypted Microsoft Excel spreadsheet to mix up their responses. The study's findings contain only the participants' pseudonyms, so their real names are not revealed. I will delete all supporting documents collected and stored in Microsoft OneDrive after five years of approval by the chief academic officer of Walden University.

Data Analysis Technique

During this study, I used data management techniques to analyze the participants' information until the overarching research question of reliability, security, and privacy implication of integrating the IoT into education was reasonably answered. Su, Ding, Lue, Lai, and Su (2017) used the concept of big data analysis to explore the interaction, unknown correlation, and hidden patterns of the phenomenon. Researchers use data analysis techniques to align research characteristics to the research population's needs and abilities (Wiseman et al., 2019). Researchers also use advanced data analysis techniques to extract and interpret data gathered to improve knowledge discovery (Paiano & Pasanisi, 2018). I extracted the data to identify themes and interpreted the data to provide knowledge on IoT integration's reliability, security, and privacy. Using big data analysis techniques, researchers can amass a large amount of data representing successful and failed cases in parallel to provide an understanding of the phenomenon (Paiano & Pasanisi, 2018). I used methodological data triangulation to derive quality findings for this study.

The purpose of this qualitative multiple case study was to explore the security strategies that IT administrators had used to secure the integration of IoT devices in educational institutions, with the focus of the overarching question being the security strategies that IT administrators use to prevent data breaches resulting from the integration of IoT devices in their educational institutions. Yin (2014) indicated that qualitative researchers perform methodological triangulation by gathering and analyzing data from sources such as interviews, institution documents, and observations. I pursued methodological triangulation by using institutions’ documents, making observations, conducting interviews, and audiotape recording interviews to review responses during the analysis. Researchers mask participants to protect them from the research (Allen & Wiles, 2016). I provided all 11 participants with pseudonyms to protect their identities from the outside world.

As part of the data analysis process, I transcribed the interview data from the participants into Microsoft Word and Excel applications. The researcher must be choosy in the kind of data they select and transcribe, as they need to consider what materials to include and exclude while keeping the research question in mind (Meredith, 2016). Azevedo et al. (2017) explained that Microsoft Word is the most used technology when transcribing participants' interviews in a research study. In a qualitative research study, interviews can be transcribed verbatim using computer-assisted data analysis applications such as NVivo coding and other data applications (Spearman, Norwood, & Waller, 2016). During this research, the interviews were transcribed and analyzed, and the documents gathered were analyzed using Microsoft Word and Excel. I used NVivo to help with sorting, arranging, and theme identification using log entries.

As part of the study, I looked for and analyzed themes that emerged during the examination of multiple data. I analyzed the Microsoft Excel and NVivo generated themes for patterns that answered the overarching research question. I also considered and analyzed the emerging themes alongside the DOI theory and the study's conceptual framework. During the analysis of the gathered data, I focused on examining emerging themes while identifying key themes to correlate the major themes with the overarching research question and the literature (including new studies published since writing the proposal) and DOI conceptual framework. I also recategorized the data into major themes until I could associate the emerging themes with DOI characteristics.

I used member checking to validate the accuracy, credibility, and quality of the participants' responses to the interview. Researchers use member checking as a tool to enhance the trustworthiness and validity of qualitative research findings (Birt et al., 2016). I considered ethical norms as part of member checking when communicating the research study results. Communicating findings requires considering ethical norms if researchers want the findings of their research studies to be valid before dissemination (Naidu & Prose, 2018). To validate the accuracy of the research, I provided participants with the opportunity to review their responses. As part of the member-checking process, researchers seek to validify their findings by providing respondents with some or all their responses (Varpio, Ajjawi, Monrouxe, O'Brien, & Rees, 2017). I performed member checking by letting the participants review their respective interview transcripts to confirm their interview responses.

Reliability and Validity

I developed reliability and validity strategies during the study to ensure the findings were grounded in the phenomenon's lived experiences. Researchers use reliability to establish the stability and consistency of testing methods. In contrast, researchers use validity to ensure the individual results are meaningful and can be trusted to help make decisions (Spearman et al., 2016). Reliability is critical to ensuring a phenomenon's precision and consistency (Dai, Chi, Lu, Wang, & Zhao, 2018). Reliability serves as a confirmation of an instrument's stability and consistency under consideration (Mohamad, Sulaiman, Sern, & Salleh, 2015). Reliability helps establish the credibility of qualitative research findings while removing bias simultaneously (MacPhail, Khoza, Abler, & Ranganathan, 2016). I used various validation checks, including interview protocols and member checking, to address validity concerns during this research study.

Validity refers to the extent to which the integrity of the methods used to ensure the findings' accuracy reflects the data, whereas reliability refers to the consistency of the analytical procedures (Noble & Smith, 2015). Mohamad et al. (2015) noted that reliability and validity are complex, as validity enables researchers to make conclusions using meaningful individual scores, and reliability depends on the test method for stability and consistency in the results. I developed strategies to ensure the reliability and validity of the findings of this study.

The study's validity hinged on the trustworthiness, credibility, authenticity, plausibility, rigor, transferability, and dependability of the results. One method to ensure the validity of a study’s findings is triangulation, enhancing credibility, transferability, and legitimacy (Moon, 2019). According to Leung (2015), validity refers to a tool’s appropriateness, methodology, process, and data to arrive at the research results. Researchers experience challenges establishing validity when conducting a qualitative research study, as numerous data points constitute validity, including trustworthiness, credibility, dependability, confirmability, authenticity, rigor, and transferability of the material (FitzPatrick, 2019). I used existing methodologies to address the underlying factors that reinforce reliability and validity in the research study.

Dependability

Dependability is the process of ensuring the consistency and quality of a research study (Yeong et al., 2018). To ensure this study’s research finding's dependability, I kept consistent documentation of the interviews, analysis, and interview data processing using an interview protocol (see Appendix B). Researchers use member checking to obtain data saturation and develop a consistent audit trail (Arnold, 2016; Moser & Korstjens, 2017). To ensure the quality of my finding, I used member checking to confirm the accuracy, integrity, and stability of the collected and interpreted interview data. To ensure the research study's dependability, I used member checking and the interview protocol, as stated in Appendix B, to confirm the participants' responses during the interview. Using member checking validates the responses from the participants to ensure accurate and high-quality data. I used the interview protocol as an instrument to provide consistency during the interviews. Ellis (2018) described dependability as the stability of data over time and in several conditions. Allowing participants to review the interview transcript before I finalized the study helped ensure the accuracy and consistency of the research study findings.

Researchers use pilot testing to determine the feasibility of the data collection method, as this enables the researchers to refine the data collection process before conducting the actual data collection process for the study (Evon, Golin, Ruffin, & Fried, 2017). Although pilot testing the data collection method could have enhanced my data collection process, I did not perform a pilot test after IRB approval because I interviewed a maximum of one participant at each educational institution using the interview questions in Appendix C.

Researchers use audit trails to confirm the authenticity and accuracy of stored data (Helfgott, 2010). I maintained an audit trail of documents, notes, interview recordings, and procedures. NVivo is one of the most widely used qualitative research tools that researchers use to continuously compare and analyze data to identify emerging themes and relationships (Min, Anderson, & Chen, 2017). NVivo helped accelerate the search for themes and patterns during the data analysis phase. I used NVivo to ensure the dependability of the study.

Credibility

To ensure credibility during this research study, I ensured transparency and applied triangulation in the data collection process. Credibility serves to confirm that the research findings reflect the responses extracted from the participants (Moser & Korstjens, 2017). To ensure confidence in the research findings, I used member checking. Casey and Murphy (2009) described credibility as the truth of the research finding. I demonstrated full engagement with and observed the participants and used proper audit trails to ensure the research study’s credibility. Researchers use multiple sources of data as a basis for the trustworthiness of the findings of a study (Stewart, Gapp, & Harwood, 2017). I interviewed as many participants as possible to achieve triangulation and to provide depth, rigor, and authenticity in the research study.

Transferability

During this study, I developed criteria to ensure a rigorous inquiry and evaluation of transferable research materials. Transferability refers to the possibility of applying the findings of a research study to other individuals or groups by generalizing the findings (FitzPatrick, 2019). Researchers use rigor, responsiveness, and purposive sampling to ensure the research findings' transferability (Stewart et al., 2017). I used purposive sampling to choose participants from institutions that met the criteria and that had integrated IoT devices in their network infrastructure. Researchers use external validity to provide interested parties opportunities to transpose research findings to another context (Morse, 2015). I created a detailed description of the research finding to make it easier for individuals, groups, or IT policymakers to apply the findings to other research or contexts.

After gathering the data from all research participants, I attained data saturation. Researchers rely on the principle of data saturation to determine the sample size of the research study (Tran et al., 2017). I achieved data saturation after interviewing 11 CIOs or IT directors during this study. According to Vasileiou et al. (2018), the point at which new data and analysis do not impact the study's findings due to the repetition of themes can be classified as data saturation. I used triangulated data from multiple sources to achieve data saturation during the data collection phase.

Confirmability

I maintained a trail of the data gathering processes and data interpretation to ensure the research study's confirmability. Confirmability is the process of determining whether the analysis and findings of a research study were fair (Haven & Van Grootel, 2019). I used NVivo to ensure the interpretations of data were accurate and reflected the base data gathered. According to Ellis (2018), researchers use confirmability to maintain a trail of the data collection process and the methods used to interpret the data gathered. I preserved the interview recordings, notes, original quotes, and other pertinent data gathered during the interviews with the participants to ensure the same data can reproduce the same findings. Confirmability requires that the research study's findings are neutral and pass the repeatability test (Connelly, 2016). I used the confirmability concept to demonstrate that the findings directly responded from the interviews with the participants and that my personal biases did not influence the results.

Transition and Summary

Section 2 of this study included the purpose statement; my role as the researcher; and a description of the participants, the research method and design, the population and sampling, reliability and validity, the data collection instrument, and the techniques used to analyze data on the integration of IoT devices. During this qualitative multiple case study, I explored the strategies used by IT administrators during the integration of IoT devices in their educational institutions in the Midwest region of the United States. Data gathering took place through interviews with participants and the review of pertinent documents from the educational institutions involved in the research to understand the strategies developed by IT managers to ensure the secure and reliable integration of IoT in educational institutions. Section 3 includes a discussion on applying the professional research practice, recommendations, implications for social change, reflections, and conclusions derived from the research study.

Section 3: Application to Professional Practice and Implication for Change

Overview of Study

The purpose of this qualitative multiple case study was to explore the security strategies that IT leaders had used to secure the integration of IoT devices in educational institutions. I collected data from semi-structured interviews I conducted online with IT leaders from 11 public K–12 educational institutions in the Midwest region of the United States. One participant represented each institution, and each participant was considered one case study. I performed member checking with all 11 participants to confirm the transcription of each interview. The IT leaders who participated in the interviews were decision-makers of their educational institutions and were responsible for securely and reliably integrating IoT devices in their educational institutions. The DOI theory served as the study's conceptual framework to explore strategies that IT leaders had used to securely and reliably integrate IoT in their educational institutions.

The methods used to collect data from the participants included semi-structured recorded interviews that were conducted online. I asked follow-up questions to the participants to obtain further clarification on the interview questions. I asked the participants if it was possible to provide company data related to the secured deployment of the IoT in their educational institutions. The collection and analysis of supporting company documents provided data triangulation to support the information gathered during the interview. The documents collected included minutes of meetings, device procurement invoices, receipts, and institutional policy documents. The interviews were transcribed using Sonix and were coded and analyzed using NVivo. Coding and classifying enabled me to deduce themes from the responses from participants easily. Three major themes emerged after the analysis of the data: (a) organizational breach prevention, (b) infrastructure management—external to IT, and (c) policy management—internal to IT. The themes that emerged from the participants' responses aligned with the characteristics of DOI, which was the conceptual framework of the study (see Table 1). As this study's findings demonstrate, the participating IT leaders were actively developing and refining strategies to prevent breaches to their IoT devices and network infrastructure.

Table 1

Number of Participant and Document References to Each Emergent Theme

	Participants		Documents	
Context	Count	Reference	Count	Reference
Organizational breach prevention	11	191	11	28
Updating and upgrading security systems	11	54	2	6
Training of users	8	32	4	12
IoT device and data security	11	56	3	1
Authentication to network	10	49	2	4
Infrastructure management—external to IT	11	286	21	7
Security technology support—collaboration with partners	10	59	3	4
Security of the IoT and infrastructure systems	11	87	4	12
IoT device types and their security	11	52	9	6
Breach prevention and network hardware	11	88	5	8
Policy management—internal to IT	11	208	23	9
IoT deployment policy	10	67	7	9
Policies to eliminate vulnerabilities	11	57	6	6
Security of user accounts and IoT devices	9	33	5	10
Vendors and stakeholders’ role in breach prevention	10	51	5	10

Presentation of Findings

This study's overarching research question was as follows: What security strategies do IT leaders use to prevent data breaches resulting from the integration of IoT devices in their educational institutions? I used semi-structured online interviews to gather data from the participants. The participants comprised 11 IT leaders from public K–12 educational institutions in the Midwest region of the United States. I was able to collect documents from the participants to support their responses during the interview. I used NVivo 12 to codify and categorize the data gathered. The themes of the study emerged after analyzing the classified data in NVivo 12. The participants' identities were masked in the findings using pseudonyms such as Prt 1 for Participant 1 of Educational Institution 1, Prt 2 for Participant 2 of Educational Institution 2, and Prt 11 for Participant 11 of Educational Institution 11. During data analysis, I used DOI theory's characteristics as the conceptual framework to guide and support the themes that emerged. Three main themes and 12 subthemes emerged from the interview questions and documents (see Table 1). I further researched the themes mentioned by the participants that were not covered in Section 1 to identify their correlation to current themes.

The overarching primary themes that emerged during my interviews with IT leaders were organizational breach prevention, infrastructure management—external to IT, and policy management—internal to IT. I based the themes on my analysis of the responses to the interview questions. I used methodical triangulation to examine and analyze the data generated from the interviews and member checking to validate the transcribed interviews. The study's findings depict the reliability, security, and privacy strategies deployed by IT leaders of public K–12 educational institutions during the integration of IoT devices, and they align well with the influence of DOI theory on the introduction of innovation in most institutions. Based on the analysis, I deduced that the participating IT leaders had strategies to ensure the security, reliability, and privacy of IoT devices and data to prevent breaches to the IoT infrastructure of their educational institutions. In the next section, I further explain the three themes and 12 subthemes. The themes and subthemes illustrate detailed strategies used by the IT leaders to prevent breaches during the integration of IoT devices in their educational institutions.

Theme 1: Organizational Breach Prevention

The first theme that surfaced from the data gathered was organizational breach prevention. Enacting policies and procedures to prevent IoT vulnerabilities was one of the main strategies of the IT leaders who participated in the study. The responses analyzed indicated that the IT leaders made concerted efforts to avert breaches of IoT devices and servers by preventing unauthorized access to students’ data and the network infrastructure. The small size of IoT devices' memory and storage space makes them vulnerable and susceptible to attack (Li et al., 2016). Due to the speed of manufacturing and delivery to the market, the weak security features in IoT devices make them a prime target for hackers to exploit. The study's IT leaders acknowledged this vulnerability, and they explained steps they took to thwart these vulnerabilities. The participants' rigorous efforts to institute measures to prevent breaches in their institution aligned with the research question, which concerned the security strategies that IT leaders use to prevent data breaches resulting from the integration of IoT devices in their educational institutions. The responses to the interview questions by the IT leaders indicated that they all had varying degrees of security of IoT devices in mind, and they had different methods of implementing the security policies within their various organizations. Prts 2, 4, and 8 indicated that they would not purchase and introduce IoT devices into their educational institutions if the product had known vulnerabilities and the vendor did not have a security patch mechanism. The responses of all 11 participants led to identifying the first theme: organizational breach prevention (see Table 2).

Table 2

Theme 1: Organizational Breach Prevention

	Participants		Documents	
Major theme and subthemes	Count	References	Count	References
Organizational breach prevention	11	191	11	28
Updating and upgrading security systems	11	54	2	6
Training of users	8	32	4	12
IoT device and data security	11	56	3	1
Authentication to network	10	49	2	4

Ensuring the security, reliability, and privacy of the IoT devices in the participants' educational institutions was a major part of the institutions’ infrastructural strategy, which was obvious in the responses provided during the interview process. Prts 2 and 11 mentioned that they do all they can to ensure the students’ data are safeguarded by mandating all users to sign onto IoT devices with usernames and passwords. According to Prts 2 and 11, using assigned credentials to access IoT devices and networks provides added layers of security and reliability to an institution's data and network. Prt 2 mentioned that to ensure the security, reliability, and privacy of IoT devices, he used “at least 802.1x authentication on user credentials, of course, but at the same time, if it is a device that’s not ours, then the user still has to authenticate to the network with active directory credentials.” All the participants felt good about the levels of security and privacy of their data because they had a couple of authenticating levels in their educational institution. Prt 10 noted,

> We always consider student safety and privacy first and foremost, which is why I told you we do not approve the use of Google Home or Amazon Echo Dot, or any other smart speakers, so we follow the security principle of least privilege.

Prt 10 further explained that limiting the number of unsecured devices in an institution's network infrastructure potentially reduces the institution's security attack surface. IT leaders already have a lot to deal with, and adding unsecured IoT devices into the mix makes them defend a broader spectrum of IoT devices alongside their applications. To increase the reliability, security, and privacy of IoT devices and data, Prt 3 stated, “We use role-based access to minimize security risks and minimize permissions to those who are needing to have those only.” According to Prt 3, this occurs more frequently when vendors do not patch the devices and applications before trading them to the educational institution. References made in the institution’s acceptable-use policies and internal IT procedure documents on authenticating to IoT devices are shown in the responses in Table 2 under “authentication to network” and “IoT device and data security.” The acceptable-use policies mentioned users' role in ensuring the institutions’ network infrastructure and data security. As stipulated in the acceptable-use policies, not sharing usernames and passwords was a step toward preventing an organizational breach, as users were required to keep their passwords confidential.

The IT leaders explained that organizational breach prevention can align with numerous studies in the literature, where IT leaders and researchers had issues with the lack of expertise in preventing breaches in educational institutions. Nicolas-Rocca and Burkhard (2019) discussed the importance of protecting user accounts' privacy and the knowledge transferred during cybersecurity education, and they concluded that transferring the right knowledge to users affects the security of user credentials. The protection of users’ privacy enhances stored data security against attacks (Delgado, Llorente, & Naro, 2017). The IT leaders reiterated the need to secure user credentials to prevent access to students’ data. According to Smith (2017), data security is threatened not only by attackers but also by users and administrators who erroneously capture and store personally identifiable data sets in the wrong storage area shared by members of the institution who do not need to view those data. The IT leaders interviewed mentioned that they do not allow users to access data on the network if they do not have the right credentials. Sebescen and Vitak (2017) evaluated the role of humans in security breaches in an organization and concluded that weak credentials could lead to phishing attacks due to weak passwords on users’ personal devices and company-provided laptops. To prevent breaches from an organization’s devices and network, IT leaders need to promulgate policies and procedures to stipulate users’ access level to the organization’s data.

The basis of this study's conceptual framework was the characteristics of DOI theory, and the responses to the interview questions by the IT leaders reflected the security, reliability, and privacy strategies deployed by the IT leaders during the integration of IoT devices in their educational institutions. The DOI theory explains the adoption of innovation in various industries (Sundstrom, 2016). As the IoT is a new technological phenomenon, the DOI theory is best suited to clarify why IT administrators in various sectors, including educational institutions, adopt and integrate new technologies into their network infrastructure. The IT leaders interviewed provided responses that could be used to collaborate the five characteristics of the DOI theory by examining social structures and determining communication practices, innovative ideas, and time constraints during the integration of IoT devices. The participants' responses shed light on some of the steps they have taken to secure the innovative technologies they have introduced in their educational institutions. Creating policies and procedures to prevent breaches to the institutions' IoT devices and network infrastructure was one of the steps to ensure the security and reliability of the IoT devices.

Subtheme 1: Updating and upgrading security systems. One of the subthemes of organizational breach prevention that emerged was ensuring all security systems are updated and upgraded regularly. Updating and upgrading IoT security systems can prevent breaches of an institution’s network and data infrastructure, like loopholes, backdoors, and other points of failure in the IoT devices will be protected by the updates. In January 2018, a barrage of cyberattacks and data breaches occurred on IoT devices in numerous industries (Amanullah et al., 2020). IoT devices are susceptible to vulnerability attacks, and educational institutions have not been exempted from unauthorized access to their infrastructure and data. The IT leaders who participated in the research interviews provided insight into their engagement level with security, reliability, privacy, and regulatory requirements to the IoT and, in particular, their educational institutions. In their responses to the interview questions, all the participants overwhelmingly stressed the importance of keeping the IoT systems and network up-to-date and, in other cases, upgrading the systems to avoid security breaches. Five participants mentioned that they regularly ensure their devices, applications, and operating systems are up to date. They updated the systems using intermediary devices or deployed updates directly from vendors' sites to the IoT devices and infrastructure in their environment. Prt 8 stated,

> So, we have to rely on our vendor partners to sell us products that are stable and are not going to be prone to cyber-attacks. So, we try to do what they asked us to do to keep things up-to-date and use them in the right way.

Prt 11 responded, "We are big proponents of updates when it comes to the operating system and things like that. We have a systems administrator who is on top of those patch notes or release notes looking for those critical vulnerabilities." Prt 4 contended that to gain the stakeholders' trust, IT administrators must prove that they can secure the IoT devices and, at the same time, ensure the privacy of their data. Securing IoT technology involves providing endpoint devices and vetting all IoT devices before purchasing them. All the participants acknowledged having performed various updates to their IoT devices to ensure they were protected from vulnerabilities.

Upgrading and updating security systems are vital roles in securing IoT devices in educational institutions' network infrastructure. Using interconnected personal objects containing personal information and connected to the Internet raises serious data security and privacy threats, and therefore ensuring that the devices are patched will prevent hackers from gaining access to the data on the devices (Huang, Wang, & Yang, 2018). The participants answered the research question regarding the prevention of breaches during the IoT integration in educational institutions. Upgrading and updating security systems can protect the IoT devices enrolled in an educational institution's network infrastructure. Patching the IoT systems and devices will ensure the IoT devices' reliability, security, and privacy. The integration of IoT devices presents numerous security challenges to IT leaders due to the multiple points of failure in the technology, and updating the operating systems to prevent security breaches was one of the participants' steps, as expressed in the interview. The focus of the research question in this study was the security strategies that IT leaders use when integrating the IoT in their educational institutions, and the participants presented adequate steps, including patching the applications that run on the network and scanning, monitoring, and upgrading systems to prevent breaches to institutions’ IoT network. Hardening the IoT systems is achieved through password complexity enforcement, authentication mechanisms, and patch updates. Prt 8 indicated that, as part of updating and upgrading security systems, they changed all default passwords to ensure attackers could not guess the passwords to essential IoT security hardware and their related applications. According to the participants, all these measures were geared toward ensuring IoT devices' security and reliability. Prt 5 indicated that he tried to connect with his industry peers to ensure his systems were secured so that users could focus on productivity without security interruptions. The complexity of IoT devices makes it imperative to streamline access-control mechanisms so that some users were not prevented from, and other users were not allowed to, access critical data, which could prove to be counterproductive or detrimental, respectively, to the financial or security viability of educational institutions. The documents used by the participants to support the updating and patching of the security systems to prevent organizational breaches included acceptable-use policies, security contracts, and internal security procedures. These documents specified when updates needed to be performed and the department that would perform the updates. The security contracts indicated when new devices and network gears need to be purchased and when the software that runs on them needs updating.

The participants' security strategies aligned with most studies described in the literature review in which the security, reliability, and privacy of IoT devices were a significant area of concern to IoT users. For example, Jose and Vijyalakshmi (2018) discussed that security is a significant threat to any network application and IoT devices and that confidentiality, integrity, and availability were of significant concern to IoT data security. According to Cangea (2019), IoT technology has been evolving, and certainly, there are benefits associated with IoT technology, but if IT leaders do not address the hazard of data theft and loss, users will lose faith in the innovative technology. The participants stated that they took steps to protect the IoT devices and the systems by ensuring the IoT systems are modernized, updated with the latest antivirus software and patches, and best practices.

The responses by all the participants aligned with the DOI theory. The five characteristics of DOI theory propose that the innovation being introduced and integrated considers the external factors and security surrounding the technology being introduced (Liao, Huang, & Hsieh, 2016). According to Liao et al. (2016), security and complexity reasons impeded the integration and adoption of Internet banking in rural South Africa. The DOI theory directly impacts the security, privacy, and reliability of IoT devices and infrastructure. As a result, it can relate to the security and reliability issues affecting the strategies needed to integrate the IoT into educational institutions successfully. The participants mentioned various steps to ensure the devices' security and privacy enrolled in their IoT environment. Some of the participants performed security penetration testing to monitor and identify security vulnerabilities on their network. Others frequently updated their systems with the latest patches and antivirus software. Some attended conferences and read white papers to learn about trending security loopholes. All the participants' responses can help secure IoT devices in educational institutions and support the assertions in the DOI theory, which promotes the introduction of innovation by various establishments.

Subtheme 2: Training of users. The second subtheme that emerged during the analysis was the level of training and education provided to users of the IoT devices. According to eight participants, training stakeholders, who include staff, teachers, students, parents, and IT leaders, to identify vulnerabilities that could lead to breaches is critical to protecting the IoT devices of the educational institutions. Nogwina, Gumbo, and Ngqulu (2019) explained that training and security awareness campaigns ranging from cybersecurity and IoT provide users with the skills to avoid security threats and breaches. The provision of security awareness training to network administrators to patch those devices was an essential part of their strategies. All the participants mentioned that they tried to create awareness of the need for security during their staff meetings and other methods such as professional development. Prts 1, 2, 3, 7, 8, 9, 10, and 11 provided various answers related to the provision of training and awareness creation that indicated they relied on vendors to provide documents relating to the security of their devices, as that was the basis for training their users and other stakeholders. These vendor-provided documents were sources of training for the IT leadership and their teams, as they, in turn, passed this knowledge to their users during professional development and internal seminars, according to Prt 5. Prt 8 stated, "We do training every year, and we also do training throughout the year to make sure that our users can spot threats and report them to us and not get tricked into any of the cyber threats." Seven other interview respondents echoed these comments. Prt 1 noted that they allowed their users to attend conferences to improve their understanding of current security technologies that could be used to prevent attacks on their IoT devices. Prts 8 and 11 stated that because users were the weakest link in most network chains, they ensured users were provided with professional development and hands-on training to confirm that users have the practical ability to thwart breaches. Prt 11 had a perspective on protecting students and their devices by ensuring federal and state regulations and legislation were followed. Prt 11 mentioned that it could be a criminal offense if they allowed students' data to be attacked and stolen due to their negligence. Prts 2 and 3 noted they used phishing-attempt simulations to educate and train users on protecting IoT devices.

Several research findings from the literature review supported the first theme that emerged: adequate training is required if users are being requested to ensure the security, reliability, and privacy of IoT devices. According to Billingsley (2019), users can become a human firewall against the increase in cybersecurity breaches if given the proper training. The lack of awareness is a major contributory factor to security breaches in the health and education sectors, and having a trained community of users ensures they identify and prevent actions that could be harmful to the network and IoT devices (Billingsley, 2019). The creation of awareness and users' education are essential elements of protecting users and their devices against phishing and social engineering attacks. IT leaders must create policies geared toward training key stakeholders to protect their privacy and prevent security attacks (Kshetri, 2017). IT leaders can deploy systems, including content filters and antivirus software, to mitigate against breaches that could occur due to human errors and IoT systems malfunctioning. IT leaders need to make substantial budgetary investments in training for their users if they want their networks to be secured, reliable, and protected from unauthorized access. Security awareness training must be provided to users who click on any icon and do not look for links that have malicious content that could be dangerous to users' personal information and the institution's data (Carella, Kotsoev, & Truta, 2017). The literature reviewed in this study demonstrated that creating a security policy for an educational institution can promote a safe working environment for staff, and training the staff to understand and adhere to the policies will be an added impetus for risk reduction. The participants mentioned the need to train and educate users to identify and report security risks.

Several researchers have examined training for users during innovative technology integration and found it to align with the DOI theory (Ghafir, Prenosil, Alhejailan, & Hammoudeh, 2016). According to Pustokhina et al. (2020), if the concept is to replace old technology with new, then there must be a systematic and skillful approach to training users. During the interview, the participants provided examples of why it is critical to imbue users with the right level of training to ensure IoT devices' security and reliability. According to Dwomoh (2015), IT leaders can create an atmosphere in which employees are constantly learning during the migration to new innovative technology and allot funding to train employees and stakeholders (Sun, 2020). Prts 8, 9, 10, and 11 mentioned that the type and cost of training, and the availability of users to be trained, had been an issue in their schools. The provision of cybersecurity and user credential training for innovation has to be at the right time if the designated users are to benefit from the training, according to Prts 10 and 11. Prt 8 stressed that IT administrators need to acknowledge and admire the incremental progress by users of new technology anytime it occurs during training. The participants supported the need to train tier users to prevent security breaches with device acceptable-use policies, internal memos, training instructions, IoT device enrollment, and user manuals. These documents guided users on how to log onto the network and what they can do while on the network. The IoT device enrollment specified the type of devices that can be enrolled in the IoT environment and who can perform it.

Education and training of users align well with the DOI theory because it provides a clear communication channel to secure IoT devices connected to an educational institution’s infrastructure, and that will protect the data of users. One of the five characteristics of the DOI theory is providing clear communication channels during the introduction of innovative technologies (Rogers, 1995). The training and education of users could potentially prevent security breaches during the integration of IoT because educated staff would be careful when using their IoT devices (Liang, Hatcher, Liao, Gao, & Yu, 2019). Most participants contended that an enlightened set of users would keep the systems and IoT devices protected to prevent unauthorized access to students’ data and the institution’s network infrastructure. The participants reiterated that a network could not be secured if the users are not aware of the vulnerabilities in the IoT devices, which are part of the educational institution's enterprise network.

I applied the characteristics of DOI to the interview responses provided by the participants. The participants enumerated as part of their IoT device infrastructure were all emerging technologies and can be classified as innovative technology, as described by Rogers (2015). Some of the participants noted that the IoT could introduce many security loopholes, and as a result, training and educating users to identify the vulnerabilities is an excellent way to prevent breaches. Alignment between the DOI theory and the participants' responses existed in communicating the innovative technology to the users. Prts 10 and 11 reiterated the need for users to be informed of the security loopholes and backdoors that exist in the IoT technologies, and IT leaders can align this to the promotion and communication of innovation among members of a social system by using the appropriate channels within a specific period.

Subtheme 3: IoT device and data security. IoT devices and their associated data security was the other subtheme that emerged from the interviews. The heterogeneous nature of the devices deployed in IoT technology makes them susceptible to attack, and identifying and patching the loopholes ensures the protection of the institutions from being breached by bad actors. Therefore, to prevent organizational data breaches, the IoT devices and data need to be safeguarded from internal and external attacks by installing and configuring the right hardware and software. All 11 participants mentioned the importance of securing the data and devices that are part of their IoT infrastructure. Prt 7 said, “We scan the network both internally and externally, to see if we find any vulnerabilities within.” Prt 11 stated, “I have to deal with ensuring that we secure student information and that we were providing the rightmost stable platform.” According to Prt 10,

> We always consider student safety and privacy first and foremost, which is why I told you we do not approve the use of Google Home or Amazon Echo Dot or any other smart speakers, so we follow the security principle of least privilege.

Most of the participants described the importance of the safety and privacy of students’ data and devices in their IoT infrastructure. For instance, Prt 2 noted the importance of securing students’ devices with 802.1x authentication and user credential protocols to prevent unauthorized access to students’ data. Prt 9 said the IT leaders of his institution automatically encrypt the data on their network traffic to avoid man-in-the-middle attacks. The participants provided invoices for IoT devices, board minutes, and training documents to support users' training to prevent IoT device breaches in their organizations. The aforementioned documents were used to provide user awareness, device security, and the network's protection from being attacked. The information in the invoice showed that the IoT devices purchased had the needed security specification and, as a result, could be configured to prevent breaches.

The concept of securing IoT devices and data has been of interest to researchers. Chaturvedi, Matheus, Nguyen, and Kolbe (2019) described IoT devices as complex distributed systems involving multiple stakeholders, applications sensors, heterogeneous data, and various personal use devices. The IT leaders who participated in an interview secured students' devices and data to prevent breaches as a strategy to ensure the reliability, security, and privacy of data and devices enrolled in the IoT infrastructure. IoT devices were developed without the necessary consideration as they have rapidly evolved from personal household devices to integrated Internet-connected technology with numerous security flaws (Andrea et al., 2016). Most of the participants adopted the security strategies to upgrade and update their systems aligned with numerous studies where successfully patching IoT devices prevented breaches of those devices. The lack of security and privacy of the IoT devices and data infrastructure made up of sensors and other wireless devices may cause a major threat due to the possible unauthorized disclosure of sensitive data to untrustworthy entities(Chaturvedi et al., 2019). The responses from the participants included strategies that answered the research question of this study, in that the IT leaders worked closely with vendors to provide security updates to the devices and applications, changed the default passwords of all newly purchased devices, and trained their users on how to identify possible vulnerabilities. According to

King and Awad (2016), IoT devices now encompass embedded systems, RFID, and sensors to collect and transmit data, and this capability has opened the technology to security vulnerabilities. The answers that the participants provided illustrated the potential existence of security strategies to prevent data breaches resulting from the integration of the IoT in their educational institutions because they developed policies and procedures on how to prevent breaches, patching devices based on recommendations from the vendors, and collaborating with partners and vendors. The volume of devices involved in collecting data from the Internet and the autonomous nature of data transfer from IoT devices to servers make the devices and data susceptible to attack (Kolomvatsos, 2019). A strong correlation existed between the research question and the IT leaders' responses, as both showed an interest in exploring the security strategies used by IT leaders to prevent breaches resulting from the integration of the IoT in their educational institutions.

The subtheme of IoT devices and data security aligned well to the DOI theory of innovative ideas or practices, clear communication channels, the element of enough time, a social system, and the security strategies adopted by the IT leaders of educational institutions interviewed. The participants' responses aligned well with the DOI theory because they had the security of IoT devices as the primary underpinning of their strategy. The alignment of the DOI characteristics and the participants' responses can promote the security, privacy, and reliability of IoT devices in their institutions, as access to students’ data and the network infrastructure is granted to authorized persons only. The introduction of innovation was stipulated as one of the main characteristics of the

DOI theory, and the protection of IoT devices and data security by the participants was in line with the proponents of the DOI theory. The security, reliability, and privacy of IoT devices are dependent on how effectively the participants can protect the devices and data from being breached.

Subtheme 4: Authentication to network. Authenticating to the institution's network was another of the subthemes frequently mentioned during the interviews with educational institutions' IT leaders. The users' accounts and passwords used to log onto the IoT devices and the network directly correlate to the institutions' network infrastructure's security. The lack of safeguards to the network authentication mechanism could lead to a breach of the institutions' IoT infrastructure. Ensuring users properly authenticate to the network could help prevent breaches by hackers. All the participants had some authentication policies geared toward preventing their IoT devices' breaches and students' data. The automatic authentication of IoT devices to the Internet and other Bluetooth devices with keyboard capabilities is a source of security worry to IT security experts (Kim & Lee, 2017). Prts 1, 2, 3, 4, 6, 7, 8, 9, 10, and 11 mentioned the need to authenticate to the network if users' IoT devices are protected from intrusion and vulnerabilities. Prts 8, 9, and 10 stressed the need to change default passwords anytime a new device is enrolled in the IoT network. According to Prts 8 and 10, the failure to remove and replace the factory password may result in the device being compromised and exposed to attacks. Prts 2, 3, 6, 8, 9, 10, and 11 noted that all their students had usernames and passwords used to access IoT devices and secure their data. In the interview with Prt 10, he mentioned that IT leaders perform penetration testing to ascertain whether some devices still had their default passwords, especially the HVAC devices that have embedded IoT chips. Prts 2 and 11 explained in the interviews that their institutions used authentication to determine the level of access and rights that students have on the network, and that policy helps ensure the security and privacy of IoT devices and students' data.

Authenticating the devices to the network can provide data and device security that will prevent breaches from occurring. The participants provided board minutes, internal memos, training, and instructional manuals that showed how users should safely authenticate to the institution's network infrastructure to prevent breaches. The participants' documents included IoT wireless network utilization documents, responsible-use documents, and user training manuals. The responsible-use document contained the username and password conventions, and all users are required to adhere to the stipulations in the documents. According to information in the responsible-use policy, users' passwords must meet password complexity standards, which is relevant to the security of the institutions' network infrastructure. The finding on the secure authentication of the IoT devices to the educational institution's network, aligned with the literature on authenticating securely to IoT networks. The development of IoT technology has changed the authentication methods used by institutions, but the inefficiencies in the sensors with low memory and low power have brought about some vulnerabilities that untrusted individuals or entities have taken advantage of (Kang, Han, Qian, & Du, 2020). Access to devices and data has been one of the banes of integrating innovative technology into a social setting, and IoT devices are no exception, as the ability to integrate microelectromechanical systems could negatively impact the expansion of the IoT (Martins et al., 2018).

Most of the participants mentioned that they used usernames and passwords to grant access to IoT devices, data, and their institutions' network infrastructure. The process of using secured user credentials to provide access to IoT devices, including HVAC and smart devices, offers insight into the strategies used by IT leaders to prevent data breaches during the integration of IoT devices in their educational institutions. Prt 11 indicated that the data traversing the network infrastructure were encrypted and encapsulated to prevent unauthorized access to the students' and facultys’ confidential data. Data encryption ensures IoT devices can protect data while they are at rest or in motion (Nikoukar et al., 2018). Prt 9 indicated that the institution’s data is automatically encrypted to prevent breaches. Some participants also mentioned that they always segment IoT devices with fewer security capabilities to prevent security breaches. Prt 10 indicated that they had segmented off their HVAC equipment from the remaining network to prevent issues related to hacking, viruses, and systems damages. According to Mao, Zhu, and Liu (2020), the protection of confidentiality and authenticity of IoT systems, device authentication, and pairing are essential components of integrating IoT in institutions. The participants' actions and existing literature aligned with the research question as IT leaders develop strategies to avoid data breaches during innovation integration.

The responses from the participants supported the tenets of the DOI theory. Two of the DOI theory characteristics are innovation and communication, and those align with the participants’ responses in the research interview regarding authenticating IoT devices to the network infrastructure of the educational institutions. All the participants mentioned that they communicate new innovative technology with their users either through training or conferences. The DOI theory requires the existence of innovative ideas or practices, clear communication channels that enhance the proposed innovation, the element of enough time, and a social system that includes the existence of formal and informal hierarchical positions and individual relationships (Rogers, 1995). All the participants stressed the importance of introducing innovative technology into their educational ecosystem to enhance productivity and security. The DOI theory aligned well with the educational environment, as both included innovations, communication, time, and social system structures. The participants' responses showed that they had to authenticate the IoT devices with usernames and passwords to access the data and network segment assigned to them. The use of various authenticating mechanisms ensures the security, reliability, and privacy of the IoT devices, which is aligned with the conceptual framework of this study. Therefore, the DOI theory is a suitable strategy to use during the integration of the IoT in educational institutions.

Theme 2: Infrastructure Management—External to IT

The second main theme derived from the interviews was managing the institutions’ infrastructure concerning external entities. The use of vendors in the management of the IoT inventory has been a long-standing practice, as manufacturers and vendors provide strategic design, systems replacement, and patching of the devices (Dasaklis & Casino, 2019). The four subthemes that emerged were (a) security technology support—collaboration with partners, (b) security of the IoT and infrastructural systems, (c) IoT device types and their security, and (d) breach prevention and network hardware (see Table 3). The participants noted that stakeholders and security vendors influenced the integration of a particular innovation and infrastructure. The educational institutions' IoT infrastructure housed the servers, network hardware and systems, IoT devices, and the Internet, and the users use the system to access and store their data. IoT devices' privacy and security are critical issues when integrating IoT into most institutions' network space (Sicari et al., 2017). The security and privacy of the data stored were essential to all the participants, as they mentioned during the interview that the level of access to students’ data was one of the primary considerations when designing the system. According to Prts 2, 5, 9, and 11, the vendors of network and IoT device apparatuses and applications played a significant role in designing and implementing a solution.

The participants stressed that their stakeholders also influenced the management and nature of their IoT infrastructure environment. Prt 1 indicated that their firewall and content filter, which were both used to protect students’ data from unwarranted Internet attackers, were managed by their vendors, and the IT leaders have to rely on the vendors to apply patches and updates for the devices. Using hardware to protect against attacks has been a strategy used by IT leaders to protect students’ data (Meneghello et al., 2019). The external vendors also ensured that network ports were not unnecessarily opened, opening the institution’s network infrastructure to attack. Prts 1, 10, and 11 asserted that their most significant issues have been with their HVAC systems, which had IoT components but were challenging to manage because the vendors do not know the vulnerability level in their products. Prt 10 mentioned that, as part of the infrastructure and security management at his educational institution, the IT administrators perform penetration tests every couple of years to weed out attackers who were exploiting vulnerabilities in their IoT infrastructure and devices. All the participants also mentioned that they engage outside security vendors to augment their local security resources to ensure they cover all aspects of their network and potentially cause them issues.

The literature review, which included a discussion on the integration of IoT devices in educational institutions and the methods used to prevent breaches, supported the security strategies described by the IT leaders of the educational institutions. The IoT is gaining ground in the educational sector, and it is opening opportunities for instructors to facilitate teaching and for students to consume the lessons being impacted (Suduc, Bizoi, & Gorghiu, 2018). Most of the participants described security as their primary challenge and as the reason why they devoted a large portion of their budgets toward the engagement of vendors and partners to help them secure their IoT devices and infrastructure. Chong, Xiong, and Proctor (2019) discussed providing security services by external entities as valuable professional services that optimize the setup and configuration of network gears to institutions, as they did not have the local expertise to perform those tasks. Prt 1 indicated that their Internet service provider's firewall configuration made them comfortable since the consultants knew what they were doing and owned the firewall and the Internetwork Operating System (IOS) that runs on the devices. According to Prt 1, the provision of antivirus software, patches, and updates by vendors is essential to the security, reliability, and privacy of IoT devices and educational institutions' infrastructure. Prts 6, 10, and 11 indicated some vulnerabilities in specific vendor-supported devices, including HVACs, Amazon Echo Dot, and sensors found in smart tablets, due to the lack of patches proprietary applications in them.

The DOI theory supports the security strategies that the educational institutions' IT leaders used to prevent security breaches. Tristani, Tomasone, Fraser-Thomas, and Bassett-gunter (2020) used the DOI theory to explain that the external factors of awareness and security are integral parts of influencing innovations. It was determined during Tristani et al.'s study that the DOI characteristic of trialability showed the extent to which teachers can test the innovation before it is integrated into the system, and compatibility provided a perceived consistency in resource usage. The experiences of teachers, coupled with security, were major impetuses for integrating and adopting IoT device technology (Tristani et al., 2020). The IT leaders demonstrated through the interviews that the strategies they deployed during the integration of IoT in their educational institutions closely mirrored the DOI theory's characteristics. Prts 8 and 9 revealed that they ensured the innovative technology introduced was compatible with the existing technology. The DOI theory has gained much interest because of the difficulty of getting new ideas adopted or integrated, though they may have advantages (Zhang, Qian, Lv, & Zhou, 2019). The standard security practices of resetting default passwords, providing the right access control, and creating virtual local area networks (VLANs) to house external parties' devices and applications were used by some of the participants during their integration IoT device innovations in their educational institutions. Though additional security structures were needed to harden the innovations, Prt 10 noted the basic security principle remained the same. Prt 1 mentioned that he used external vendors to leverage his IoT devices' security by tapping their expertise to ensure conformity to best security practices.

Table 3

Theme 2: Organizational Breach Prevention

	Participants		Documents	
Major theme and subthemes	Count	Reference	Count	Reference
Infrastructure management—external to IT	11	286	21	7
Security technology support—collaboration with partners	10	59	3	4
Security of the IoT and infrastructure systems	11	87	4	12
IoT device types and their security	11	52	9	6
Breach prevention and network hardware	11	88	5	8

Subtheme 1: Security technology support—collaboration with partners. The first subtheme that emerged under the infrastructure management—external to IT main theme was security technology support—collaboration with partners. The participants provided various instances when they had to collaborate with various partners to ensure the security of the technologies involved in providing IoT services to the students. Prts 1, 3, 5, 6, 7, 8, 9, and 10 indicated they had to rely on vendors to provide them with security support, a knowledge base, and security applications to support their IoT devices securely. Prts 1, 3, 4, 5, 6, 7, 8, 9, and 10 stressed the nature of their relationships with their security partners who provide security white papers and seminars on security and IoT integration best practices. Prts 1 and 10 stated that they are staunch readers of the HECClist, which is a digital document circulated by the Hosier Education Computer

Coordinators (HECC). The HECClist, according to Prts 1 and 10, provides information on security trends, current vulnerabilities, and industry trends to IT leaders in Indiana. Prts 3, 6, 7, and 8 said that they made use of the Consortium for School Networking (COSN) to stay current, maintain industry standards, and share ideas among like-minded peers. Prt 3 responded, “I have to depend on organizations to bring updates to me, so groups like COSN I think are incredibly important as well as honestly a lot of the networking that happens.” Prt 6 stated, “My best answer to your question is, we talk to NIST (National Institute of Standards and Technology) group and I also go to COSN for other resources and for help with questions I have regarding the security of our IoT devices.” Prts 1, 3, 4, 5, 6, 7, 8, and 9 indicated they use vendors in varying degrees to secure their network and provide critical services needed to prevent breaches. Some participants indicated that they collaborated with partners to gain insight into trending vulnerabilities in IoT devices, which enabled them to understand the attack surface. Prt 7 stated that he gathered IoT device security information from the State of Indiana through agencies such as COSN and the HECClist, as they share relevant IoT security vulnerabilities with public K–12 institutions in Indiana. Five participants provided supporting documents in contracts with security vendors, invoices, receipts for IoT devices, board minutes, and device user policies to confirm and support the security technology support by collaborating with vendors. The security contract provided information on the level of collaboration that exists between the institutions and the vendors. The board minutes provided insight into the various institutions’ boards' commitment to creating partnerships with the vendors.

There is limited research literature on the cooperation between security vendors and educational IT leaders. Smart campuses take advantage of IoT devices and cloud computers with the support of vendors who specialize in interconnected devices' security (Fernández-Caramés & Fraga-Lamas, 2019). One of the participants' consistent responses was the collaboration with partners to ensure users have the relevant tools to protect the innovation from intrusion. One of the challenges facing the integration of the IoT is the collaboration between institutions and innovative technologies in the transfer of knowledge to institutions implementing the innovative technology (Goduscheit & Knudsen, 2015). The protection of the innovative technology being integrated by organizations is critical to the security of the organization's data, and this corroborates the responses received from participants. Drubin (2016) found that IoT partners focus on end-to-end solutions based on their area of operations, and this operation enables collaboration among hardware and security software across multiple technologies. The provision of services by partnering organizations and vendors is mutually beneficial to the educational institutions, as the educational institution will have its data and IoT devices secured, and the partnering organization will earn contracts and revenue (Leiba et al., 2019). During the interviews, multiple participants indicated that partnering with vendors as part of their security strategies was essential when earning their stakeholders' trust.

The responses from the participants aligned with the DOI theory as posited by Rogers (1995). The DOI theory component of communicating using clear communication channels and social systems aligned with the participants' reactions, as the collaborating partners did communicate industry standards, current security, and vulnerabilities, therefore bringing together IT leaders to discuss security issues in the integration of IoT devices in educational institutions. One of the DOI theory components is the clear communication of ideas or practices, and the role of collaborating partners in the dissemination of security information to IT leaders falls in line with the characteristics of DOI theory (Ntemana & Olatokun, 2012). Communicating current vulnerabilities and ways to patch innovative technology aligns with the DOI theory. Prt 11 mentioned some strategic similarities between the current technology and the innovative IoT innovative technology being introduced. The statement by Prt 11 that IT leaders organize quarterly professional development and training sessions focused on the security of the innovative technology confirmed the correlation between the five characteristics of DOI and the innovation being integrated by the IT leaders.

Subtheme 2: Security of IoT and infrastructure system. The second subtheme that emerged under infrastructure management—external to IT was the security of IoT and infrastructure systems. One of the problems of IoT devices is the propensity to be attacked due to the miniature nature of the memory embedded in the devices (Ahanger & Aljumah, 2019). All participants mentioned various measures that they had put in place to ensure the security of IoT devices and their infrastructural systems. Prt 1 said that he ensured his antivirus software is up-to-date and applied to all the IoT devices and infrastructure. Prt 10 stated, “We have got the iPads and Chromebooks locked down pretty well using web filtering and what they can and cannot do on them to help secure that better.” Prt 10 again mentioned that he tried to maintain proper patch management of all their institutions' devices in his infrastructure, and this was corroborated by Prt 5, who said that not allowing the software license to expire was an excellent idea, as the devices that housed the installed applications could become vulnerable to attack. Prt 11 mentioned that all their institution’s IoT devices were filtered for vulnerabilities and always connected to managed networks.

According to Prt 11, ensuring the protection of his students’ information requires the IoT devices' security and providing a stable IoT infrastructure platform to prevent the violation of the Family Educational Rights and Privacy Act (FERPA). Prts 2 and 3 stated that they had segmented their network and provided a separate network for their IoT devices, including HVAC, smart lighting systems, and building automation. The use of preshared keys as passwords to authenticate to an organization's network ensures that unscrupulous individuals do not get access to the devices and the network infrastructure (Safa et al., 2015). Prt 4 stated that the most significant network intrusions on educational institutions were on the IoT devices' security, and he made an effort to educate his users and stakeholders on how to prevent breaches. Prt 5 noted that SSL decryption was one of the tools that the IT administrators used to secure the IoT devices and the network infrastructure. Prt 6 said, “It is just a matter of continued testing if issues arose and constantly looking at the resources that are out there to update security protocols.” Prt 7 indicated during the interview that “we make sure that the device can handle 802.1x authentication. If it cannot, then we have to look at whether we are willing to maintain that device on our network using another method of security.” He also mentioned that his institution scans the network both internally and externally for vulnerabilities. Prt 9 responded to the interview question by stating that he relied on vendors to fill his security space since they understood their technology better and can help the users stay informed. The participants provided numerous documents to support this subtheme, including security policies, IoT network utilization policies, board minutes, security contracts, and access-control documents. The participants' documents were designed to act as an incentive for users to apply best practices to promote the security of the educational institutions' IoT infrastructure systems. The IoT utilization policy document was a broad statement to the users informing them of the institutions' support for 802.1x authentication and preshared keys in each IoT device.

There is literature on IoT device infrastructure security that supports connecting IoT devices to the network and Internet of educational institutions. The responses from the participants confirmed the viability of the findings from the literature that was reviewed. According to Yang, Zhang, Chen, Zhuansun, and Liu (2020), modern IoT devices' security and privacy have become popular as sensor technology and wireless communication components have become conduits for accessing educational materials, health knowledge, and intelligent lifestyle data. Prts 10 and 2 signaled that the use of endpoints, HVAC, and other sensor-embedded IoT devices had become a significant part of their IoT infrastructure, and special efforts are paid to securing those devices. The independent resources in the IoT infrastructure and devices make it difficult to secure the actuators and WSNs vulnerable to attacks (Peng et al., 2020). The introduction and migration of user accounts and data to the cloud have added an extra layer of difficulty in securing the IoT infrastructure and systems that reside on them, as the physical threat to the cloud network has grown exponentially (Agarkhed, 2017). According to Sivanathan, Habibi Gharakheili, and Sivaraman (2020), cybersecurity has changed the dynamics of securing the IoT infrastructure and their devices to the extent that monitoring and performing traffic analysis are not enough to secure the networks. The use of IoT in institutions has created uncertainties in security because numerous vulnerabilities exist that threaten the continuous reliability, confidentiality, integrity, and availability of systems that users depend upon (Liang et al., 2019). Most of the participants stressed the importance of training users to secure the IoT devices and applications. Prt 8, for instance, mentioned that training was probably the most significant, high-impact, low-cost solution that his institution's IT administrators use to protect their network environment. Computer basic cybersecurity awareness and identification of vulnerabilities training have to be provided to students and teachers in educational institutions (Nogwina et al., 2019). The literature reviewed during the study supported the participants' responses on the security of IoT devices.

The DOI theory supports the communication of innovation using established channels in the organization. The study participants developed clear communication channels with their stakeholders by informing them of the innovation being introduced and the vulnerabilities associated with IoT device integration. IoT devices are being deployed and integrated into most educational institutions and have become the most common everyday devices connected to the Internet and used by students to learn (Kassab et al., 2018). Attacks on these devices have become rampant because cybersecurity and DDoS attackers have effectively used the known vulnerabilities in IoT devices to cause havoc to institutions that have integrated IoT devices in their network environment. Rahi and Ghani (2018) mentioned that innovativeness and perceived technology security were the most critical considerations of users who intended to integrate and adopt innovative technologies. The diffusion of innovative technology occurs through a series of communication channels by the end-users of an institution, who have intentions to integrate technology, which correlates to the responses by the participants of the research study (Hsu & Lin, 2018). According to Lamanna (2019), one of the methods used to integrate innovation is to first train staff on IoT devices' security before educating stakeholders on preventing breaches.

Subtheme 3: IoT device types and their security. IoT device types and their security were the third subtheme that emerged after analyzing the participants' interviews. The types of devices deployed in the IoT ecosystems of the participants interviewed have a considerable influence on the nature of the security systems and applications designed for the institutions, as they could be divided into resource-rich devices such as computers and resource-constrained devices such as embedded systems, RFIDs, and sensors (Li & Palanisamy, 2019). The multiplicity of IoT devices in the educational sector was the general consent among all the participants. Prts 1, 7, and 10 indicated that they deployed Chromebooks in their educational institutions. Prts 1, 2, 4, 5, 6, 7, 9, 10, and 11 explained during the interview that they have iPads in their educational institutions. According to the participants who had deployed iPads in their educational institutions, security updates to the devices were managed using Filewave and other media. The participants with Chromebooks deployed in their educational institutions, however, indicated that they use Google mobile device management (MDM) to push security updates and other applications to their Chromebooks. Prts 1, 6, 7, 8, 10, and 11 had HVACs installed in their educational institutions, and those were the devices that posed the biggest security threat to their IoT infrastructure. Prts 1, 2, 3, 4, 5, 7, 9, 10, and 11 had other IoT systems such as public address systems, security cameras, smart televisions, Amazon Echo Dot, Google Home, and smart doorbells, and these IoT devices created some challenges, so they had to place them on a separate VLAN or take steps to isolate them due to their vulnerabilities. The IT leaders interviewed provided device invoices, IoT device specifications, contracts for IoT devices, board minutes supporting the IoT device types being deployed in the institutions, and access control to the devices. The IoT invoices provided a list of the IoT devices purchased and showed the level of security that existed in those devices. The IoT device specifications also provided information on the year of manufacture of the devices and the version of the protocols that run on them.

Researchers have conducted and authored numerous studies to support the security of various types of IoT devices. The IoT has introduced many physical objects with sensors, actuators, and controllers connected to the Internet, but the exponential increase in the use of the IoT has increased vulnerabilities that have allowed hackers to infringe on the security and privacy of the device users (Siboni et al., 2019). The integration strategies mentioned by the IT leaders of the institutions aligned with the study, as IoT device users had to contend with multiple heterogeneous devices in their institutions. Ensuring that the IoT device types deployed in the network infrastructure are secured and protected from intrusion and other vulnerabilities is critical to the security of the institution’s data and network infrastructure (Samanta et al., 2018). According to Azad, Bag, Hao, and Shalaginov (2020), the management of IoT devices requires dual privacy preservation strategies to ensure the encrypted sensitive data cannot be traced to their file servers while at the same time ensuring access control does not prevent users from performing their job functions. The importance of ensuring sensitive data encryption was echoed by most participants, as they contended that determining the kind of access to provide the users of IoT devices in their institutions did open their data and critical infrastructure to security vulnerabilities. Leiba et al. (2019) mentioned that most IoT devices that are not correctly designed have weaknesses in the security of the hardware and applications embedded in IoT devices. The scalability and manageability of IoT devices have tremendous potential due to the range of devices enrolled in the technology; therefore, an access-control mechanism must be put in place to control users' privileges (Mahalle, Anggorojati, Prasad, & Prasad, 2012). The feedback from Prts 1, 2, 4, and 6 showed that these participants ensured users had the exact privileges needed to access the institution’s data while they continuously looked out for vulnerabilities and patched their systems before falling prey to cyber and other attacks. Most of the participants also mentioned that they had installed security firewalls in their institutions, and all users and devices were required to authenticate to the network before accessing data as a means to prevent intrusion by unauthorized users.

This study's conceptual framework clarified the IT leaders' position regarding the strategies used to integrate the numerous IT devices in their institutions. The five characteristics of DOI theory, coupled with security and awareness factors, influence IoT devices' integration in an organization (Ramavhona & Mokwena, 2018). All the participants indicated that they had IoT devices in their institutions and, as a result, took extra security and precautionary measures to harden the devices to prevent attacks to their data and essential infrastructure. Prts 1, 6, 7, 8, 10, and 11 stated that sensors embedded in HVAC and public address systems are the IoT devices that gave them the most problems, as those devices' management rests with the vendors. Rogers’s DOI encourages adopters and integrators to explore the concept of the trialability of their innovative technology, which will enable them to fine-tune the technology (Strömberg et al., 2016). Some participants stated that they try and test innovative technology before adopting and integrating. Uploading data from IoT devices to the cloud poses several challenges to the data of the institutions. IoT devices and sensors have limited computational power and must hop from one frequency to another, which creates encryption problems during their communication with the Internet (Sadeeq et al., 2018). The IoT devices described by the IT leaders who participated in an interview were depicted as having smaller memory, lower frequencies, and less storage space, making the reauthentication to networks very volatile.

Subtheme 4: Breach prevention and network hardware. The fourth subtheme that emerged under the infrastructure management-external to IT central theme was breach prevention and network hardware. All the participants noted the importance of hardening IoT infrastructure to prevent breaches and introducing software to manage access to the network hardware. Prts 1, 4, 5, 6, and 10 mentioned that they had firewalls, a virtual private network (VPNs), and antivirus software in their educational institutions to prevent their infrastructure's hardware breaches. Prt 1 stated that his institution used a firewall and content filter to control the data that traverses their network. Prt 10 mentioned that he had to segment their institution’s HVAC from the network to prevent breaches due to the vulnerabilities associated with HVACs. Prt 10 also took one more action, which he described in the answer he provided to the interview question: “We have done some penetration tests, and that is actually what made the HVAC jump up on our radar. So, we are taking steps to prevent issues, and then just with authentication, some of them may have default passwords.” When answering an interview question, Prt 3 stated, “So we do penetration tests with different companies from time to time because we know that IoT is a potential gateway for security vulnerabilities.”

As part of his breach prevention strategies, Prt 11 stated,

> For the most part, I think we adopt what I consider to be at least a standard security practice, which is the most restrictive first, and then you whittle away as you figure out identity and you figure out the purpose.

Prt 11 again described his systems administrator's role as someone who is on top of all patch and release notes and who performs all updates and upgrades to prevent security breaches. All participants mentioned that if they detect vulnerabilities and release a patch or update, they immediately perform the update so that any loophole or backdoor will be patched. Prt 2 said,

> There may have been some devices a couple of years ago that would not do WPA2 or some of those current authentications, but if it does not at least meet our standards, then we would not let it connect to our network.

Prt 2 again mentioned that he had endpoint protections on all their institution's devices, but the Apple devices were more resolute than the other IoT devices. To prevent unauthorized access to the hardware of the institution, Prt 9 stated that it was his policy not to provide vendors with VPN access. According to Prt 9, all vendors have to physically visit the site and access their HVAC, IoT security cameras, or any other sensors they have onsite. Prt 8 stated, “We try to use encryption as much as we can, and we use account security best practices with passwords and also only allow approved IoT devices on our network.” Prt 8 said, “We have good reliable backups that we can pull up if we need, and we test those.” All the participants mentioned that they have antivirus applications on their network and devices and always make sure the latest antivirus policy is applied. To prevent breaches, Prt 5 indicated that they test and retest their hardware, replace all default passwords or devices, and employ a security consultant's services to scan their network once a year. All the prior-mentioned responses were practices that the IT leaders applied to prevent breaches and unauthorized access to their network hardware.

The study demonstrated the role hardened security hardware plays in the security of IoT devices and the organization's network systems, which aligned with the participants' responses. IoT devices connect to the physical world and network using embedded sensors, processors, and actuators, causing security challenges and privacy concerns (Yuan, Lin, Alasad, & Taheri, 2017). Most of the study participants acknowledged the security and privacy challenges that exist in the IoT devices. They indicated that they took steps to alleviate the challenges by continuously updating and patching the IoT devices. Yuan et al. (2017) further contended that IoT devices could be used to attack other hardware that resides on the same network or external devices, as is the case with DDoS attacks. Prts 1, 4, 5, and 10 mentioned that they installed firewalls on their network to prevent breaches to their network and IoT devices due to the inherent security challenges in those devices. Prts 6, 8, and 9 stated that they would not even allow their vendors to remote into the systems without using VPN tunneling as a means to control access levels and prevent unauthorized access. The participants provided supporting documents such as IoT security device contracts, acceptable-use policies, institutional procedures on accessing their networks, and intrusion prevention documents to demonstrate the strategies to prevent breaches and secure the network hardware that operates in the infrastructure ecosystem of the institutions. IoT security device contracts provided information on the vendor's role in performing network and port-scanning servers every couple of years to identify and block vulnerabilities that exist on the IoT network of the institutions.

The findings of this subtheme aligned with numerous studies on preventing breaches in IoT hardware and systems. Many studies support the construct that there are security requirements for using applications to protect IoT devices from breaches, including antivirus software, DNS threat mitigation hardware and applications, penetration testing applications, and threat sensors (Iles et al., 2017). The images generated by IoT devices are at continuous risk of allowing access to security and privacy data, and, therefore, IT leaders need to protect their data by developing policies to prevent unlimited access by third parties and vendors (Khan & Byun, 2020). In a study on the IoT and machine-learning-hardware, Dong, Chen, Guo, and Zou (2019) stipulated that hardware security was one of the main issues affecting the security of the IoT in the modern era, and researchers have grappled with the security detection methods that exist on the chip of IoT hardware. To prevent security breaches on the institutions' network infrastructure, all participants mentioned that all the devices were updated and patched at regular intervals, and they most often engage the services of external vendors to run vulnerability tests on their behalf. The responses from most of the participants indicated that they performed penetration tests annually to isolate intruders; they invested in security hardware to prevent attackers from exploiting their networks, and they continuously patched their networks to update their applications that have known vulnerabilities. Technology has become inevitable to humans and institutions, but the security vulnerabilities that exist in these IoT devices have become easy to compromise (Amanullah et al., 2020). It is common these days for IoT devices to be breached because of the difficulties involved in protecting IoT devices, which have low memory and are heterogeneous.

The DOI theory directly impacts the security of devices introduced in innovative technology, and the responses from the participants correlated with the tenets of the DOI theory. IT administrators physically separate network segments from other network gears to ensure IoT networks' security (Pek, Buttyan, & Bencsath, 2013). All the participants commented that they invested in hardware and related services to prevent intrusion into their networks and unwarranted access to the IoT devices in their institutions. Using Rogers's (1962) DOI theory, the five characteristics of compatibility, relative advantage, trialability, observability, and complexity aligned to this research study, as the participants' responses during the interview indicated that they could be related to the five characteristics of DOI Prts 1, 2, 4, 5, 7, and 9 noted that they were conscious of the fact that the IoT devices being integrated had a relative advantage over previous technologies. For the five characteristics of the DOI theory to be effective, a good understanding of the theory's various components is necessary. The theory is built on the idea that there has to be a prior condition that urges adopters to be aware of the resource and perceived need for additional improvement for integration to work (Tristani et al., 2020). The participants noted they invested in security hardware as part of their effort to protect the network and IoT devices from unauthorized access and improve productivity, preventing downtime due to breaches.

Theme 3: Policy Management—Internal to IT

The last theme extrapolated from the interviews was the internal development of management policies to guide users and stakeholders on safeguarding the IoT devices in the institutions' infrastructure network and the data that reside on the network. The theme policy management—internal to IT is all-encompassing, as it has a direct implication on how users and other stakeholders adhere to the security concerns of the technology and innovations in their institutions. To effectively manage the wireless sensors and RFIDs in the IoT devices, IT leaders need to construct a mechanism to guide users on the security and privacy practices of the IoT devices in the institution (Baagyere et al., 2016). Prts 10 and 11 noted that the strategies, policies, and procedures developed by the institution’s IT leadership and management were geared toward protecting the IoT devices and the network infrastructure. Six participants noted they had internal documents designed to control the access level that users have to the organization's data and network infrastructure. Prts 2, 4, and 8 indicated that they develop training manuals and documents to guide users to avoid the pitfalls associated with IoT device vulnerabilities. According to Koniagina, Belotserkovich, and Vorona-slivinskaya (2020), IoT technology's security and privacy require the development of compelling strategic policies aimed at blocking vulnerabilities in the technologies. All the participants interviewed mentioned that they provided policies and training to their stakeholders to ensure uniform methods exist to ensure the security and privacy of the IoT devices and infrastructure. As displayed in Table 4, the participants' responses showed that they had policies to eliminate vulnerabilities and provided a level of security access that ensured the safety of the IoT device infrastructure. The participants provided internal memos, board minutes, and acceptable-use policies, and vendors provided documents to support the internal policies of the IT department of the institutions. The acceptable-use policy explained the access level that users have to the network and data, while vendor documents provided internal users with instruction on the devices' specifications.

Table 4

Theme 3: Policy Management—Internal to IT

	Participants		Documents	
Major theme and subthemes	Count	Reference	Count	Reference
Policy management—internal to IT	11	208	23	9
IoT deployment policy	10	67	7	9
Policies to eliminate vulnerabilities	11	57	6	6
Security of user accounts and IoT devices	9	33	5	10
Vendors and stakeholders' role in breach prevention	10	51	5	10

The findings of the subthemes were supported by existing literature. Although the protection of IoT devices is essential, policies to guide users on best practices are necessary to supplement the applications meant to protect the devices (Koo & Kim, 2018). Existing literature supported the participants' positions regarding the need to develop internal policies to guide the management of the institutions' devices. The complexity and heterogeneous nature of IoT devices require the application of multiple protocols. As a result, adequate policies are necessary to ensure IoT data security and regulate access to managed data (Sicari et al., 2017). Prts 5, 6, 7, 10, and 11 stated that they developed internal policies to ensure users were aware of the implications of not securing their access to IoT devices. According to Sicari et al. (2015), the policy enforcement framework must distribute and synchronize the resources available to all users, especially when resources are not centralized. Most of the IT leaders who participated in the study stressed the need to provide their users with policies that determine the level of access available to them and the implication of not adhering to stated policies and procedures. Koo et al. (2018) determined that the lack of security policies for IoT devices and infrastructure could lead to financial loss for institutions, as their financial, confidential, and personal data could be leaked or stolen. The participants indicated that they took precautions to prevent unauthorized access to institutional data by implementing pragmatic security policies for their users.

The conceptual framework of this study is applicable to the development of internal policies. The DOI theory explains the stages of integrating technology in an institution and the dissimilation of information and policies through social networks (Akinyemi, Harris, & Kawonga, 2019). Rogers (1995) contended that IT leaders can adopt innovation by using communication channels via social networks over time. The participants in the study reiterated the importance of promoting policies that protect networks from unauthorized access. Tristani et al. (2020) noted that teachers' training resources could be useful when there is a systematic approach to integration using the DOI theory framework and concluded that successful integration could result in the communication and promotion of good policies and strategies. Prts 5, 7, 10, and 11 indicated that they disseminated their policies to their users during seminars and training sessions. Prts 5, 10, and 11 noted that they explain security and access levels to users to ensure that they adhere to the security plans being implemented. The DOI theory allowed the people to contextualize the integration concept and provide a perspective of the IT leaders (Strömberg et al., 2016). The policies provided to the users and stakeholders must be curated and presented to be easy to comprehend and assimilate. The DOI definition provided by Rogers has three evident characteristics: (a) leaders attitude toward change; (b) internal components of the institution based on centralization factors, complexity, formalization, interconnectedness, and size of the institution; and (c) the external components of the institution that influence the preparedness to adopt technological innovation. Some participants indicated that the complexities involved in integrating IoT devices in their various institutions require the use of policies, rules, and regulations to influence the acceptance of processes put in place to prevent breaches. The technology adoption approach in organizations is a complex undertaking, and multiple individuals, rules, and regulations influence the decision process (Ramavhona & Mokwena, 2018). Although the framework articulates the variation of decision making over stages, it is not without weaknesses concerning explaining the integration process.

Subtheme 1: IoT deployment policy. The first subtheme that emerged under the main theme of policy management—internal to IT was IoT deployment policy. To prevent breaches, accurate and reliable data are essential, and developing policies and procedures can ensure the deployment of IoT devices (Kao, Nawata, & Huang, 2019). The successful implementation and integration of IoT devices in educational institutions was the basis for this study, and participants had a variety of IoT deployment policies. Prt 1 responded that his institution's policy was to perform an initial deployment on a smaller scale and test the systems before performing a widespread rollout. Prt 11 mentioned that his institution’s deployment strategy ensured there is as little human interference as possible during the deployment and configuration of IoT devices. He also noted that his institution’s policy was to support all IoT devices and segment the network to which the devices are connected. Prt 11 further said that anytime IT administrators provision IoT devices, they always had the users and stakeholders in mind and not the IT administrator. Prt 2 stated, “The first thing before we even consider any device is, is there a justification for it to be on the network.” Prts 8 and 10 noted that they must justify and ensure the IoT devices being deployed are curriculum-driven and, at the same time, adapted to their infrastructure environment. Users do not like some policies because they have to perform extra steps to secure IoT devices, including two-factor authentication, which causes inconvenience to the users (Sicari et al., 2017). Prt 3 mentioned that he built a separate VLAN for the IoT devices introduced due to their propensity to be attacked and indicated that all deployed devices need to have the latest security update and password enabled.

Continuing with the vulnerabilities of IoT devices, Prts 4 and 5 noted that, owing to the vulnerabilities of IoT devices, it is their policy to refresh their IoT infrastructure every four years. One of Prt 6’s institution policies was to ensure the devices can be filtered, even when users are at home, not to introduce vulnerabilities into the network the next time it authenticates. Prt 6 stated,

> Every single device required a district-managed username and password as a way of securing the devices that are deployed on the network. The password changes every 60 days. It is relatively secure in the sense that it is a minimum of 8 characters, [and] requires a number and a special character.

According to Prt 7, “But as I talked about it with my team, really it is tested and verify, test and verify, and use of the product right.” Prt 7 also noted that IT leaders at his institution mainly apply the IoT device policy to their HVAC systems due to the number of vulnerabilities that make them unstable and highly susceptible to attacks. Prt 8 indicated, “We do not let people just go out and buy whatever they want. We do not let people bring things and put them on our main network" and "We only allow approved devices on our network as part of our policies." Prt 8 continued, stating, "We know what is on our network, and we do not allow external devices to connect to our main network." The policies provided by most of the participants served to ensure that IoT devices that are susceptible to attacks are not placed on the network infrastructure or are given extra attention. Prt 9 mentioned that his institution's policy was to use MDM to deploy applications and update their IoT devices. Security and strategic policies help IT leaders standardize their operations, as users will have a document to use as a point of reference. Participants provided their institution's board minutes that contained approvals for purchasing and deploying IoT devices in the institutions. Some participants also provided their responsible-use policies, which stipulated the users' permission levels and the protection of IoT data and devices. Using these documents helped ensure the deployed devices are protected from unauthorized access by users, putting the IoT network and data at risk. The internal responsible-use policy documents also indicated the access level that the users had to the deployed IoT devices and the data on the networks. The internal policy documents were geared toward protecting the IoT devices and networks of the institutions.

I found literature to support IoT devices' deployment in institutions and corroborated the IT leaders' responses who participated in the research study. The dynamic environment of IoT creates situations where predefined access-control policies cannot meet the security and privacy objectives of the educational institutions for extended periods (Alkhresheh, Elgazzar, & Hassanein, 2020). Prt 5 indicated that IT administrators had to craft their deployment policies and refine them very frequently to keep up with the vulnerabilities presented to them during the day-to-day deployment and management of the IoT devices. According to most of the participants, controlling access to data and systems was at the top of their list of priorities, and providing users with the wrong access could negatively affect data and the network of an institution. According to Alkhresheh et al. (2020), relaxing security policies during the deployment of IoT technology may increase the risk of insider attacks, making the maintenance and deployment of IoT devices cumbersome for the institutions. Alkhresheh et al. advanced the process of frequently updating institutions' security policies by advocating for the automation of frequently updating the institutions' security and privacy policies to minimize human intervention in the assignment of access-control permission. Prt 11 stated that IT leaders engage high-level consultants to help them streamline the deployment process to prevent errors when determining the level of access to provide to specific users. With the increased use of sensors in IoT devices, the performance of these devices needs to be optimized, and as a result, there need to be policies that will guide the performance, reliability, range, and security of the IoT devices enrolled in the network infrastructure of the educational institutions (Alkhresheh et al., 2020). Prt 10 mentioned that IT leaders had to craft special policies to accommodate the HVACs, public address systems, and other specialized IoT devices that require continuous updates.

This study's conceptual framework was the DOI theory, and th**e** responses provided by the IT leaders who participated in the research study aligned with the DOI theory. There is a vast amount of literature on DOI, and the predominant theme that runs through most of the literature is how information flows through institutions' social systems (Scott & Mcguire, 2017). Most participants asserted that disseminating information through policy documents, training sessions, seminars, and procedures is one of the methods they use to let information flow to their user community. According to Prt 6, clear policies and standards helped IT leaders provide best practices and procedures to all users on the network to prevent breaches due to the vulnerabilities in the IoT network and IoT devices in the educational institution. To demonstrate the complexity of IoT deployment concerning the DOI theory, Shin and Hall (2018) discussed the complexity of innovation policies and patterns when applying DOI theory. Some policies could have a substantial impact while others could have minimal impact, and leaders of institutions must find a balance and amalgamate the various policies to provide a seamless process for IoT device users (Shin & Hall, 2018). Prt 8 revealed that IT leaders of his institution had policies for traditional IoT devices that they controlled but struggled to manage specialized devices such as HVACs, smart key card entry systems, and Echo Dot that were managed by external vendors who do not provide IT leaders, with the backend configuration of the devices and therefore make it cumbersome to support the devices through policy prescriptions.

Subtheme 2: Policies to eliminate vulnerabilities. The second subtheme that emerged under the main theme of IoT deployment policies was policies to eliminate vulnerabilities. It is well-known that IoT devices are prone to vulnerabilities (Sadeeq et al., 2018), and the IT leaders who participated in the research interviews had that concept in mind. Prt 1 mentioned that as part of the IT leader’s policies to eliminate vulnerabilities in the IoT environment, they ensured their passwords were highly protected. Prt 10 indicated that it was the IT leader’s policy to “have to segment our HVAC equipment off from the rest of our work, just to prevent any issues.” Also, according to Prt 10, as part of the policies to eliminate IoT vulnerabilities, the IT leaders perform penetration testing to determine which devices present vulnerabilities to the institution’s network system and then take steps to block the vulnerabilities. Prts 2 and 5 also mentioned that they segmented their networks as part of their policy to eliminate their network vulnerabilities. Prt 2 stated, “We have a separate wireless network for those devices and IoT network; each specific device has its preshared key password. So we do try to be as secure with those devices as we can.” Prts 5 and 11 noted that their institutions filter their public and guest networks to identify and isolate attackers. Prt 11 indicated that filtering packets is their focus for security and, by extension, eliminating vulnerabilities. According to Prt 2, IT leaders limit users’ access to only the users' data when their IoT devices are connected to the network. The strictly controlled devices include Amazon Echo Dot, cloud-based security cameras, and other devices that need to authenticate using 802.1X protocol were not allowed on the network of Prt 2’s institution. Prts 3 and 8 indicated that one of their policies was to keep unknown devices off their network and noted this had been a struggle since numerous IoT devices were on their network systems. Prt 5 mentioned that the IT leader’s policy was to restrict internal and external connections to only the devices that need to be connected. According to Prt 5, IT leaders monitor the network for vulnerabilities using a vendor and various hardware types that act as another security layer. All the participants mentioned that they perform tests to verify whether there are intruders on the network.

The IoT aims to use different day-to-day personal devices connected to the Internet to gather electronic data that sensors and RFIDs have generated (Meneghello et al., 2019). The information that traverses the devices using the Internet could be personal or confidential and could have security and privacy implications if it ends up in the wrong hands. To ensure there was no man-in-the-middle attack, Prt 5 said that security updates were pushed using MDM and that the student network had been separated from the faculty network. Prt 6 mentioned that his IT administrators had implemented a password policy that ensured their users’ passwords expired every 60 days, at which time users had to change their passwords. Prt 7 mentioned that the IT leader’s policy was to comb through the documentation and recommendations for vulnerabilities and updates when purchasing new IoT devices. According to Prt 7, identifying vulnerabilities ensures that IT leaders can patch the applications that run on IoT devices. Prt 8 stated that the It leaders invested in endpoint protections to block vulnerabilities before they even attempt to enter the IoT network. The institution’s IT leader also tried to encrypt most of their passwords, packets, and data that traverse the network. According to Prt 9, all vendors must go through physical security any time they want to access their network, which means they cannot use remote access or a VPN to access the network infrastructure. To eliminate vulnerabilities, Prt 9 said the IT leaders also use malware and virus-scanning tools to understand IoT client devices' state. Some of the documents that participants used to support this theme were responsible-use policies, firewall policies, purchase orders, invoices, and board minutes. These documents were geared toward protecting the IoT devices and the network. The institution’s IT leaders used the acceptable-use policies to thwart attacks by internal users and hackers who would want to take advantage of the weakness in users’ attitudes and actions.

Information on methods to eliminate vulnerabilities using institutional policies is well-documented in the existing literature. Institutions need to have policies that will secure the authentication protocols created to connect to IoT devices to eliminate vulnerabilities in the IoT’s RFIDs and other sensors (Alamr, Kausar, Kim, & Seo, 2018). Creating policies to eliminate vulnerabilities was one of the main subthemes that emerged during the interview with the IT leaders. The existing application on IoT devices used to be analyzed with expert human eyes to determine vulnerabilities that exist in these devices, but this method of determining vulnerabilities had flaws, and the resulting development of automated systems to detect and eliminate vulnerabilities is a step in the right direction (Liu et al., 2020). Prts 8 and 11 claimed that the rapid and dynamic changes in the IoT technology make it challenging to keep up with the vulnerabilities, so security experts' engagement makes it easier for them to stay abreast of security updates and patches. Prt 10 confirmed that the IT leader runs penetration tests with security consultants' help to plug open ports and other vulnerabilities in the IoT device and network ecosystem. IoT policies are required to define and secure data access-control mechanisms, including the encryption of data that traverse institutions’ IoT networks (Huang et al., 2018). Prt 10 again mentioned that the IT leader created policies geared toward educating users about the existing vulnerabilities and preventing external attackers from exploiting the IoT device infrastructure's weaknesses. The enforcement of security policies that promote privacy, security, and enhanced reliability in IoT devices enables the security complexities that the IoT presents to be hardened (Tabrizi & Ibrahim, 2016). Most of the participants commented that they were proactive by asking vendors to provide patches and updates as part of their policies and procedures, eliminating the vulnerabilities in these autonomous low-memory IoT devices.

The DOI theory aligns with the responses received from the IT leaders who participated in a research interview. The effective communication of new security weaknesses to stakeholders ensures the successful adoption of technology in an institution. Also, it enhances the safety of data and infrastructure by employing one of the DOI elements of communicating using social network channels (Iles et al., 2017). Most of the participants in the study mentioned that, as part of their policies to eliminate vulnerabilities, they had enshrined in their policies that all users require strong passwords and do not share their usernames and passwords with anyone to develop better and safer practices to promote the privacy and security of data. Some of the participants mentioned protecting sensitive data against cyber-attacks as one of the areas for which they had created policies to eliminate some of the vulnerabilities. The DOI theory lends itself to innovative technological integration and adoption using social network channels (Thomas et al., 2016). The decisions made by the participants during the adoption and integration of IoT devices paved the way for their users to use IoT technology efficiently and securely in a productive and safe environment.

Subtheme 3: Security of user accounts and IoT devices. The third subtheme that emerged was the security of user accounts in the IoT devices, which significantly affects preventing breaches in educational institutions. Stealing user credentials is one of the methods attackers use to access IoT devices and infrastructure (Meneghello et al., 2019). Prt 10 noted that his institution always holds in high esteem the safety and privacy of students' data. Hence, he ensured the security principle of least privilege was actively practiced in his institution. According to Prt 10, this was the main reason smartwatches, Google Home, and Amazon Echo Dot were not allowed on his network. All the participants answered the interview questions on device security by saying they ensured they reset all default passwords of any device they purchased.

One of the vulnerabilities of IoT devices is the access that attackers gain using brute force to attack weak passwords or using default passwords that were not changed (Cristian et al., 2018). Prt 11 stated, "If you enter your username and password for the actual authenticated users network based on who you are if you are a student or a staff member, you are going to get different rights." Authenticating users to the network allows various users to access various networks and shared data (Granjal et al., 2015). Prt 3 indicated that access control must be strictly adhered to so that only administrators have exclusive access to the entire network and data. Most participants said it was essential to perform a continuous update to ensure usernames and passwords were not compromised due to vulnerabilities discovered by attackers in the applications that run on IoT devices. Prts 3, 6, 7, and 8 mentioned that it is vital to reset passwords every 60 days, enforce password complexity, set permission, and isolate passwords for edge IoT devices on the network. Prt 9 stated, “Generally speaking, in terms of security, we have standards for setting up passwords for objects that are linked to our active directory services and that provides us with some central administration of credentials.” Prt 8 noted, “We try to use encryption as much as we can, and we use account security best practices with passwords.” Prt 8 indicated that offering user training on username and password security is essential to the security of user data, IoT devices, and the network infrastructure, and as a result, IT leaders use multifactor authentication on all user accounts. Prt 8 also mentioned that IT leaders do not provide standard users with administrator usernames and passwords, as the administrator’s username and password are kept to a small group of people. The documents provided by the participants included responsible-use documents, IoT device management, IoT network authentication policies, classroom technology integration documents, and technology data solution documents. The documents that the participants provided, including their responsible-use policies and internal security documents stipulating encryption and authentication policies, supported this subtheme. The documents ensure user accounts' protection and prevent external unauthorized persons from accessing the IoT devices using compromised accounts.

This finding, which was the importance of ensuring reliability, security, and privacy during the integration of IoT devices, was supported in the literature. For example, Chen and Zhu (2019) indicated that IoT device users must secure their IoT applications due to the increased number of devices enrolled in innovative technology. According to Chen and Zhu, not knowing IT administrators' security policy decisions could leave users in limbo, which could be detrimental to educational institutions' network infrastructure. The use of username and passwords enables users to access their online or on-premises services, but when those accounts are compromised, it could be devastating for both users and the entity that host the user accounts (Abdelaziz, Napoli, & Chiasson, 2019). Prts 1, 2, 6, and 8 mentioned that they provide users with usernames and passwords to access the correct data using the IT department's mechanisms. All the participants explained that they abide by the principle of least privilege, where users are given precisely the rights they require to perform their job functions. Abdelaziz et al. (2019) wrote that proactively applying two-factor authentication to online credentials as protection from unwarranted access ensures the protection of the user accounts and the devices and data that reside on the network.

DOI formed the anchor of the study results. The subtheme of security of user accounts and IoT devices aligns with the DOI theory, as the process of integrating innovative technology in the modern era has some similarities to the characteristics mentioned in the DOI theory. Rogers (2015) posited that the ease of technology use, as described in the DOI theory, simplifies the technology innovation process and stakeholders’ perception of the technology. During the interviews, all the participants demonstrated that they introduced IoT device technology to their users by explaining the ease of use and increased productivity that the technology brings to the institution and the users. The benefits of using social networks and channels to demonstrate the DOI theory to like-minded individuals provide an understanding of the technology and accelerated acceptance of the innovation (Akinyemi et al., 2019). Prts 3, 5, and 9 noted that they provide training to all users, integrate IoT devices over a lengthy period, and provide abundant literature on the innovative technology to their users, hoping that the users will be eased into accepting the IoT devices being integrated. According to Vargo, Akaka, and Wieland (2020), diffusion is an essential impetus for spreading innovative technology throughout society, and DOI brings to light the rate that adopters accept, use, and spread new technology. Most of the participants described the steps they take to ensure users understand the technology and share their understanding with other users. The level of training and communication provided to users and stakeholders is key to the technological innovation's success being integrated.

Subtheme 4: Vendors and stakeholders role in breach prevention. The fourth subtheme was the vendors’ and stakeholders’ role in breach prevention in the IoT ecosystem. The collaboration between educational institutions and vendors plays an essential role in the security of IoT devices and educational institutions' network infrastructure (Chong et al., 2019). All the participants had a relationship with at least one vendor to secure IoT devices, the provision of upgraded devices, and security applications. To this end, Prts 2 and 10 indicated that they use their vendors, who are IoT experts, to provide fixes for their vulnerabilities and data on their network infrastructure. Prt 11 explained that they receive mostly updates on loopholes and vulnerabilities from their vendors and transfer that knowledge to their teachers, students, administrative users, and parents through training and professional development. Prt 3 stressed that, because manufacturers of IoT devices do not always follow up with a security update on their devices, IT leaders must rely on vendors to provide follow-up security updates and training on patching the network infrastructure and IoT devices with the updates.

Vendors can help IT leaders implement security projects using established local institutional deployment policies (Johnson et al., 2018). According to Prt 3, an effective way to build confidence in stakeholders is by letting them know that you have their best interests in mind. All the strategies put in place are to protect the privacy and reliability of their IoT devices and their data. Prts 2, 4, 5, 6, 7, 10, and 11 mentioned that they ensure the data, identity management, and privacy of users are protected at all times.

The use of vendors to facilitate the security of IoT devices and an educational institution's infrastructure was a collaborative policy that helped the inventory and productivity of institutions (Dasaklis & Casino, 2019). Prts 3, 6, and 7 noted they relied on vendor partners such as COSN for professional development materials, security update information, and peer-mentoring. Prt 3 stated, “I have to depend on organizations to bring security knowledge to me, so groups like COSN I think are incredibly important, as well as honestly a lot of the networking that happens.” Prt 4 indicated that he leverages his vendors for answers to his security questions and issues that are outside his security knowledge. Prt 5 mentioned that implementing firewalls to protect IoT devices, and the network infrastructure was one of the solutions that helped secure the network infrastructure. The configuration, management, integration, and deployment of heterogeneous devices require expert knowledge (Siboni et al., 2019). The vendors help the educational institutions’ IT leaders to fortify their network infrastructure. Prt 5 answered the interview question by indicating that, in IT leaders dealings with vendors,

> they try to make sure that those solutions also have known patch management for security vulnerabilities, that they are constantly applying those software updates,

> and they try not to let products that go into end-of-life stay in their network for too long.

All the participants stressed the critical role that vendors play as they introduce upgrades, patch updates, and newer technologies in the educational institutions’ network settings. Prt 6 noted his security vendor provides another layer of security that protects the educational institution. Prts 7, 8, and 11 mentioned that they put pressure on their vendors to provide updates and patches to the network and IoT devices they supply to the institutions. Prt 7 also mentioned that the Indiana Department of Education provides updates, education, and guidance to IT leaders to secure the institutions' network infrastructure. Prt 7 stated, “We are following the security protocols that come out from our vendors and reading and watching that material carefully. So it is really about reading, research, and education.” Prt 8 noted that vendors providing services, which included professional insight on cybersecurity threats, allowed IT leaders to pay close attention to the security threat landscape. Prt 8 stated,

> At some point, we have to rely on our vendors to sell us products that are going to be stable and reliable and are not going to be susceptible to cybersecurity threats, and I think that is a big part of making sure that everything is up-to-date.

A caveat to the vendor relation that was also mentioned by Prt 8 was that IT leaders look at vendors' history to ensure they are capable of helping secure IoT devices with timely patches and updates. If vendors have been prone to cyber-risk and security dis-information, the IT leadership stays away from those products. Prt 9 noted that vendors' online resources were invaluable, and Gartner, for instance, provides threat analysis that includes security information. Prt 9 stated,

> I am pretty much always looking for vendors, particularly in the security space that understands the state of the technology market and can help us get to stay informed about what is out there because that space is moving very quickly right now.

The role of vendors in ensuring IoT devices are secured and safe is paramount when designing IoT deployment plans. IoT integrators are aware that IoT device vendors have different types of IoT devices, which has become a challenge to the It leaders who dare integrate the technology (Yang, Li, & Sun, 2019). All the study participants mentioned that they had numerous IoT devices in their institutions, including HVACs, public address systems, iPads, Chromebooks, and other devices with sensors. IoT device vendors have a role in securing the dynamic IoT technology industry, presenting a multidimensional challenge to IT leaders who deploy the technology in the technological ecosystem (Kumar et al., 2017). The participants' documents that could be used to support this subtheme included internal memos on wireless configuration and security, responsible-use policies, and internal documents on device care, device issuance, device inspection, and purchase. The documents on vendor contracts and invoices showed that the vendors provided devices that had encryption technologies with security-enhanced capabilities. Technology solution documents provided a collaboration between the institutions and vendors on the students' information systems' security prescription and management, a database with students’ grades, attendance, and transcripts.

This study's findings were grounded in the DOI theory, and the responses from all the participants correlated with the tenets expressed in the DOI theory. As the conceptual framework of this research study, the DOI’s five characteristics provided the IT leaders with a structure to outline the security strategies they had used to prevent breaches in their institutions. There will be an increase in cybersecurity breaches if vendors and manufacturers fail to secure their devices, affecting organizations' purchasing decisions (Manky, 2017). All the IT leaders who participated in the study expressed the importance of engaging IoT vendors to provide product information, training, vulnerability information, updates, and patches for the IoT devices because they are heterogeneous and numerous. The five characteristics of DOI and outside influences are essential to the integration of IoT in banking (Ramavhona & Mokwena, 2018). All the participants' experiences in this study mirrored the five characteristics of DOI as the external factors of vendors, manufacturers, stakeholders, and security threats from attackers influenced the adoption and integration of IoT devices in educational institutions. The data that flow through the IoT networks to the devices have to be highly accurate due to the number of vendors with proprietary software (Sivanathan et al., 2020). Prts 2, 4, 5, and 11 reiterated their close coordination with security and software vendors to protect the devices from being attacked and provide training to their institutions. Leiba et al. (2019) mentioned that vendors and manufacturers do not patch their IoT devices as often as they should.

Application to Professional Practice

This study's objective was to explore IT leaders' security strategies to prevent data breaches resulting from the integration of IoT devices in their educational institutions. The participants in this study provided the strategies they used to secure the IoT devices enrolled in their network infrastructure. The IT leaders' strategies were to prevent breaches emanating from the nonhardening of IoT devices and infrastructure in their educational institutions. IT leaders can use the strategies highlighted in this research study for preventing security breaches during the integration of IoT devices in educational institutions to protect their data and secure their network infrastructure.

The concept of IoT integration has caught on in most K–12 public schools owing to the ability to be easily connected to the Internet and the efficiencies that exist in the transfer of data from one device to the other. However, some vulnerabilities in the data transmission process from one IoT device to another due to the IoT devices' low memory and data storage space (Radisavljevic-Gajic et al., 2018). IT leaders of educational institutions have been worried about the security vulnerabilities that exist in IoT devices and, as a result, have instituted measures to prevent their IoT devices from being attacked by hackers. Protecting IoT devices in an educational setting was essential to the participants, as breaches can negatively affect students’ data and the school districts' network infrastructure, productivity, and profitability. The participants expressed their concerns about IoT vulnerabilities by indicating that one of the first steps they took when they procured IoT devices was to change the default passwords. A primary security practice is to change the preinstalled password of a device before its first use

(Meneghello et al., 2019). This practice can be applied to professional practices, as all IT professionals need to change all default passwords any time they purchase and install new IoT devices in educational institutions. Practicing password security and complexity will promote students' data's reliability, privacy, and security and protect the confidential information in school districts and school districts' network infrastructure.

The IT leaders who participated in the research study described some of the difficulties they encountered during the IoT integration in their educational institutions. The lack of funding to implement cutting-edge technologies to improve the IoT process's integration was a reason cited by some of the participants and corroborated by Suduc et al. (2018). The participants mentioned that they leverage e-rate funding, which is federal funds for public K–12 institutions, to procure network gears to secure these institutions' IoT network infrastructure. The cost of securing students' IoT devices and protecting the data generated by the IoT is so high that school districts are grappling with funding sources for these kinds of activities (Nieuwenhuijsen et al., 2018).

The other aspect of the research study that could apply to professional practice was the participants' experience and expertise. Based on the responses from the participants, they knew that if they could secure the IoT network infrastructure and the devices enrolled on them with usernames and passwords, antivirus software, patches for applications, and other best practices, they would achieve a significant objective of securing the data of users and prevent breaches. The practice of patching networks and making users authenticate to the network can be transferred to other industries where IT leaders are interested in securing their network and preventing breaches during the integration and deployment of IoT devices. The expertise shared by the participants has the potential to positively affect the management and implementation of projects in both the education sector and other similar industries. The participants stressed the importance of keeping up-to-date on scanning their network, working with vendors to apply solutions to identified vulnerabilities, and segmenting IoT devices on the network to avoid breaches. Researchers could apply the participants' responses to most industries, and vendors play a major partnering role with IT leaders to ensure their infrastructures' security is optimized up to 99.999% of the time.

Furthermore, the participants mentioned that collaborating with partners and vendors was smart to stay abreast of technology's cutting-edge side. According to most of the participants, collaborating with vendors could lead to users' training and, by extension, could improve the security of IoT devices and IoT infrastructure. The concept of continuous collaboration with partners could be potentially transferred to other practices, as most industries have vendors and are willing to collaborate with their customers. Among the vendors who could ensure collaboration are Internet service providers, software vendors, and security organizations. There is also a possibility that collaborating with partners could lead to further training of IT leaders and their teams to identify vulnerabilities and patch them accordingly. An enlightened and trained team in an organization could potentially lead to the protection of businesses' data and network infrastructure, including other sectors of education institutions such as universities and technical colleges.

Implications for Social Change

The development of strategies to prevent IoT breaches in educational institutions can introduce awareness and alertness to educational institutions and other industries' IoT technological environment. This study's findings may influence the development of strategies to prevent IoT devices' breaches during the integration of the IoT in educational institutions. According to Amanullah et al. (2020), IoT devices in numerous industries have been hit by cyber-attacks due to the number of objects connected to the Internet. Introducing steps to prevent vulnerabilities' exploitation could enable IT leaders to align institutions' business with data security. The protection of data is paramount to most industries' success, and the development of strategies to prevent data breaches was at the core of the actions taken by the IT leaders; and the strategies developed can be applied in most settings to secure the data of an organization. The strategies developed during this study may allow IT leaders to have firm control over the data in their institutions to secure the IoT infrastructural environment. Developing methodologies and coordinating with partners will lead to instructions with in-depth and rich analytical tools to fight attackers and secure organizations' data assets.

Identifying vulnerabilities in IoT devices requires knowledge of IT leaders' variables to prevent large-scale breaches. IT leaders may unambiguously communicate the remediations with stakeholders to ensure data loss and damage to the IoT infrastructure are minimized. Effective communication to users and other partners requires creating IoT security and device policies that are concise, clear, forward-leaning, and user-centered. The lack of a detailed method of effectively communicating policies could lead to the loss of productivity, frustration, and IoT infrastructure damage if an intruder manages to access vital resources. The alignment of security policies and users' efficient performance needs to be clearly defined to avoid friction, confusion, and confrontation.

The IoT has gained notoriety for being heterogeneous and evolving quickly. Training and educating users promotes an understanding of the security vulnerabilities, technical efficiencies, and safety of the users and the IoT devices. An informed user group could potentially create a safe working environment and enhance productivity. Collaboration with partners, vendors, industry leaders, and IoT security experts may lead to a secure working environment due to knowledge transfer. Experts and partners typically have training sessions and share trending vulnerabilities with IT leaders, creating awareness and ensuring patching and updates.

Recommendations for Action

The implementation of security strategies to prevent breaches during the integration of IoT devices in educational institutions requires IT leaders and their institutional leaders to develop policies and collaborate with stakeholders while not compromising the confidentiality of the institutions' data and the reliability, security, and privacy of the systems and data on the network. I explored security strategies used by IT leaders to prevent breaches while maintaining the reliability, security, and privacy of IoT devices during the integration of those devices in educational institutions. The first recommendation for IT leaders is to fine-tune the alignment between the security of IoT devices and productivity. The primary function of an IT department and IoT devices is to ensure all students and faculty can perform their job functions without interruption. The security policies adopted by the IT leaders to prevent breaches should not be so stringent that users cannot complete the essential services they were hired to perform. However, relaxing the security policies should not make it possible for IoT devices to be infected, hijacked, or prevented from accessing the IoT network infrastructure and data that reside on an educational institution's network. The alignment of IT security strategies and device performance can lead to continuous usage of IoT devices and allow users to be productive at the same time.

The second recommendation is for IT leaders to establish the capacity to manage the various facets of IoT device integration to not depend on vendors for patching and upgrading their IoT devices and infrastructure. The patching and upgrading capacities of institutions require establishing a knowledge base and a culture of learning and curating the materials necessary for preventing breaches during the integration of the IoT. Collaboration with vendors and industry partners could be a good idea. Still, depending on the vendors who provide IT leaders with security updates and patches, collaboration could also be a dangerous proposition, as some may not be willing to admit that vulnerabilities exist in their applications. IT leaders who build the local capacity of educational institutions will promote the security, reliability, and privacy of IoT devices, as IT leaders will be proactive in seeking and preventing breaches before harm is done to the IoT infrastructure ecosystem. Preventing breaches requires building a knowledge base and developing best practices, an efficient team, and a policy document spelling out all the requirements to ensure the systems are always up-to-date. One way for IT leaders to create knowledge is to identify vulnerabilities and stay up-to-date on patching IoT devices and educational institutions' infrastructure. IT leaders could achieve this by attending security conferences, collaborating with vendors, hiring consultants to work with the IT leadership and teams, and staying abreast of new vulnerabilities that could lead to security breaches. As a modern heterogeneous innovation, IoT technology encourages IT leaders to acquire the skills, practice, and policies to stay up-to-date on the updates and patches introduced to avoid vulnerabilities.

The third recommendation is for IT leaders to develop systems to help the community understand the security vulnerabilities in their devices that fall under the IoT technology umbrella. IoT devices could be personal and home-use devices that connect to the Internet. Although these devices may not be enrolled in the network infrastructure, they are still susceptible to the vulnerabilities that exist due to the miniature of the devices and access to the Internet. IT leaders' recommendation is to make the knowledge gained, lessons learned and experiences accumulated available to the community, so community members do not fall prey to attacks that steal their personal information. Ways for IT leaders to disseminate information could involve participating in information sessions and seminars or sharing pamphlets with community members. Community members need to know how to protect their data, ensure they have password complexity in place and have devices patched and updated as often as possible. The application of IoT integration strategies and practices in educational institutions requires IT leaders to develop policies, vendor and partner relationships, a culture of staying up-to-date on updates and upgrades, and an environment where users can be creative and innovative.

The same understanding could be applied to the community by teaching community members to patch and update their devices and adhere to best practices to prevent breaches. In addition to IT leaders in public education, the study results might be relevant to other IT leaders who want to integrate IoT devices securely into their organizations. I plan to disseminate this study's findings through events, training sessions, conferences, and as part of my work. I will also provide copies of this research study to the IT leaders who participated in this research as the case institutions' representatives.

Recommendations for Further Study

I derived some recommendations for further research from this research study's findings and the associated assumptions, limitations, and delimitations for IT leaders who want to introduce IoT device integration securely in their educational institutions. In this qualitative multiple case study, I explored the security strategies that 11 IT leaders in the Midwest region of the United States used to secure the integration of IoT devices in their educational institutions. The study was limited in its geographical setting to five cities in Indiana: Carmel, Fishers, Indianapolis, Muncie, and Wabash. The first recommendation is for IT leaders to research and identify vulnerabilities in the IoT devices they plan to integrate and stay up-to-date on patching those IoT devices and educational institutions' infrastructure. Knowing the vulnerabilities associated with any IoT device will help the IT leaders evaluate the device's advantages and disadvantages before making an informed decision to procure the devices. The IT leaders could achieve this by attending security conferences, collaborating with vendors, hiring consultants to work with the IT leadership and teams, and staying abreast of new vulnerabilities that could lead to security breaches. Understanding the potential security breaches in IoT devices could help with the stability of the IoT network infrastructure and help avoid downtime due to the possible exploitation of loopholes and backdoors.

I recommend that IT leaders be socially responsible to the communities where their students live. If they do not enlighten community members on the potential of breaches, the vulnerability may show up on their network in their educational institutions’ devices because the families may have students in these institutions. Another recommendation is that IT leaders develop systems to help their community understand the security vulnerabilities. Thus, IT leaders could transfer the lessons learned to the students and their families to prevent them from falling into the traps that the IT leaders are trying to avoid. The lack of knowledge on vulnerabilities could be detrimental to communities because individuals could take advantage of the ignorance of IoT device users in the community. The study participants interact with students and their families frequently and, therefore, can use that channel as a communication conduit to help the families prevent costly and damaging breaches to the IoT devices of community members.

IT leaders of educational institutions make essential decisions on behalf of the educational institutions and the families in the community. They are also involved in planning, designing, implementing, and evaluating IoT device integration and installing the educational institutions' IoT network infrastructure. The use of IoT devices in education has become widespread, and the adoption and integration of these devices have become routine and acceptable in the educational setting. To be successful in their decision making, IT leaders need to work with a consortium of stakeholders, including security experts, collaborating partners, vendors, users, and the institutions' leaders. The themes derived from interviewing the participants reflected the IT leaders' understanding of the requirements needed to make the right decision. As a result, another recommendation is to involve various stakeholders in determining which security strategies are necessary to integrate IoT devices in an educational institution. Examining the security strategies can produce enhanced security practices that could save students’ data and IoT devices. The examination of integration strategies may help to ensure IoT devices, and their infrastructure in educational institutions are secured, stable, and reliable and ensure the privacy of user data.

Reflections

It has been my lifelong dream to attain the highest degree in my chosen profession, and deciding to pursue a doctoral degree was just a matter of time. Obtaining this doctoral degree will culminate a journey that started 15 years ago when I came to the United States at age 35. After I arrived, I decided to restart my higher education journey to ensure my IT field success. In the subsequent 15 years, I have since accumulated an associate’s degree, a bachelor’s degree, two master’s degrees, and now a doctoral degree. During the first class on my doctoral journey, after some feedback provided by my professor, I started to wonder if I could complete the journey. However, my doubt subsided after I recalibrated my thinking to understand that it was in my best interest to understand the professor's constructive suggestions. The journey put a strain on my family life, as I spent countless days and nights at my desk, either doing my assignments or writing my analysis, but on the whole, they were understanding and cooperative. My professional experience presenting and training users made it a little easier for me to work on doctoral papers, as I was already adept at writing.

The exploration of the security vulnerabilities that occur during the integration of the IoT in an educational institution has enhanced my understanding of IT leaders' issues every day. I have always worked in the education sector and am fascinated by the fast pace of IoT devices' growth and the associated vulnerabilities. I eventually became interested in the breaches that could occur if IT leaders do not securely integrate the IoT in their educational institutions. At that point, I had been an IT professional for over 15 years, and I understood operating systems and security vulnerabilities, but I did not understand the effect of the heterogeneous smart devices being introduced and integrated into educational institutions every day. The security vulnerabilities that exist during the integration of the IoT became the focus of my education. This sector has not been extensively researched on a large scale, and IoT innovation is relatively new; however, the security of data, IoT devices, and network infrastructure made it imperative to examine the strategies that IT leaders use to prevent data breaches resulting from the integration of IoT devices in their educational institutions.

Although I always planned to interview IT leaders in educational institutions, securing individual IT leaders' consent was more difficult than I expected. The difficulty obtaining participants’ consent was compounded by the outbreak of the coronavirus disease 2019, which resulted in the closure of all K–12 public schools in Indiana. As a result of the closures, the IT leaders were almost unreachable. Focusing on the interview questions and asking a follow-up question was also problematic, as the participants initially gave short answers to the interview question, and I had to pry further information from them by asking follow-up questions based on the initial answers they provided. I made every effort not to introduce bias into the interview and analyze the interview responses; however, I may have unknowingly or inadvertently influenced the data collection and analysis due to my in-depth understanding of my course's subject matter work.

Summary and Study Conclusions

Integrating IoT devices into education institutions is a painstaking task, and the role of IT leaders in preventing breaches during the integration process is critical. Integrating IoT devices in educational institutions requires IT leaders to develop strategies that demand extensive collaboration with all stakeholders. The role of stakeholders in ensuring the security of IoT devices and data is paramount. IoT integration policies must align with educational institutions' business strategies, and IT leaders must ensure they develop a culture of training and a process of educating all users. The engagement of users in securing the IoT devices connected to the network requires careful and systematic planning, development, and implementation of strategies to educate users on the ramification of a security breach. The harnessing of knowledge that occurred during the introduction, implementation, and integration of IoT devices in educational institutions was enhanced through collaborations with IoT device vendors and security partners. The inclusion of external partners in developing policies and best practices made it possible for the various institutions' IT leaders to stay ahead of potential security breaches. While the task of securing IoT devices during the integration process can be tedious and overwhelming, the outcome can help to ensure productivity, profitability, data stability, and potentially a productive user base.

IoT device integration in education has played a significant role in teaching and learning in educational institutions. IT leaders are still learning to secure the devices in educational settings, as the technology's value and capabilities are still being discovered, and so are the associated vulnerabilities. Furthermore, the designing and introduction of the IoT in educational institutions are complicated due to the number of facets that IoT devices interface with, including internal IoT users, security experts, network administrators, vendors, and collaborating partners. Although there may be some vulnerabilities associated with IoT technology and its associated devices, when the devices are well-managed, patched, and updated, and when the users are well-trained, there are many positive attributes associated with using IoT devices in educational institutions.

References

Abdelaziz, Y., Napoli, D., & Chiasson, S. (2019, August 26–29). *End-users and service providers: trust and distributed responsibility for account security*. Paper presented at the 2019 17th International Conference on Privacy, Security and Trust, Fredericton, NB, Canada.

Abdullah, N., Karim, N. H. A., Sanni, S. A., Ngah, Z. A., & Waheed, M. (2014). Using the diffusion of innovation concept to explain the factors that contribute to the adoption rate of e-journal publishing. *Serials Review*, *39*(4), 250–257. doi:10.1080/00987913.2013.10766406

Aburahma, M. H., & Mohamed, H. M. (2017). Peer teaching as an educational tool in pharmacy schools: Fruitful or futile. *Currents in Pharmacy Teaching and Learning*, *9*(6), 1170–1179. doi:10.1016/j.cptl.2017.07.026

Abuzneid, A. S., Sobh, T., Faezipour, M., Mahmood, A., & James, J. (2015). Fortified anonymous communication protocol for location privacy in WSN: A modular approach. *Sensors*, *15*(3), 5820–5864. doi:10.3390/s150305820

Adams, M. (2017). Technology innovation management review. *Technology Innovation Management Review* (Vol. 7). Retrieved from https://timreview.ca/article/1067

Agarkhed, J. (2017). Security and privacy of cyber-physical systems in IoT using cloud infrastructure, *International Journal of Advanced Research in Computer Science*, *8*(8), 580–582. doi:10.26483/ijarcs.v8i8.4841

Ahanger, T. A., & Aljumah, A. (2019). Internet of things: A comprehensive study of security issues and defense mechanisms. *IEEE Access*, *7*, 11020–11028. doi:10.1109/ACCESS.2018.2876939

Ahmed, E., Yaqoob, I., Gani, A., Imran, M., & Guizani, M. (2016). Internet-of-things-based smart environments: State of the art, taxonomy, and open research challenges. *IEEE Wireless Communications*, *23*(5), 10–16. doi:10.1109/MWC.2016.7721736

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl & J. Beckmann (Eds.), *Action control: From cognition to behavior* (pp. 11–39). New York, NY: Springer.

Akinyemi, O., Harris, B., & Kawonga, M. (2019). Innovation diffusion: How homogenous networks influence the uptake of community-based injectable contraceptives. *BMC Public Health*, *19*, 1–13. doi:10.1186/s12889-019-7819-5

Alaeddini, A., Morgansen, K., & Mesbahi, M. (2017, May 24–26). Adaptive communication networks with privacy guarantees. *Proceedings of the American Control Conference*, pp. 4460–4465. doi:10.23919/ACC.2017.7963642

Alam, S. S., Omar, N. A., Mohd Ariffin, A. A., & Nik Hashim, N. M. H. (2018). Integrating TPB, TAM and DOI theories: An empirical evidence for the adoption of mobile banking among customers in Klang valley, Malaysia. *International Journal of Business and Management Science*, *8(2)*, 385–403. Retrieved from http://www.safaworld.org/ijbms/

Alam, T., & Benaida, M. (2018). CICS: Cloud–Internet communication security framework for the Internet of smart devices. *International Journal of Interactive Mobile Technologies*, *12*(6), 74-84. doi:10.3991/ijim.v12i6.6776

Alamr, A. A., Kausar, F., Kim, J., & Seo, C. (2018). A secure ECC-based RFID mutual authentication protocol for Internet of things. *Journal of Supercomputing*, *74*, 4281–4294. doi:10.1007/s11227-016-1861-1

AlBar, A. M., & Hoque, M. R. (2019). Factors affecting cloud ERP adoption in Saudi Arabia: An empirical study. *Information Development*, *35*, 150–164. doi:10.1177/0266666917735677

Aldowah, H., Ul Rehman, S., Ghazal, S., & Naufal Umar, I. (2017). Internet of things in higher education: A study on future learning. *Journal of Physics: Conference Series, 892*(1). doi:10.1088/1742-6596/892/1/012017

Ali, S., Qaisar, S. B., Saeed, H., Khan, M. F., Naeem, M., & Anpalagan, A. (2015). Network challenges for cyber-physical systems with tiny wireless devices: A case study on reliable pipeline condition monitoring. *Sensors*, *15*(4), 7172-7205. doi:10.3390/s150407172

Al-Imarah, A. A., & Shields, R. (2018). MOOCs, disruptive innovation and the future of higher education: A conceptual analysis. *Innovations in Education and Teaching International*, *56*, 258–269. doi:10.1080/14703297.2018.1443828

Alkhresheh, A., Elgazzar, K., & Hassanein, H. S. (2020, June 15–19). *Adaptive access control policies for IoT deployments*. Paper presented at the 2020 International Wireless Communications and Mobile Computing, Limassol, Cyprus.

Allen, C., & Foulkes, W. D. (2011). Qualitative thematic analysis of consent forms used in cancer genome sequencing. *BMC Medical Ethics, 12*, 14. Retrieved from https://bmcmedethics.biomedcentral.com/

Allen, R. E. S., & Wiles, J. L. (2016). A rose by any other name: participants choosing research pseudonyms. *Qualitative Research in Psychology*, *13*, 149–165. doi:10.1080/14780887.2015.1133746

Almeida, F., Carvalho, I., & Cruz, F. (2018). Structure and challenges of a security policy on small and medium enterprises. *KSII Transactions on Internet and Information Systems, 12*(2), 747–763. doi:10.3837/tiis.2018.02.012

Al-Rahmi, W. M., Yahaya, N., Aldraiweesh, A. A., Alamri, M. M., Aljarboa, N. A., Alturki, U., & Aljeraiwi, A. A. (2019). Integrating technology acceptance model with innovation diffusion theory: An empirical investigation on students' intention to use e-learning systems. *IEEE Access, 7*, 1. doi:10.1109/ACCESS.2019.2899368

Amanullah, M. A., Habeeb, R. A. A., Nasaruddin, F. H., Gani, A., Ahmed, E., Nainar, A. S. M., . . . Imran, M. (2020). *Deep learning and big data technologies for IoT security. Computer Communications, 151*, 495–517. doi:10.1016/j.comcom.2020.01.016

Ames, H., Glenton, C., & Lewin, S. (2019). Purposive sampling in a qualitative evidence synthesis: A worked example from a synthesis on parental perceptions of vaccination communication. *BMC Medical Research Methodology, 19*, 1–10. doi:10.1186/s12874-019-0665-4

Ammari, H. M. (2018). Investigating physical security in stealthy lattice wireless sensor networks using k-barrier coverage. *Ad Hoc Networks, 89*, 142-160. doi:10.1016/j.adhoc.2018.11.003

Anderson, S. F., Kelley, K., & Maxwell, S. E. (2017). Sample-size planning for more accurate statistical power: A method adjusting sample effect sizes for publication bias and uncertainty. *Psychological Science*, *28*(11), 1547–1562. doi:10.1177/0956797617723724

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2016). Internet of Things: Security vulnerabilities and challenges. *Proceedings—IEEE Symposium on Computers and Communications,* pp. 180–187. doi:10.1109/ISCC.2015.7405513

Arnold, L. R. (2016). *Strategies for reducing high turnover among information technology professionals* (Doctoral dissertation). Available from ProQuest Dissertations and Theses database. doi:10.1111/j.1467-8616.2008.00521.x Malik

Arsel, Z. (2017). Asking questions with reflexive focus: A tutorial on designing and conducting interviews. *Journal of Consumer Research*, *44*(4), 939–948. doi:10.1093/jcr/ucx096

Arvie, D., & Tanaamah, A. R. (2018). Technology acceptance model for evaluating IT of online-based transportation acceptance: A case of GO-JEK in Salatiga. *TELKOMNIKA (Telecommunication Computing Electronics and Control), 17*(2), 667-675. doi:10.12928/telkomnika.v17i2.9634

Ashrafzadeh, A., & Sayadian, S. (2015). University instructors' concerns and perceptions of technology integration. *Computers in Human Behavior, 49*, 62–73. doi:10.1016/j.chb.2015.01.071

Aslani, A., & Naaranoja, M. (2015). A systematic-qualitative research for diffusion of innovation in the primary healthcare centers. *Journal of Modelling in Management*, *10*, 105–117. doi:10.1108/JM2-04-2013-0016

Asraf, H. M., Dalila, K. A. N., Zakiah, M. Y., Amar Faiz, Z. A., & Nooritawati, M. T. (2018). Computer assisted e-laboratory using LabVIEW and internet-of-things platform as teaching aids in the industrial instrumentation course. *International Journal of Online Engineering*, *14*(12), 26–42. doi:10.3991/ijoe.v14i12.8992

Assiri, A., & Almagwashi, H. (2018, April 4–6). *IoT security and privacy issues.* Paper presented at the 1st International Conference on Computer Applications and Information Security, Saudi Arabia.

Ax, C., & Greve, J. (2017). Adoption of management accounting innovations: Organizational culture compatibility and perceived outcomes. *Management Accounting Research, 34*, 59–74. doi:10.1016/j.mar.2016.07.007

Azad, M. A., Bag, S., Hao, F., & Shalaginov, A. (2020). Discrimination-aware trust management for social internet of things. *Computer Networks, 178*(4), 2690–2703. doi:10.1016/j.comnet.2020.107254

Azevedo, V., Carvalho, M., Costa, F., Mesquita, S., Soares, J., Teixeira, F., & Maia, Â. (2017). Interview transcription: conceptual issues, practical guidelines, and challenges. *Revista de Enfermagem Referência, IV Série, 14,* 159–168. doi:10.12707/RIV17018

Baagyere, E. Y., Qin, Z., Xiong, H., & Zhiguang, Q. (2016). The structural properties of online social networks and their application areas. *IAENG International Journal of Computer Science, 43,* 156–166. doi:10.1002/sec

Bahrami, M., Khan, A., & Singhal, M. (2016). An energy efficient data privacy scheme for IoT devices in mobile cloud computing. *Proceedings—2016 IEEE International Conference on Mobile Services,* pp. 190–195. doi:10.1109/MobServ.2016.37

Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2018). Ethical design in the Internet of Things. *Science and Engineering Ethics, 24*(3), 905–925. doi:10.1007/s11948-016-9754-5

Banerjee, P., Wei, K. K., & Ma, L. (2012). Role of trialability in B2B e-business adoption: Theoretical insights from two case studies. *Behaviour and Information Technology, 31*, 815–827. doi:10.1080/0144929X.2010.497564

Banerjee, T., & Sheth, A. (2017). IoT quality control for data and application needs. *IEEE Intelligent Systems, 32*(2), 68–73. doi:10.1109/MIS.2017.35

Barga, R. (2016). Processing big data in motion. *2016 IEEE International Conference on Cloud Engineering (IC2E),* 171–171. doi:10.1109/ic2e.2016.52

Barkhordari-Sharifabad, M., Ashktorab, T., & Atashzadeh-Shoorideh, F. (2018). Ethical leadership outcomes in nursing: A qualitative study. *Nursing Ethics, 25*(8), 1051–1063. doi:10.1177/0969733016687157

Bennati, S., & Pournaras, E. (2018). Privacy-enhancing aggregation of Internet of Things data via sensors grouping. *Sustainable Cities and Society, 39*, 387–400. doi:10.1016/j.scs.2018.02.013

Bertino, E., & Islam, N. (2017). Botnets and Internet of Things security. *Computer*, *50*(2), 76-79. doi:10.1109/MC.2017.62

Billet, B., & Erie, V. A. L. (2017). SPINEL: An opportunistic proxy for connecting sensors. *ACM Transactions on Internet Technology, 17*(2), 1–21. doi:10.1145/3041025

Billingsley, L. (2019). Cybersmart: Protect the patient, protect the data. *Journal of Radiology Nursing*, *38*(4), 261–263. doi:10.1016/j.jradnu.2019.09.010

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation*? Qualitative Health Research, 26*, 1802–1811. doi:10.1177/1049732316654870

Boeren, E. (2018). The methodological underdog: *A Review of Quantitative Research in the Key Adult Education Journals. Adult Education Quarterly*, *68*(1), 63-79. doi:10.1177/0741713617739347

Boit, C. (2017). Technologies for heterogeneous integration—Challenges and chances for fault isolation*. Microelectronics Reliability, 76–77*, 184–187. doi:10.1016/j.microrel.2017.06.071

Bonafini, F., Rinaldi, S., Depari, A., Flammini, A., Ferrari, P., & Sisinni, E. (2019). Cluster of IoT sensors for smart cities: Impact of the communication infrastructure over computational performance. *2019 IEEE Sensors Applications Symposium, Conference Proceedings*, pp. 1–6. doi:10.1109/SAS.2019.8706079

Bosunia, M. R., Hasan, K., Nasir, N. A., Kwon, S., & Jeong, S. H. (2016). Efficient data delivery based on content-centric networking for Internet of Things applications. *International Journal of Distributed Sensor Networks, 12*(8). doi:10.1177/1550147716665518

Brear, M. (2019). Process and outcomes of a recursive, dialogic member checking approach: A project ethnography. *Qualitative Health Research*, *29*(7), 944–957. doi:10.1177/1049732318812448

Bregon, A., Alonso-González, C. J., & Pulido, B. (2014). Integration of simulation and state observers for online fault detection of nonlinear continuous systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 44*(12), 1553–1568. doi:10.1109/TSMC.2014.2322581

Brooks, L., & Alam, M. S. (2015). Designing an information system for updating land records in Bangladesh: Action design ethnographic research (ADER). *IFIP Advances in Information and Communication Technology, 402*, 359–374. doi:10.1007/978-3-642-38862-0_22

Byrne, D. (2015). Response to Fugard and Potts: supporting thinking on sample sizes for thematic analyses: A quantitative tool. *International Journal of Social Research Methodology, 18*(6), 689–691. doi:10.1080/13645579.2015.1005455

Byun, S. S.-E. (2011). Exploring perceptions toward biometric technology in service encounters: a comparison of current users and potential adopters. *Behaviour & Information Technology*, *32*(3), 1–14. doi:10.1080/0144929X.2011.553741

Cangea, O. (2019). A comparative analysis of Internet of Things security strategies. *Gaze Din Ploiesti*, *71*, 1–10. Retrieved from https://upg-bulletin-se.ro/

Carella, A., Kotsoev, M., & Truta, T. M. (2017). Impact of security awareness training on phishing click-through rates. *Proceedings—2017 IEEE International Conference on Big Data*, pp. 4458–4466. doi:10.1109/BigData.2017.8258485

Casey, D., & Murphy, K. (2009). Issues in using methodological triangulation in research. *Nurse Researcher*, *16*(4), 40–55. doi:10.7748/nr2009.07.16.4.40.c7160

Casoni, M., Grazia, C. A., & Klapez, M. (2017). SDN-based resource pooling to provide transparent multi-path communications. *IEEE Communications Magazine, 55*(12), 172–178. doi:10.1109/MCOM.2017.1601214

Castaño, F., Beruvides, G., Villalonga, A., & Haber, R. E. (2018). Self-tuning method for increased obstacle detection reliability based on Internet of Things LiDAR sensor models. *Sensors*, *18*(5), 1–17. doi:10.3390/s18051508

Castillo-Montoya, M. (2016). The qualitative report preparing for interview research: The interview protocol refinement framework. *Qualitative Report*, *21*, 811–831. Retrieved from https://nsuworks.nova.edu/tqr

Chaturvedi, K., Matheus, A., Nguyen, S. H., & Kolbe, T. H. (2019). Securing spatial data infrastructures for distributed smart city applications and services. *Future Generation Computer Systems*, *101*, 723–736. doi:10.1016/j.future.2019.07.002

Chen, C. K., Zhang, Z. K., Lee, S. H., & Shieh, S. (2018). Penetration testing in the IoT age. *Computer, 51*(4), 82–85. doi:10.1109/MC.2018.2141033

Chen, H., Wu, C., Huang, W., Wu, Y., & Xiong, N. (2018). Design and application of system with dual-control of water and electricity based on wireless sensor network and video recognition technology. *International Journal of Distributed Sensor Networks, 14*(9). doi:10.1177/1550147718795951

Chen, J., & Zhu, Q. (2019). Interdependent strategic security risk management with bounded rationality in the Internet of Things. *IEEE Transactions on Information Forensics and Security, 14*, 2958–2971. doi:10.1109/TIFS.2019.2911112

Chen, Y., López, L., Martínez, J.-F., & Castillejo, P. (2018). A lightweight privacy protection user authentication and key agreement scheme tailored for the Internet of Things environment: LightPriAuth. *Journal of Sensors, 2018,* 1–16. doi:10.1155/2018/7574238

Cheng, H. H. (2017). The antecedents of creative article diffusion on blogs: Integrating innovation diffusion theory and social network theory. *Online Information Review, 41*(1), 70–84. doi:10.1108/OIR-07-2015-0221

Cheng, Y.-M. (2015). Towards an understanding of the factors affecting m-learning acceptance: roles of technological characteristics and compatibility. *Asia Pacific Management Review, 20,* 109–119.

Chervyakov, N., Babenko, M., Tchernykh, A., Kucherov, N., Miranda-López, V., & Cortés-Mendoza, J. M. (2017). AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security. *Future Generation Computer Systems, 92,* 1080–1092. doi:10.1016/j.future.2017.09.061

Chipidza, W., Green, G., & Riemenschneider, C. (2019). Why do students not major in MIS? An application of the theory of planned behavior. *Journal of Information Systems Education, 30*, 111–127.

Choi, J., Nazareth, D. L., & Ngo-Ye, T. L. (2018). The effect of innovation characteristics on cloud computing diffusion. *Journal of Computer Information Systems*, *58*, 325–333. doi:10.1080/08874417.2016.1261377

Choi, S. K., Yang, C. H., & Kwak, J. (2018). System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats. *KSII Transactions on Internet and Information Systems*, *12*, 906–918. doi:10.3837/tiis.2018.02.022

Chong, I., Xiong, A., & Proctor, R. W. (2019). Human factors in the privacy and security of the Internet of Things. *Ergonomics in Design*, *27*(3), 5–10. doi:10.1177/1064804617750321

Chpa, J. M. W. (2015). Budget reductions vs. loss of security training. *Journal of Healthcare Protection Management, 31*(2), 91–98. Retrieved from https://www.iahss.org/page/Journal?

Christenson, J. D., & Gutierrez, D. M. (2016). Using qualitative, quantitative, and mixed methods research to promote family therapy with adolescents in residential settings. *Contemporary Family Therapy*, *38*, 52–61. doi:10.1007/s10591-016-9374-x

Chu, H., & Ke, Q. (2017). Research methods: What's in the name? *Library and Information Science Research, 39*(4), 284–294. doi:10.1016/j.lisr.2017.11.001

Clandinin, D. J., Cave, M. T., & Berendonk, C. (2017). Narrative inquiry: A relational research methodology for medical education. *Medical Education, 51*, 89–96. doi:10.1111/medu.13136

Condry, M. W., & Nelson, C. B. (2016). Using smart edge IoT devices for safer, rapid response with industry IoT control operations. *Proceedings of the IEEE, 104*(5), 938–946. doi:10.1109/JPROC.2015.2513672

Connelly, L. M. (2016). Trustworthiness in Qualitative Research. *Medsurg Nursing, 25*(6), 435–437. Retrieved from http://www.medsurgnursing.net/cgi-bin/WebObjects/MSNJournal.woa

Constantinou, C. S., Georgiou, M., & Perdikogianni, M. (2017). A comparative method for themes saturation (CoMeTS) in qualitative interviews. *Qualitative Research, 17*(5), 571–588. doi:10.1177/1468794116686650

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*, 544–546. doi:10.1016/j.future.2017.07.060

Corneille, M., Carter, L., Hall-Byers, N. M., Clark, T., & Younge, S. (2014). Exploring user acceptance of a text-message based health intervention. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2759–2767. doi:10.1109/HICSS.2014.346

Cornel, C.-E. (2015). The role of Internet of Things for a continuous improvement in education. *Hyperion Economic Journal Year III, 2*(3), 24-31. Retrieved from http://www.idc.com

Coursaris, C. K., Van Osch, W., & Sung, J. (2013a). A “cloud lifestyle”: The diffusion of cloud computing applications and the effect of demographic and lifestyle clusters. *Proceedings of the Annual Hawaii International Conference on System Sciences,* pp. 2803–2812. doi:10.1109/HICSS.2013.2

Crane, S., & Broome, M. E. (2017). Understanding ethical issues of research participation from the perspective of participating children and adolescents: A systematic review. *Worldviews on Evidence-Based Nursing*, *14*(3), 200–209. doi:10.1111/wvn.12209

Cristian, S., Grigorescu, O., Deaconescu, R., & Mihnea, C. (2018). Why IoT security is failing: The need for a test-driven security approach. In *2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1-6 doi:10.1109/ROEDUNET.2018.8514135

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher*, *21*(5), 19–27. doi:10.7748/nr.21.5.19.e1240

Curran, D., Kekewich, M., & Foreman, T. (2019). Examining the use of consent forms to promote dissemination of research results to participants. *Research Ethics*, *15*(1), 1–28. doi:10.1177/1747016118798877

Dai, W., Chi, Y., Lu, Z., Wang, M., & Zhao, Y. (2018). Research on reliability assessment of mechanical equipment based on the performance–feature model. *Applied Sciences, 8*(9), 1619. doi:10.3390/app8091619

Dan, V., Osterheider, A., & Raupp, J. (2019). The diffusion of innovations in agricultural circles: An explorative study on alternative antimicrobial agents. *Science Communication, 41*(1), 3–37. doi:10.1177/1075547018819159

Das, A., Degeling, M., Smullen, D., & Sadeh, N. (2018). Personalized privacy assistants for the internet of things: Providing users with notice and choice. *IEEE Pervasive Computing, 17*(3), 35–46. doi:10.1109/MPRV.2018.03367733

Dasaklis, T., & Casino, F. (2019). Improving vendor-managed inventory strategy based on Internet of Things (IoT) applications and blockchain technology. *IEEE International Conference on Blockchain and Cryptocurrency,* 50–55. doi:10.1109/BLOC.2019.8751478

Davis, D., LeBeau, J., Brooks, S., & Brown, S. (2014). Adoption of technological innovations: A Case Study of the ASSESS website. *Advances in Engineering Education, 4*, 1–25. Retrieved from https://advances.asee.org/

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340. doi:10.2307/249008

Dearing, J. W. (2008). Evolution of diffusion and dissemination theory. *Journal of Public Health Management and Practice, 14*(2), 99–108. doi:10.1097/01.PHH.0000311886.98627.b7

De Cremer, D., Nguyen, B., & Simkin, L. (2017). The integrity challenge of the Internet-of-Things (IoT): On understanding its dark side. *Journal of Marketing Management, 33*, 145–158. doi:10.1080/0267257X.2016.1247517

DeGarmo, M. J. (2012). The diffusion of innovation among United States policing jurisdictions: A cautionary tale for theorists and researchers. *International Journal of Criminal Justice Sciences, 7*(1), 450–465. Retrieved from http://www.sascv.org/ijcjs/

Değerli, A., Aytekin, Ç., & Değerli, B. (2015). Analyzing information technology status and networked readiness index in context of diffusion of innovations theory. *Procedia Social and Behavioral Sciences, 195*, 1553–1562. doi:10.1016/j.sbspro.2015.06.190

Deif, D., & Gadallah, Y. (2017). A comprehensive wireless sensor network reliability metric for critical Internet of Things applications. *Eurasip Journal on Wireless Communications and Networking, 2017, 145*. doi:10.1186/s13638-017-0930-3

Delgado, J., Llorente, S., & Naro, D. (2017). Protecting privacy of genomic information. *Studies in Health Technology and Informatics, 235*, 318–322. doi:10.3233/978-1-61499-753-5-318

Derrick, J. L., Eliseo-Arras, R. K., Hanny, C., Britton, M., & Haddad, S. (2017). Comparison of internet and mailing methods to recruit couples into research on unaided smoking cessation. *Addictive Behaviors, 75*, 12–16. doi:10.1016/j.addbeh.2017.06.012

Deslonde, V., & Becerra, M. (2019). The technology acceptance model (TAM): Exploring school counselors' acceptance and use of Naviance. *Professional Counselor, 8*(4), 369–382. doi:10.15241/vd.8.4.369

Dierickx, S., Balen, J., Longman, C., Rahbari, L., Clarke, E., Jarju, B., & Coene, G. (2019). "We are always desperate and will try anything to conceive": The convoluted and dynamic process of health seeking among women with infertility in the West Coast Region of The Gambia. *PLoS ONE, 14*, 1–21. doi:10.1371/journal.pone.0211634

Dintoe, S. S. (2018). Educational technology adopters: A case study in University of Botswana. *International Journal of Education and Development Using Information and Communication Technology, 14*, 52–90. Retrieved from http://ijedict.dec.uwi.edu/

Dong, C., Chen, J., Guo, W., & Zou, J. (2019). A machine-learning-based hardware-Trojan detection approach for chips in the Internet of Things. *International Journal of Distributed Sensor Networks, 15*(12), 1-14. doi:10.1177/1550147719888098

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops* (pp. 618–623). IEEE. doi:10.1109/PERCOMW.2017.7917634

Doyle, G., & Budz, B. (2016). Diffusing innovations in nursing education: From PDAs to OERs. *Studies in Health Technology and Informatics*, *225*, 981–982. doi:10.3233/978-1-61499-658-3-981

Drira, K. (2017). Multiscale and multiobjective modelling: A perspective for mastering the design and operation complexity of IoT systems. 2017. *Proceedings of the 40th International Convention on Information and Communication Technology, Electronics and Microelectronics*, pp. 555–557. doi:10.23919/MIPRO.2017.7973487

Drubin, C. (2016). IoT partner programs expand to combat ecosystem complexity.

Dunne, S. (2016). How do they research? An ethnographic study of final year undergraduate research behavior in an Irish university. *New Review of Academic Librarianship, 22*, 410–429. doi:10.1080/13614533.2016.1168747

Dutta, S., & Omolayole, O. (2016). Are there differences between men and women in information technology innovation adoption behaviors: A theoretical study. *Journal of Business Diversity*, *16*, 106–114. Retrieved from https://articlegateway.com/index.php/JBD/index

Dwomoh, G. (2015). The relationship between businesses' acquired knowledge, skills, abilities (SKAs) and shareholders wealth maximization: The mediating role of training investment. *Journal of Investment and Management, 4*, 171–176. doi:10.11648/j.jim.20150405.15

Eatough, V., & Shaw, K. (2017). 'I'm worried about getting water in the holes in my head': A phenomenological psychology case study of the experience of undergoing deep brain stimulation surgery for Parkinson’s disease. *British Journal of Health Psychology, 22,* 94–109. doi:10.1111/bjhp.12219

Ellis, P. (2018). The language of research (Part 19): Understanding the quality of a qualitative paper. *Wounds UK, 14*(5), 134–135. Retrieved from https://www.wounds-uk.com/

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology, 6,* 323–337. Retrieved from http://iisit.org/

Ellram, L. M., & Tate, W. L. (2016). The use of secondary data in purchasing and supply management (P/SM) research. *Journal of Purchasing and Supply Management, 22*(4), 250–254. doi:10.1016/j.pursup.2016.08.005

Elsaadany, A., & Soliman, M. (2017). Experimental evaluation of Internet of Things in the educational environment. *International Journal of Engineering Pedagogy, 7*(3), 50. doi:10.3991/ijep.v7i3.7187

Evangelinou-Yiannakis, A. (2017). A reflection on the methodology used for a qualitative longitudinal study. *Issues in Educational Research, 27*, 269–284.

Evon, D. M., Golin, C. E., Ruffin, R., & Fried, M. W. (2017). Development and pilot-testing of a cognitive behavioral coping skills group intervention for patients with chronic hepatitis C. *Contemporary Clinical Trials Communications*, *6,* 85–96. doi:10.1016/j.conctc.2017.03.008

Farhan, M., Jabbar, S., Aslam, M., Ahmad, A., Iqbal, M. M., Khan, M., & Maria, M. E. A. (2018). A real-time data mining approach for interaction analytics assessment:

IoT based student interaction framework. *International Journal of Parallel Programming, 46,* 886–903. doi:10.1007/s10766-017-0553-7

Fawaz, K., & Shin, K. G. (2016). Security and privacy in the Internet of Things. In *Internet of Things: Principles and paradigms* (pp. 183–200). doi:10.1016/B978-0-12-805395-9.00010-1

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2019). Towards next generation teaching, learning, and context-aware applications for higher education: A review on blockchain, IoT, Fog and edge computing enabled smart campuses and universities. *Applied Sciences, 9*(21). doi:10.3390/app9214479

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in Pharmacy Teaching and Learning, 11*, 211–217. doi:10.1016/j.cptl.2018.11.014

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61*, 169–183. doi:10.1016/j.cose.2016.06.002

Flynn, S. V., & Korcuska, J. S. (2018). Credible phenomenological research: A mixed-methods study. *Counselor Education and Supervision, 57,* 34–50. doi:10.1002/ceas.12092

Freund, J., Fritts, S., & Marius, J. (2016). Using data breach reports to assess risk analysis quality. *ISSA Journal*, 19–24. Retrieved from https://www.issa.org/journal/

Fu, K., & Xu, W. (2018). Risks of trusting the physics of sensors. *Communications of the ACM, 61*(2), 20–23. doi:10.1145/3176402

Fu, Y., Wang, H., Xu, K., Mi, H., & Wang, Y. (2019). Mixup based privacy preserving mixed collaboration learning. *Proceedings—13th IEEE International Conference on Service-Oriented System Engineering, 10th International Workshop on Joint Cloud Computing, and 2019 IEEE International Workshop on Cloud Computing in Robotic Systems,* pp. 275–280. doi:10.1109/SOSE.2019.00047

Fuchs, K. L., Haldimann, M., Vuckovac, D., & Ilic, A. (2018). Automation of data collection techniques for recording food intake: A review of publicly available and well-adopted diet apps. *9th International Conference on Information and Communication Technology Convergence: ICT Convergence Powered by Smart Intelligence, ICTC 2018,* 58–65. doi:10.1109/ICTC.2018.8539468

Galembeck, E. (2017). The Internet of Things, mobile devices and the promising future for science education. *Revista de Ensino de Bioquímica, 15*, 224. doi:10.16923/reb.v15i0.776

Galinina, O., Andreev, S., Komarov, M., & Maltseva, S. (2017). Leveraging heterogeneous device connectivity in a converged 5G-IoT ecosystem. *Computer Networks, 128*(2017), 123–132. doi:10.1016/j.comnet.2017.04.051

Ganglmair-Wooliscroft, A., & Wooliscroft, B. (2016). Diffusion of innovation: The case of ethical tourism behavior. *Journal of Business Research, 69,* 2711–2720. doi:10.1016/j.jbusres.2015.11.006

Garg, R. (2018). Open data privacy and security policy issues and its influence on embracing the Internet of Things. *First Monday, 23*(5), 1. Retrieved from https://firstmonday.org/ojs/index.php/fm/issue/view/682

Ge, M., Hong, J. B., Guttmann, W., & Kim, D. S. (2017). A framework for automating security analysis of the internet of things. *Journal of Network and Computer Applications***,** *83*, 12-27. doi:10.1016/j.jnca.2017.01.033

Georgakopoulos, D., Jayaraman, P. P., Fazia, M., Villari, M., & Ranjan, R. (2016). Internet of Things and edge cloud computing roadmap for manufacturing. *IEEE Cloud Computing, 3*(4), 66–73. doi:10.1109/MCC.2016.91

George, G., & Thampi, S. M. (2019). Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things. *Pervasive and Mobile Computing*, *59*, 101068. doi:10.1016/j.pmcj.2019.101068

Georgescu, M., & Popescu, D. (2015). How could Internet of Things change the e-learning environment. *The International Scientific Conference eLearning and Software for Education,* 1, 68–71. doi:10.12753/2066-026X-15-009

Ghafir, I., Prenosil, V., Alhejailan, A., & Hammoudeh, M. (2016). Social engineering attack strategies and defence approaches. *Proceedings—2016 IEEE 4th International Conference on Future Internet of Things and Cloud,* pp. 145–149. doi:10.1109/FiCloud.2016.28

Gibson, R., Sampalli, T., Lawson, B., Burge, F., Wood, S., & Warner, G. (2018). Applying the consolidated framework for implementation research to identify barriers affecting implementation of an online frailty tool into primary health care: A qualitative study. *BMC Health Services Research, 18,* 1–12. doi:10.1186/s12913-018-3163-1

Girma, A. (2018). Analysis of security vulnerability and analytics of Internet of Things (IOT) platform. In *Advances in intelligent systems and computing, 738,* 101-104. doi:10.1007/978-3-319-77028-4_16

Given, L. M., & Olson, H. A. (2003). Knowledge organization in research: A conceptual model for organizing data. *Library and Information Science Research, 25*(2), 157–176. doi:10.1016/S0740-8188(03)00005-7

Goduscheit, R. C., & Knudsen, M. P. (2015). How barriers to collaboration prevent progress in demand for knowledge: A dyadic study of small and medium-sized firms, research and technology organizations and universities. *Creativity and Innovation Management, 24,* 29–54. doi:10.1111/caim.12101

Gokceli, S., Zhmurov, N., Kurt, G. K., & Ors, B. (2017). IoT in action: Design and implementation of a building evacuation service. *Journal of Computer Networks and Communications*, *2017*. doi:10.1155/2017/8595404

Granjal, J., Monteiro, E., & Sa Silva, J. (2015). Security for the Internet of Things: A survey of existing protocols and open research issues. *IEEE Communications Surveys and Tutorials, 17*, 1294–1312. doi:10.1109/COMST.2015.2388550

Greig, A., Renaud, K., & Flowerday, S. (2015). An ethnographic study to assess the enactment of information security culture in a retail store. *2015 World Congress on Internet Security,* 61–66. doi:10.1109/WorldCIS.2015.7359415

Guan, W. (2018). Reliability analysis of the Internet of Things based on ordered binary decision diagram. *International Journal of Online Engineering, 14*(8), 20–34. doi:10.3991/ijoe.v14i08.9185

Guillemin, M., Barnard, E., Allen, A., Stewart, P., Walker, H., Rosenthal, D., & Gillam, L. (2018). Do research participants trust researchers or their institution? *Journal of Empirical Research on Human Research Ethics, 13*, 285–294. doi:10.1177/1556264618763253

Guo, J.-H. (2018). Applications of the Internet of Things technology in advanced planning systems. *Sensors and Materials*, *30*(8), 1723. doi:10.18494/SAM.2018.1874

Guo, M., Huang, Y., Guan, Q., Xie, Z., & Wu, L. (2017). An efficient data organization and scheduling strategy for accelerating large vector data rendering. *Transactions in GIS, 21*, 1217–1236. doi:10.1111/tgis.12275

Haddud, A., DeSouza, A., Khare, A., & Lee, H. (2017). Examining potential benefits and challenges associated with the Internet of Things integration in supply chains. *Journal of Manufacturing Technology Management, 28*, 1055–1085. doi:10.1108/JMTM-05-2017-0094

Haegele, J. A., & Hodge, S. R. (2015). Quantitative methodology: A guide for emerging physical education and adapted physical education researchers. *Physical Educator*, *72*(2012), 59–75. doi:10.18666/tpe-2015-v72-i5-6133

Hagen, C. (2014). Eleed, e-learning & education. *E-learning and Education*, *1*(10). Retrieved from https://eleed.campussource.de/

Hameed, K., Khan, A., Ahmed, M., Reddy, A. G., & Rathore, M. M. (2018). Towards a formally verified zero watermarking scheme for data integrity in the Internet of

Things based-wireless sensor networks. *Future Generation Computer Systems, 82*, 274–289. doi:10.1016/j.future.2017.12.009

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of trust: A decentralized blockchain-based authentication system for IoT. *Computers and Security*, *78*, 126-142. doi:10.1016/j.cose.2018.06.004

Hart, J., & Sutcliffe, A. (2019). Is it all about the apps or the device? User experience and technology acceptance among iPad users. *International Journal of Human Computer Studies*, *130*, 93–112. doi:10.1016/j.ijhcs.2019.05.002

Haven, T. L., & Van Grootel, L. (2019). Preregistering qualitative research. *Accountability in Research, 26*(3), 1–16. doi:10.1080/08989621.2019.1580147

Hayes, K. J., Eljiz, K., Dadich, A., Fitzgerald, J. A., & Sloan, T. (2015). Trialability, observability and risk reduction accelerating individual innovation adoption decisions. *Journal of Health, Organisation and Management, 29*, 271–294. doi:10.1108/JHOM-08-2013-0171

He, J., Lo, D. C. T., Xie, Y., & Lartigue, J. (2016). Integrating Internet of things (IoT) into STEM undergraduate education: Case study of a modern technology infused courseware for embedded system course. *Proceedings—Frontiers in Education Conference,* pp. 1–9. doi:10.1109/FIE.2016.7757458

He, Q., Xu, Y., Liu, Z., He, J., Sun, Y., & Zhang, R. (2018). A privacy-preserving Internet of Things device management scheme based on blockchain. *International Journal of Distributed Sensor Networks, 14*(11). doi:10.1177/1550147718808750

Helfgott, J. S. (2010). Understanding the US Food and Drug Administration's May 2007 guidance – 'Computerized Systems Used in Clinical Investigations.' *Drug Development, 5*(May 2007), 56–58.

Hernández-Ramos, J. L., Pérez, S., Hennebert, C., Bernabé, J. B., Denis, B., Macabies, A., & Skarmeta, A. F. (2018). Protecting personal data in IoT platform scenarios through encryption-based selective disclosure. *Computer Communications, 130,* 20–37. doi:10.1016/j.comcom.2018.08.010

Horkoff, J., Maiden, N. A., & Asboth, D. (2019). Creative goal modeling for innovative requirements. *Information and Software Technology, 106*, 85–100. doi:10.1016/j.infsof.2018.09.005

Hou, J., Qu, L., & Shi, W. (2018). A survey on Internet of Things security from data perspectives. *Computer Networks, 148*, 295–306. doi:10.1016/j.comnet.2018.11.026

Høyland, S., Hollund, J. G., & Olsen, O. E. (2015). Gaining access to a research site and participants in medical and nursing research: A synthesis of accounts. *Medical Education, 49*, 224–232. doi:10.1111/medu.12622

Hsu, C.-L., & Lin, J. C. C. (2016). Factors affecting the adoption of cloud services in enterprises. *Information Systems and E-Business Management, 14*, 791–822. doi:10.1007/s10257-015-0300-9

Hsu, C.-L., & Lin, J. C.-C. (2018). Exploring factors affecting the adoption of Internet of Things services. *Journal of Computer Information Systems, 58*, 49–57. doi:10.1080/08874417.2016.1186524

Hsu, L. (2016). Diffusion of innovation and use of technology in hospitality education: An empirical assessment with multilevel analyses of learning effectiveness. *Asia-Pacific Education Researcher, 25*, 135–145. doi:10.1007/s40299-015-0244-3

Huang, Q., Wang, L., & Yang, Y. (2018). DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices. *World Wide Web*, *21*(1), 151–167. doi:10.1007/s11280-017-0462-0

Hwang, G., Lee, J., Park, J., & Chang, T.-W. (2017). Developing performance measurement system for Internet of Things and smart factory environment. *International Journal of Production Research*, *559*, 2590–2602. doi:10.1080/00207543.2016.1245883

Hwang, Y. H. (2015). IoT security & privacy: Threats and challenges. *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security*. doi:10.1145/2732209.2732216

Iftene, A., & Trandabăț, D. (2018). Enhancing the attractiveness of learning through augmented reality. *Procedia Computer Science*, *126*, 166–175. doi:10.1016/j.procs.2018.07.220

Iivari, N. (2018). Using member checking in interpretive research practice: A hermeneutic analysis of informants’ interpretation of their organizational realities. *Information Technology and People, 31*, 111–133. doi:10.1108/ITP-07-2016-0168

Iles, I. A., Egnoto, M. J., Fisher Liu, B., Ackerman, G., Roberts, H., & Smith, D. (2017). Understanding the adoption process of national security technology: An integration of diffusion of innovations and volitional behavior theories. *Risk Analysis, 37,* 2246–2259. doi:10.1111/risa.12771

Ilie-Zudor, E., Kemény, Z., & Preuveneers, D. (2016). Efficiency and security of process transparency in production networks—A view of expectations, obstacles and potentials. *Procedia CIRP, 52,* 84–89. doi:10.1016/j.procir.2016.07.018

Im, I., Kim, Y., Oommen, E., Kim, H., & Ko, M. H. (2012). The effects of bolus consistency in pharyngeal transit duration during normal swallowing. *Annals of Rehabilitation Medicine, 36*, 220–225. doi:10.5535/arm.2012.36.2.220

Inoue, S., & Nohara, Y. (2009). On the observability of RFID data privacy. *Proceedings of the 2009 2nd International Conference on Computer Science and Its Applications, CSA 2009,* 1–5. doi:10.1109/CSA.2009.5404178

Irani, Z., Weerakkody, V., Dwivedi, Y. K., Sivarajah, U., & Kapoor, K. (2016). Open data and its usability: an empirical view from the citizen's perspective. *Information Systems Frontiers, 19*, 285–300. doi:10.1007/s10796-016-9679-1

Jang, I., Lee, D., Choi, J., & Son, Y. (2019). An approach to share self-taught knowledge between home IoT devices at the edge. *Sensors, 19*(4). doi:10.3390/s19040833

Javaid, N., Sher, A., Nasir, H., & Guizani, N. (2018). Intelligence in IoT-based 5G networks: Opportunities and challenges. *IEEE Communications Magazine, 56*(10), 94–100. doi:10.1109/MCOM.2018.1800036

Jesus, E. F., Chicarino, V. R. L., De Albuquerque, C. V. N., & Rocha, A. A. D. A. (2018). A survey of how to use blockchain to secure Internet of Things and the stalker attack. *Security and Communication Networks, 2018*. doi:10.1155/2018/9675050

Jia, G., Zhu, Y., Li, Y., Zhu, Z., & Zhou, L. (2019). Analysis of the effect of the reliability of the NB-Iot network on the intelligent system. *IEEE Access*, *7*, 112809–112820. doi:10.1109/access.2019.2932870

Jiang, H., Shen, F., Chen, S., Li, K. C., & Jeong, Y. S. (2015). A secure and scalable storage system for aggregate data in IoT. *Future Generation Computer Systems, 49*, 133–141. doi:10.1016/j.future.2014.11.009

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-payment services. *Computers in Human Behavior, 79*, 111–122. doi:10.1016/j.chb.2017.10.035

Jose, D. V., & Vijyalakshmi, A. (2018). An overview of security in Internet of Things. *Procedia Computer Science, 143*, 744–748. doi:10.1016/j.procs.2018.10.439

Journot, V., Perusat-Villetorte, S., Bouyssou, C., Couffin-Cadiergues, S., Tall, A., Fagard, C., & Chene, G. (2013). Preserving participant anonymity during remote preenrollment consent form checking. *Clinical Trials, 10*(3), 460–462. doi:10.1177/1740774513480962

Jwaifell, M., & Gasaymeh, A. (2013). Using the diffusion of innovation theory to explain the degree of English teachers’ adoption of interactive whiteboards in the modern systems school in Jordan: A case study. *Contemporary Educational Technology, 4*(2), 138–149. doi:10.30935/cedtech/6098

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing, 72*, 2954–2965. doi:10.1111/jan.13031

Kalyani, G., Rao, M. V. P. C. S., & Janakiramaiah, B. (2018). Privacy-preserving classification rule mining for balancing data utility and knowledge privacy using adapted binary firefly algorithm. *Arabian Journal for Science and Engineering, 43*, 3903–3925. doi:10.1007/s13369-017-2693-x

Kamin, D. A. (2017). Abstract exploring security, privacy, and reliability strategies to enable the adoption of IoT. *Walden University*. Retrieved from https://waldenu.edu/

Kamyod, C. (2018). End-to-end reliability analysis of an IoT based smart agriculture. *3rd International Conference on Digital Arts, Media and Technology, ICDAMT 2018*, 258–261. doi:10.1109/ICDAMT.2018.8376535

Kang, B., Han, Y., Qian, K., & Du, J. (2020). Analysis and improvement on an authentication protocol for IoT-enabled devices in distributed cloud computing environment. *Mathematical Problems in Engineering, 2020*, 1-6. doi:10.1155/2020/1970798

Kao, Y. S., Nawata, K., & Huang, C. Y. (2019). Evaluating the performance of systemic innovation problems of the IoT in manufacturing industries by novel MCDM methods. *Sustainability, 11*(18), 1–33. doi:10.3390/su11184970

Kapoor, K. K., Dwivedi, Y. K., & Williams, M. D. (2014). Rogers' innovation adoption attributes: A systematic review and synthesis of existing research. *Information Systems Management, 31*, 74–91. doi:10.1080/10580530.2014.854103

Karagiozis, N. (2018). The complexities of the researcher's role in qualitative research: The power of reflexivity. *International Journal of Interdisciplinary Educational Studies, 13*, 19–31. doi:10.18848/2327-011x/cgp/v13i01/19-31

Karahoca, A., Karahoca, D., & Aksöz, M. (2018). Examining intention to adopt to internet of things in healthcare technology products. *Kybernetes, 47*, 742–770. doi:10.1108/K-02-2017-0045

Kasperavičiūtė-Černiauskienė, R., & Serafinas, D. (2018). The adoption of ISO 9001 standard within higher education institutions in Lithuania: Innovation diffusion approach. *Total Quality Management and Business Excellence, 29,* 74–93. doi:10.1080/14783363.2016.1164012

Kassab, M., Defranco, J. F., & Voas, J. (2018). Smarter education. *IT Professional, 20*(5), 20–24. doi:10.1109/MITP.2018.053891333

Kawar, L. N., Pugh, D. M., & Scruth, E. A. (2016). Understanding the role and legal requirements of the institutional review board. *Clinical Nurse Specialist, 30*(3), 137–140. doi:10.1097/nur.0000000000000197

Keller, A., Aguilar, A., & Hanss, D. (2018). Car sharers' interest in integrated multimodal mobility platforms: A diffusion of innovations perspective. *Sustainability, 10*(12), 4689. doi:10.3390/su10124689

Kendall, K. (2014). JAN Forum. *Journal of Advanced Nursing, 70,* 238. doi:10.1111/jan.12146

Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the Internet of Things: A standardization perspective. *IEEE Internet of Things Journal*, *1*(3), 265-275. doi:10.1109/JIOT.2014.2323395

Kevin, C. R., & Vealé, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology, 89,* 482–486. Retrieved from http://www.radiologictechnology.org/

Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems, 82*, 395-411. doi:10.1016/j.future.2017.11.022

Khan, P. W., & Byun, Y. (2020). A blockchain-based secure image encryption scheme for the industrial internet of things. *Entropy*, *22*(2). doi:10.3390/e22020175

Khan, S. N. (2014). Qualitative research method—Phenomenology. *Asian Social Science, 10*(21), 298–310. doi:10.5539/ass.v10n21p298

Kiernan, M., Oppezzo, M. A., Resnicow, K., & Alexander, G. L. (2018). Effects of a methodological infographic on research participants' knowledge, transparency, and trust. *Health Psychology, 37,* 782–786. doi:10.1037/hea0000631

Kılınç, H., & Fırat, M. (2017). Opinions of expert academicians on online data collection and voluntary participation in social sciences research. *Kuram ve Uygulamada Egitim Bilimleri*, *17,* 1461–1486. doi:10.12738/estp.2017.5.0261

Kim, D. J., Hebeler, J., Yoon, V., & Davis, F. (2018). Exploring determinants of semantic web technology adoption from IT professionals' perspective: Industry competition, organization innovativeness, and data management capability. *Computers in Human Behavior, 86*, 18–33. doi:10.1016/j.chb.2018.04.014

Kim, H., & Lee, E. A. (2017). Authentication and authorization for the Internet of Things. *IT Professional*, *19*(5), 27–33. doi:10.1109/MITP.2017.3680960

King, J., & Awad, A. I. (2016). A distributed security mechanism for resource-constrained IoT devices. *Informatica, 40*, 133–143. Retrieved from http://www.informatica.si/index.php/informatica

Kirtley, B. J., & Memmel, S. (2018). Too Smart for Its Own Good: Challenges of the Internet of Things. *Journal of Internet Law, 22*(4), 18-30.

Kiryakova, G., Yordanova, L., & Angelova, N. (2017). Can we make schools and universities smarter with the Internet of Things? *TEM Journal, 6*, 80–84. doi:10.18421/TEM61-11

Ko, M., Wagner, L., & Spetz, J. (2018). Nursing home implementation of health information technology: Review of the literature finds inadequate investment in preparation, infrastructure, and training. *Inquiry*, *55*, 1-9. doi:10.1177/0046958018778902

Kolomvatsos, K. (2019). A distributed, proactive intelligent scheme for securing quality in large scale data processing. *Computing, 101*, 1687–1710. doi:10.1007/s00607-018-0683-9

Kolvereid, L., & Isaksen, E. (2006). New business start-up and subsequent entry into self-employment. *Journal of Business Venturing, 21*, 866–885. doi:10.1016/j.jbusvent.2005.06.008

Koniagina, M., Belotserkovich, D., & Vorona-slivinskaya, L. (2020). Development trends of an Internet of Things in context to information security policy of a person, business and the state. *Talent Development & Excellence, 12*, 1181–1193. Retrieved from https://iratde.com/index.php/jtde

Koo, C. J., & Kim, J. Y. (2018). Enforcing high-level security policies for Internet of Things. *Journal of Supercomputing, 74*, 4497–4505. doi:10.1007/s11227-017-2201-9

Koo, D., Shin, Y., Yun, J., & Hur, J. (2018). Improving security and reliability in Merkle tree-based online data authentication with leakage resilience. *Applied Sciences, 8*(12). doi:10.3390/app8122532

Koro-Ljungberg, M., Gemignani, M., Brodeur, C. W., & Kmiec, C. (2007). The technologies of normalization and self. *Qualitative Inquiry, 13*, 1075–1094. doi:10.1177/1077800407308822

Krause, M. S. (2016). Case sampling for psychotherapy practice, theory, and policy guidance: Qualities and quantities. *Psychotherapy Research, 26*, 530–544. doi:10.1080/10503307.2015.1051161

Kshetri, N. (2017). Blockchain’s roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy, 41*, 1027–1038. doi:10.1016/j.telpol.2017.09.003

Kumar, K. S., Rao, G. H., Sahoo, S., & Mahapatra, K. K. (2017). Secure split test techniques to prevent IC piracy for IoT devices. *Integration: The VLSI Journal*, *58*, 390–400. doi:10.1016/j.vlsi.2016.09.004

Lai, G., Zhang, Y., Tong, X., Li, K., & Ding, L. (2018). Research on automatic generation and data organization method of control points. *Proceedings—2018 10th IAPR Workshop on Pattern Recognition in Remote Sensing*, pp. 1–5.

Lamanna, T. J. (2019). On educating patrons on privacy and maximizing library resources. *Information Technology and Libraries, 38*(3), 4–7. doi:10.6017/ital.v38i3.11571

Laplante, P. A., Voas, J., & Laplante, N. (2016). Standards for the Internet of Things: A case study in disaster response. *Computer, 49*(5), 87–90. doi:10.1109/MC.2016.137

LeCroix, R. H., Goodrum, N. M., Hufstetler, S., & Armistead, L. P. (2017). Community data collection with children of mothers living with HIV: Boundaries of the researcher role. *American Journal of Community Psychology*, *60*, 368–374. doi:10.1002/ajcp.12193

Lee, C. C., Chen, S. D., Li, C. T., Cheng, C. L., & Lai, Y. M. (2019). Security enhancement on an RFID ownership transfer protocol based on cloud. *Future Generation Computer Systems*, *93*, 266–277. doi:10.1016/j.future.2018.10.040

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431-440. doi:10.1016/j.bushor.2015.03.008

Lee, Y., Kozar, K. A., & Larsen, K. R. T. (2018). The technology acceptance model: Past, present, and future. *Communications of the Association for Information Systems, 12*(December), 50. doi:10.17705/1cais.01250

Leiba, O., Bitton, R., Yitzchak, Y., Nadler, A., Kashi, D., & Shabtai, A. (2019). IoTPatchPool: Incentivized delivery network of IoT software updates based on proofs-of-distribution. *Pervasive and Mobile Computing, 58*, 101019. doi:10.1016/j.pmcj.2019.04.010

Lennvall, T., Gidlund, M., & Akerberg, J. (2017). Challenges when bringing IoT into industrial automation. *2017 IEEE AFRICON: Science, Technology and Innovation for Africa,* pp. 905–910. doi:10.1109/AFRCON.2017.8095602

Leon, N., Scheneider, H., & Daviaud, E. (2012). Applying a framework for assessing the health system challenges to scaling up mHealth in South Africa. *BMC Medical Informatics and Decision Making, 12*(1), 123. doi:10.1186/1472-6947-12-123

Le Roy, F., Robert, M., & Lasch, F. (2016). Choosing the best partner for product innovation. *International Studies of Management and Organization*, *46*, 136–158. doi:10.1080/00208825.2016.1112148

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care, 4*(3), 324. doi:10.4103/2249-4863.161306

Levitt, H. M., Motulsky, S. L., Wertz, F. J., Morrow, S. L., & Ponterotto, J. G. (2017). Recommendations for designing and reviewing qualitative research in psychology: Promoting methodological integrity. *Qualitative Psychology, 4*, 2–22. doi:10.1037/qup0000082

Leyva-Moral, J. M., & Feijoo-Cid, M. (2017). Participants’ safety versus confidentiality: A case study of HIV research. *Nursing Ethics, 24,* 376–380. doi:10.1177/0969733016669865

Li, C., & Palanisamy, B. (2019). Privacy in Internet of Things: From principles to technologies. *IEEE Internet of Things Journal*, *6*, 488–505. doi:10.1109/JIOT.2018.2864168

Li, J., Yan, Q., & Chang, V. (2018). Internet of Things: Security and privacy in a connected world. *Future Generation Computer Systems, 78,* 931–932. doi:10.1016/j.future.2017.09.017

Li, S., Tryfonas, T., & Li, H. (2016). The Internet of Things: A security point of view. *Internet Research, 26*(2), 337-359. doi:10.1108/IntR-07-2014-0173

Li, S., Xu, L. D., & Zhao, S. (2015). The Internet of Things: A survey. *Information Systems Frontiers*, *17*(2), 243-259 doi:10.1007/s10796-014-9492-7

Li, Z., Shahidehpour, M., & Liu, X. (2018). Cyber-secure decentralized energy management for IoT-enabled active distribution networks. *Journal of Modern Power Systems and Clean Energy, 6,* 900–917. doi:10.1007/s40565-018-0425-1

Liang, F., Hatcher, W. G., Liao, W., Gao, W., & Yu, W. (2019). Machine learning for security and the Internet of Things: The good, the bad, and the ugly. *IEEE Access, 7*, 158126–158147. doi:10.1109/ACCESS.2019.2948912

Liao, C., Huang, Y. J., & Hsieh, T. H. (2016). Factors influencing Internet banking adoption. *Social Behavior and Personality, 44*, 1443–1455. doi:10.2224/sbp.2016.44.9.1443

Liao, H., & Hitchcock, J. (2018). Reported credibility techniques in higher education evaluation studies that use qualitative methods: A research synthesis. *Evaluation and Program Planning, 68*, 157–165. doi:10.1016/j.evalprogplan.2018.03.005

Liu, S., Dibaei, M., Tai, Y., Chen, C., Zhang, J., & Xiang, Y. (2020). Cyber vulnerability intelligence for Internet of Things binary. *IEEE Transactions on Industrial Informatics, 16*, 2154–2163. doi:10.1109/TII.2019.2942800

Liu, Z., & Liu, J. (2019). Formal verification of blockchain smart contract based on colored petri net models. *2019 IEEE 43rd Annual Computer Software and Applications Conference*, *2*, 555–560. doi:10.1109/compsac.2019.10265

MacPhail, C., Khoza, N., Abler, L., & Ranganathan, M. (2016). Process guidelines for establishing intercoder reliability in qualitative studies. *Qualitative Research, 16,* 198–212. doi:10.1177/1468794115577012

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A literature review. *Journal of Computer and Communications, 3*(5), 164–173. doi:10.4236/jcc.2015.35021

Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2012). Identity authentication and capability based access control (IACAC) for the Internet of Things. *Journal of Cyber Security and Mobility, 1*(4), 309–348.

Makovhololo, M. L. (2018). Effects of GWEA implementation on ICT standardisation across SA government departments. *Proceedings—2018 Open Innovations Conference*, pp. 339–345. doi:10.1109/OI.2018.8535893

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample Size in Qualitative Interview Studies: Guided by Information Power. *Qualitative Health Research, 26*(13), 1753–1760. doi:10.1177/1049732315617444

Mamun, A. A. (2018). Diffusion of innovation among Malaysian manufacturing SMEs. *European Journal of Innovation Management*, *21*, 113–141. doi:10.1108/EJIM-02-2017-0017

Mangaya, B., Issa, S., & Chapter, M. (2018). A Data-Centric, Defense-in-Depth approach for securing the Internet of Things. *ISSA Journal*, *16*(6), 40–46.

Manky, D. (2017). Fortinet: 2017 marks tipping point for cybersecurity. *Network World Asia*, (November-December), 7. Retrieved from https://www.networksasia.net/

Mao, J., Zhu, S., & Liu, J. (2020). An inaudible voice attack to context-based device authentication in smart IoT systems. *Journal of Systems Architecture, 104*, 101696. doi:10.1016/j.sysarc.2019.101696

Mapande, F. V., Zuva, T., & Appiah, M. (2018). Users' perceptions on security of mobile computing for adoption of e-applications in South Africa. *Proceedings—2018 International Conference on Advances in Big Data, Computing and Data Communication Systems*, pp. 1–8. doi:10.1109/ICABCD.2018.8465127

Maras, M.-H. (2015). Internet of Things: Security and privacy implications. *International Data Privacy Law*, *5*(2), 99–104. doi:10.1093/idpl/ipv004

Martins, A., Pinheiro, M., Ferreira, A. F., Almeida, R., Matos, F., Oliveira, J., . . . Gamboa, H. (2018). Heterogeneous integration challenges within wafer level fan-out SiP for wearables and IoT. *Proceedings—Electronic Components and Technology Conference, 2018*, pp. 1485–1492. doi:10.1109/ECTC.2018.00226

Mataloto, B., Ferreira, J. C., & Cruz, N. (2019). LoBEMS—IoT for building and energy management systems. *Electronics*, *8*(7), 763. doi:10.3390/electronics8070763

Mavropoulos, O., Mouratidis, H., Fish, A., Panaousis, E., & Kalloniatis, C. (2017). A conceptual model to support analysis in the Internet of Things. *Computer Science & Information Systems, 14*, 557-578. doi:10.2298/CSIS160110016M

McCarthy, S., Fitzgerald, G., Forero, R., De Costa, J., Aboagye-Sarfo, P., Mohsin, M., . . . Nahidi, S. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research, 18*, 1–12. doi:10.1186/s12913-018-2915-2

Mcinnis, D., & Rodriguez, B. (2016). Tracking and interviewing family options study participants. *Cityscape: A Journal of Policy Development and Research, 18*(2), 201–220. Retrieved from https://www.huduser.gov/portal/home.html

Mcleod, A. (1994). Prospects of Internet of Things in Education System. *The CTE Journal, 3*(2), 32–43. Retrieved from https://www.thectejournal.com/

Mekonnen, F. A., Ambaw, Y. A., & Neri, G. T. (2018). Socio-economic determinants of anemia in pregnancy in North Shoa Zone, Ethiopia. *PLoS ONE, 13*(8), 1–10. doi:10.1371/journal.pone.0202734

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, *6*, 8182–8201. doi:10.1109/JIOT.2019.2935189

Menon, A. (2017). Smart cities, livable cities. *GfK Marketing Intelligence Review, 9*, 48–52. doi:10.1021/acs.jpclett.8b00044

Meredith, J. (2016). Transcribing screen-capture data: the process of developing a transcription system for multi-modal text-based data. *International Journal of Social Research Methodology, 19*, 663–676. doi:10.1080/13645579.2015.1082291

Metz, R. (2016). Finding insecurity in the Internet of Things. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/ *2*, 76.

Miloslavskaya, N., Nikiforov, A., & Budzko, V. (2018). Standardization of ensuring information security for big data technologies. *2018 6th International Conference on Future Internet of Things and Cloud Workshops*, pp. 56–63. doi:10.1109/W-FiCloud.2018.00015

Min, M., Anderson, J. A., & Chen, M. (2017). What do we know about full-service community schools? Integrative research review with NVivo. *School Community Journal*, *27*, 29–54. Retrieved from http://www.schoolcommunitynetwork.org/index.html

Mini, G. V., & Viji, K. S. A. (2017). A comprehensive cloud security model with enhanced key management, access control and data anonymization features.

International Journal of Communication Networks and Information Security, 9, 263–273. Retrieved from https://www.ijcnis.org/index.php/ijcnis

Miranda, J. A., Vaskova, A., Portela-Garcia, M., Garcia-Valderas, M., & Lopez-Ongil, C. (2017). On-line testing of sensor networks: A case study. *2017 IEEE 23rd International Symposium on On-Line Testing and Robust System Design*, pp. 201–202. doi:10.1109/IOLTS.2017.8046218

Mishra, N., Verma, L. P., Srivastava, P. K., & Gupta, A. (2018). An analysis of IoT congestion control policies. *Procedia Computer Science, 132*, 444–450. doi:10.1016/j.procs.2018.05.158

Moerman, G. (2017). *Qualitative research methods.* doi:10.1097/DCC.0000000000000322

Moghaddam, F. F., Wieder, P., & Yahyapour, R. (2016). Policy Engine as a Service (PEaaS): An approach to a reliable policy management framework in cloud computing environments. *Proceedings—2016 IEEE 4th International Conference on Future Internet of Things and Cloud*, pp. 139–144. doi:10.1109/FiCloud.2016.27

Mohamad, M. M., Sulaiman, N. L., Sern, L. C., & Salleh, K. M. (2015). Measuring the validity and reliability of research instruments. *Procedia Social and Behavioral Sciences, 204*, 164–171. doi:10.1016/j.sbspro.2015.08.129

Mokwena, S., & Hlebela, C. (2018). Factors affecting the adoption of Software as a Service in South African small medium enterprises. *2018 Open Innovations Conference*, pp. 134–139. doi:10.1109/OI.2018.8535714

Mollah, M. B., Azad, A. K., & Vasilakos, A. (2017). Secure data sharing and searching at the edge of cloud-assisted internet of things. *IEEE Cloud Computing, 4*, 34–42. doi:10.1109/MCC.2017.9

Montoya, J. S., & Kita, T. (2018). Exponential growth in product performance and its implications for disruptive innovation theory. *International Journal of Business and Information*, *13*, 1–36. doi:10.6702/ijbi.201803

Moon, M. D. (2019). Triangulation: A method to increase validity, reliability, and legitimation in clinical research. *Journal of Emergency Nursing, 45*, 103–105. doi:10.1016/j.jen.2018.11.004

Moore, R., & Burrus, J. (2019). Predicting STEM major and career intentions with the theory of planned behavior. *Career Development Quarterly*, *67*, 139–155. doi:10.1002/cdq.12177

Morrison, J. R., Reilly, J. M., & Ross, S. M. (2019). Getting along with others as an educational goal. *Journal of Research in Innovative Teaching & Learning*, *12*, 16–34. doi:10.1108/jrit-03-2019-0042

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative Health Research, 25*, 1212–1222. doi:10.1177/1049732315588501

Moseley, S. F. (2004). Everett Rogers' diffusion of innovations theory: Its utility and value in public health. *Journal of Health Communication, 9*(sup1), 149–151. doi:10.1080/10810730490271601

Moser, A., & Korstjens, I. (2017). Series: Practical guidance to qualitative research. Part 1: Introduction. *European Journal of General Practice, 23*, 271–273. doi:10.1080/13814788.2017.1375093

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice, 24*, 9–18. doi:10.1080/13814788.2017.1375091

Mourtzis, D., Vlachou, E., & Milas, N. (2016). Industrial big data as a result of IoT adoption in manufacturing. *Procedia CIRP, 55*, 290–295. doi:10.1016/j.procir.2016.07.038

Mukred, M., Yusof, Z. M., Alotaibi, F. M., Mokhtar, U. A., & Fauzi, F. (2019). The key factors in adopting an Electronic Records Management System (ERMS) in the educational sector: A UTAUT-based framework. *IEEE Access*, *7*, 35963–35980. doi:10.1109/ACCESS.2019.2904617

Munea, T. L., Lim, H., & Shon, T. (2017). Design and implementation of fuzzing framework based on IoT applications. *Wireless Personal Communications*, *93*, 365–382. doi:10.1007/s11277-016-3322-9

Naidu, T., & Prose, N. (2018). Re-envisioning member checking and communicating results as accountability practice in qualitative research: A South African community-based organization example. *Forum Qualitative Sozialforschung, 19*(3). doi:10.17169/fqs-19.3.3153

Najjar-Ghabel, S., Yousefi, S., & Farzinvash, L. (2018). Reliable data gathering in the Internet of Things using artificial bee colony. *Turkish Journal of Electrical Engineering and Computer Sciences*, *26*, 1710–1723. doi:10.3906/elk-1801-100

Nakamura, E. T. (2018). *A privacy, security, safety, resilience and reliability focused risk assessment methodology for IIoT systems steps to build and use secure IIoT systems.* doi:10.1109/GIOTS.2018.8534521

Nandan, S., Ramya, K. C., Rani, S. S., Gupta, D., Shankar, K., Lakshmanaprabu, S. K., & Khanna, A. (2020). An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy. *Future Generation Computer Systems*, *102*, 1027–1037. doi:10.1016/j.future.2019.09.050

Natarajan, T., Balasubramanian, S. A., & Kasilingam, D. L. (2017). Understanding the intention to use mobile shopping applications and its influence on price sensitivity. *Journal of Retailing and Consumer Services*, *37*, 8–22. doi:10.1016/j.jretconser.2017.02.010

Nawaz, T. (2018). Determinants and consequences of disruptive innovations: Evidence from the UK financial services sector. *Journal of Accounting and Management Information Systems*, *12*(2), 234–251. doi:10.24818/jamis.2018.02003

Nebeker, C., Linares-Orozco, R., & Crist, K. (2015). A multi-case study of research using mobile imaging, sensing and tracking technologies to objectively measure behavior. *Journal of Research Administration*, *46*, 118–137. Retrieved from https://www.srainternational.org/home

Nehme, E. K., Pérez, A., Ranjit, N., Amick, B. C., & Kohl, H. W. (2016). Behavioral theory and transportation cycling research: Application of diffusion of innovations. *Journal of Transport and Health, 3*, 346–356. doi:10.1016/j.jth.2016.05.127

Neshenko, N., Bou-harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, *21*(3), 2702-2733**.** doi:10.1109/COMST.2019.2910750

Ness, P., & Fusch, L. (2015). Are we there yet? Saturation in qualitative research. *Qualitative Report, 20*, 1409–1416. Retrieved from https://nsuworks.nova.edu/tqr/

Newman, I., & Houchins, D. E. (2018). Conceptualizing mixed methods questions in special education research. *Mid-South Educational Research Association, 25*(2), 23–33. Retrieved from http://www.msera.org/

Nguyen, T-H., & Yoo, M. (2017). Analysis of attacks on device manager in software-defined Internet of Things. *International Journal of Distributed Sensor Networks, 13*(8), 1-11. doi:10.1177/1550147717728681

Nicolas-Rocca, T. S., & Burkhard, R. J. (2019). Information security in libraries: Examining the effects of knowledge transfer. *Information Technology and Libraries, 38*(2), 58–71. doi:10.6017/ital.v38i2.10973

Nieuwenhuijsen, J., Correia, G. H. de A., Milakis, D., van Arem, B., & van Daalen, E. (2018). Towards a quantitative method to analyze the long-term innovation diffusion of automated vehicles technology using system dynamics.

Transportation Research Part C: Emerging Technologies, *86*, 300–327. doi:10.1016/j.trc.2017.11.016

Nikoukar, A., Raza, S., Poole, A., Gunes, M., & Dezfouli, B. (2018). Low-power wireless for the Internet of Things: Standards and applications. *IEEE Access*, *6*, 67893–67926. doi:10.1109/ACCESS.2018.2879189

Nilson, C. (2017). A journey toward cultural competence: The role of researcher reflexivity in indigenous research. *Journal of Transcultural Nursing*, *28*, 119–127. doi:10.1177/1043659616642825

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence-Based Nursing*, *18*(2), 34–35. doi:10.1136/eb-2015-102054

Nogwina, M., Gumbo, S., & Ngqulu, N. (2019). An overview of the Eastern Cape eSkills Colab training and awareness programmes. *2019 IST-Africa Week Conference*, pp. 1–7. doi:10.23919/ISTAFRICA.2019.8764825

Nouri-Mahdavi, K. (2016). Risk factors. *Pearls of Glaucoma Management: Second Edition*, (June), 213–222. doi:10.1007/978-3-662-49042-6_22

Ntemana, T. J., & Olatokun, W. (2012). Analyzing the influence of diffusion of innovation attributes on lecturers' attitude towards information and communication technologies. *Human Technology an Interdisciplinary Journal on Humans in ICT Environments*, *8*, 179–197. doi:10.17011/ht/urn.201211203034

Nurunnabi, M., & Hossain, M. A. (2019). Data falsification and question on academic integrity. *Accountability in Research*, *26*, 108–122. doi:10.1080/08989621.2018.1564664

Oliveira, T., Thomas, M., Baptista, G., & Campos, F. (2016). Mobile payment: Understanding the determinants of customer adoption and intention to recommend the technology. *Computers in Human Behavior*, *61*(2016), 404–414. doi:10.1016/j.chb.2016.03.030

Oteng-Ababio, M., Sarfo, K. O., & Owusu-Sekyere, E. (2015). Exploring the realities of resilience: Case study of Kantamanto Market fire in Accra, Ghana. *International Journal of Disaster Risk Reduction, 12,* 311–318. doi:10.1016/j.ijdrr.2015.02.005

Pacheco, L. A. B., Alchieri, E. A. P., & Barreto, P. A. S. M. (2018). Device-based security to improve user privacy in the Internet of Things. *Sensors, 18*(8). doi:10.3390/s18082664

Paiano, R., & Pasanisi, S. (2018). How to discover hidden knowledge according to different type data set: A guideline to apply the right hybrid information mining approach. *BRAIN—Broad Research in Artificial Intelligence and Neuroscience, 9*(4), 83–99. Retrieved from https://www.edusoft.ro/brain/index.php/brain

Palinkas, L. A. (2014). Qualitative and mixed methods in mental health services and implementation research. *Journal of Clinical Child and Adolescent Psychology, 43,* 851–861. doi:10.1080/15374416.2014.910791

Panagiotou, P., Sklavos, N., & Zaharakis, I. D. (2018). Design and implementation of a privacy framework for the internet of things (IoT). *Proceedings of the 21st Euromicro Conference on Digital System Design,* pp. 586–591. doi:10.1109/DSD.2018.00103

Park, J., & Park, M. (2016). Qualitative versus quantitative research methods: Discovery or justification? *Journal of Marketing Thought, 3,* 1–7. Retrieved from https://www.ama.org/journal-of-marketing/

Pashaeypoor, S., Ashktorab, T., Rassouli, M., & Alavi-majd, H. (2008). This month in laryngoscope effect of body mass index on chemoradiation outcomes in head and neck cancer the natural history of idiopathic unilateral vocal fold paralysis. *Evidence and Problems, 52*(1137), 2008. doi:10.1080/10376178.2016.1188019

Pashaeypoor, S., Ashktorab, T., Rassouli, M., & Alavi-Majd, H. (2016). Predicting the adoption of evidence-based practice using "Rogers diffusion of innovation model." *Contemporary Nurse, 52*(1), 85-94. doi:10.1080/10376178.2016.1188019

Pasquier, T., Singh, J., Powles, J., Eyers, D., Seltzer, M., & Bacon, J. (2018). Data provenance to audit compliance with privacy policy in the Internet of Things. *Personal and Ubiquitous Computing*, *22*, 333–344. doi:10.1007/s00779-017-1067-4

Pathak, P., Vyas, N., & Joshi, S. (2017). Security challenges for communications on IOT & big data. *International Journal of Advanced Computer Research, 8,* 431–436. Retrieved from http://ijarcs.in/index.php/Ijarcs/article/view/3031

Pek, G., Buttyan, L., & Bencsath, B. (2013). A survey of security issues in hardware virtualization. *ACM Computing Surveys, 45*(3), 1-34. doi:10.1145/2480741.2480757

Peng, H., Liu, C., Zhao, D., Ye, H., Fang, Z., & Wang, W. (2020). Security analysis of CPS systems under different swapping strategies in IoT environments. *IEEE Access, 8*, 63567–63576. doi:10.1109/ACCESS.2020.2983335

Perera, C., Ranjan, R., Wang, L., Khan, S. U., & Zomaya, A. Y. (2015). Big data privacy in the Internet of Things era. *IT Professional*, *17*(3), 32–39. doi:10.1109/MITP.2015.34

Persada, S. F., Miraja, B. A., & Nadlifatin, R. (2019). Understanding the generation z behavior on D-learning: A unified theory of acceptance and use of technology (UTAUT) approach. *International Journal of Emerging Technologies in Learning*, *14*(5), 20–33. doi:10.3991/ijet.v14i05.9993

Pinka, K., Kampars, J., & Minkevičs, V. (2017). Case study: IoT data integration for higher education institution. *Information Technology and Management Science, 19*, 71–77. doi:10.1515/itms-2016-0014

Pliakas, T., Hawkesworth, S., Silverwood, R. J., Nanchahal, K., Grundy, C., Armstrong, B., . . . Lock, K. (2017). Optimising measurement of health-related characteristics of the built environment: Comparing data collected by foot-based street audits, virtual street audits and routine secondary data sources. *Health and Place*, *43,* 75–84. doi:10.1016/j.healthplace.2016.10.001

Pokorni, S. (2019). Reliability and availability of the Internet of things. *Vojnotehnicki Glasnik, 67*, 588–600. doi:10.5937/vojtehg67-21363

Prescott, M. B. (1995). Diffusion of innovation theory. *ACM SIGMIS Database*. doi:10.1145/217278.217283

Pustokhina, I. V., Pustokhin, D. A., Gupta, D., Khanna, A., Shankar, K., & Nguyen, G. N. (2020). An effective training scheme for deep neural network in edge computing enabled Internet of Medical Things (IoMT) systems. *IEEE Access, 8*, 107112–107123. doi:10.1109/ACCESS.2020.3000322

Qu, Y., Yu, S., Zhou, W., Peng, S., Wang, G., & Xiao, K. (2018). Privacy of things: Emerging challenges and opportunities in wireless Internet of Things. *IEEE Wireless Communications, 25*(6), 91–97. doi:10.1109/MWC.2017.1800112

Radisavljevic-Gajic, V., Park, S., & Chasaki, D. (2018). Vulnerabilities of control systems in Internet of Things applications. *IEEE Internet of Things Journal, 5*, 1023–1032. doi:10.1109/JIOT.2017.2787962

Rahi, S., & Ghani, M. (2018). The role of UTAUT, DOI, perceived technology security and game elements in internet banking adoption. *World Journal of Science, Technology and Sustainable Development, 15*, 338–356. doi:10.1108/wjstsd-05-2018-0040

Rahimi, B., Timpka, T., Vimarlund, V., Uppugunduri, S., & Svensson, M. (2009). Organization-wide adoption of computerized provider order entry systems: A study based on diffusion of innovations theory. *BMC Medical Informatics and Decision Making, 9*, 1–12. doi:10.1186/1472-6947-9-52

Rajamaki, J. (2018, April). Industry-university collaboration on IoT cyber security education: Academic course: “Resilience of Internet of Things and cyber-physical systems.” *IEEE Global Engineering Education Conference,* pp. 1969–1977. doi:10.1109/EDUCON.2018.8363477

Rakic, S., Novakovic, B., Stevic, S., & Niskanovic, J. (2018). Introduction of safety and quality standards for private health care providers: A case-study from the

Republic of Srpska, Bosnia and Herzegovina. *International Journal for Equity in Health*, *17,* 92. doi:10.1186/s12939-018-0806-0

Ramavhona, C. T., & Mokwena, S. (2018). Factors influencing Internet banking adoption in African rural areas. *South African Journal of Information Management, 18*(2), 1–14. doi:10.4102/sajim.v8i2.642

Rana, S. M. S., Halim, M. A., & Kabir, M. H. (2018). Design and implementation of a security improvement framework of Zigbee network for intelligent monitoring in IoT Platform. *Applied Sciences, 8*(11). doi:10.3390/app8112305

Rauti, S., Mäki, P., Leppänen, V., Laurén, S., Hosseinzadeh, S., Holvitie, J., & Koivunen, L. (2018). Internal interface diversification as a security measure in sensor networks. *Journal of Sensor and Actuator Networks, 7*, 12. doi:10.3390/jsan7010012

Raza, S., Helgason, T., Papadimitratos, P., & Voigt, T. (2017). SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things. *Future Generation Computer Systems*, *77*, 40–51. doi:10.1016/j.future.2017.06.008

Ren, H., Li, H., Dai, Y., Yang, K., & Lin, X. (2018). Querying in Internet of Things with privacy preserving: Challenges, solutions and opportunities. *IEEE Network, 32*, 144–151. doi:10.1109/MNET.2018.1700374

Ren, J., Pan, Y., Goscinski, A., & Beyah, R. A. (2018). Edge computing for the Internet of Things. *IEEE Network, 32*, 6–7. doi:10.1109/MNET.2018.8270624

Riahi Sfar, A., Natalizio, E., Challal, Y., & Chtourou, Z. (2018). A roadmap for security challenges in the Internet of Things. *Digital Communications and Networks, 4*, 118–137. doi:10.1016/j.dcan.2017.04.003

Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2018, January). Towards using blockchain technology for IoT data access protection. *Proceedings of the 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband*, pp. 1–5. doi:10.1109/ICUWB.2017.8251003

Riga, S. A. (2017). Two breaches, two enforcement actions, and a DDoS attack: Data security and the rise of the Internet of Things. *Journal of Internet Law, 20*(9), 3–7.

Rimando, M., Brace, A. M., Namageyo-Funa, A., Parr, T. L., Sealy, D., Davis, T. L., . . . Christiana, R. W. (2015). Data collection challenges and recommendations for early career researchers. *Qualitative Report, 20*, 2025–2036. Retrieved from https://nsuworks.nova.edu/tqr/

Rjab, A. B., & Mellouli, S. (2018). *Smart cities in the era of artificial intelligence and Internet of Things, 6*, 1–10. doi:10.1145/3209281.3209380

Roberts, L. D. (2015). Ethical issues in conducting qualitative research in online communities. *Qualitative Research in Psychology, 12*, 314–325. doi:10.1080/14780887.2015.1008909

Rogers, E. M. (1962). *Diffusion of innovations*. New York, NY: Free Press.

Rogers, E. M. (1995). *Diffusion of innovations. Elements of diffusion* (3rd ed.). doi:10.1007/s10661-014-3885-4

Rogers, E. M. (2015). Evolution: Diffusion of innovations. In J. D. Wright (Ed.), *International encyclopedia of the social & behavioral sciences* (2nd ed., pp. 378–381). doi:10.1016/B978-0-08-097086-8.81064-8

Roldán, J. L., Real, J. C., & Ceballos, S. S. (2018). Antecedents and consequences of knowledge management performance: The role of IT infrastructure. *Intangible Capital, 14,* 518–535. doi:10.3926/ic.1074

Ross, M. W., Iguchi, M. Y., & Panicker, S. (2018). Ethical aspects of data sharing and research participant protections. *American Psychologist, 73,* 138–145. doi:10.1037/amp0000240

Rutberg, S., & Bouikidis, C. D. (2018). Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative research. *Exploring the Evidence Quantitative and Qualitative Research, 45*(2), 209–214. Retrieved from https://www.annanurse.org/

Ruth, T., Lamm, A., Rumble, J., & Ellis, J. (2018). Conversing about citrus greening: Extension’s role in educating about genetic modification science as a solution. *Journal of Agricultural Education, 58*(4), 34–49. doi:10.5032/jae.2017.04034

Ruth, T., Rumble, J., Lamm, A., & Ellis, J. (2018). A model for understanding decision-making related to agriculture and natural resource science and technology. *Journal of Agricultural Education, 59*(4), 224–237. doi:10.5032/jae.2018.04224

Sadeeq, M. A. M., Zeebaree, S. R. M., Qashi, R., Ahmed, S. H., & Jacksi, K. (2018). Internet of Things security: A survey. *International Conference on Advanced Science and Engineering, 88,* 162–166. doi:10.1109/ICOASE.2018.8548785

Sadique, K. M., Rahmani, R., & Johannesson, P. (2019). Trust in Internet of Things: An architecture for the future IoT network. *2018 International Conference on Innovation in Engineering and Technology,* pp. 1–5. doi:10.1109/CIET.2018.8660784

Sáenz-Royo, C., Gracia-Lázaro, C., & Moreno, Y. (2015). The role of the organization structure in the diffusion of innovations. *PLoS ONE, 10*(5), 1–14. doi:10.1371/journal.pone.0126076

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security, 53,* 65–78. doi:10.1016/j.cose.2015.05.012

Safaei, B., Mahdi, A., Monazzah, H., Bafroei, M. B., & Ejlali, A. (2017). Reliability side-effects in Internet of Things application layer protocols. In *2017 2nd International Conference on System Reliability and Safety (ICSRS)*, 207-212. doi:10.1109/ICSRS.2017.8272822

Safari, F., Safari, N., & Hasanzadeh, A. (2015). The adoption of software-as-a-service (SaaS): Ranking the determinants. *Journal of Enterprise Information Management, 28*, 400–422. doi:10.1108/JEIM-02-2014-0017

Sahin, I. (2006). MIC diffusion artigo. *Turkish Online Journal of Educational Technology, 5,* 1303–6521. doi:10.1287/mnsc.43.7.934

Sahmim, S., & Gharsellaoui, H. (2017). Privacy and security in Internet-based computing: Cloud computing, Internet of Things, Cloud of Things: A review. *Procedia Computer Science, 112,* 1516-1522. doi:10.1016/j.procs.2017.08.050

Salierno, D. (2015). Device risks under the radar. *Internal Auditor*, *72*(6), 14–15. Retrieved from https://na.theiia.org/Pages/IIAHome.aspx

Samanta, P., Kelly, E., Bashir, A., & Debroy, S. (2018). Collaborative adversarial modeling for spectrum aware IoT communications. *2018 International Conference on Computing, Networking and Communications,* pp. 447–451. doi:10.1109/ICCNC.2018.8390289

Sanyal, S., & Zhang, P. (2018). Improving quality of data: IoT data aggregation using device to device communications. *IEEE Access, 6,* 67830–87840. doi:10.1109/ACCESS.2018.2878640

Sathiyanarayanan, M., Govindraj, V., & Jahagirdar, N. (2018). Challenges and opportunities of integrating Internet of Things (IoT) and Light Fidelity (LiFi*). Proceedings of the 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology,* pp. 137–142. doi:10.1109/ICATCCT.2017.8389121

Schoenung, B., & Dikova, D. (2016). Reflections on organizational team diversity research. *Equality, Diversity and Inclusion: An International Journal, 35*, 221–231. doi:10.1108/edi-11-2015-0095

Scott, S., & Mcguire, J. (2017). Using diffusion of innovation theory to promote universally designed college instruction. *International Journal of Teaching and Learning in Higher Education, 29*, 119–128. Retrieved from http://www.isetl.org/ijtlhe/

Sebescen, N., & Vitak, J. (2017). Securing the human: Employee security vulnerability risk in organizational settings. *Journal of the American Society for Information Science and Technology, 64*, 1852–1863. doi:10.1002/asi.23851

Segev, A., Rovner, M., Ian Appel, D., Abrams, A. W., Rotem, M., & Bloch, Y. (2016). Possible biases of researchers' attitudes toward video games: Publication trends analysis of the medical literature (1980-2013). *Journal of Medical Internet Research, 18*(7). doi:10.2196/jmir.5935

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architecture, protocols and applications. *International Journal of Engineering Research and Applications, 07*(06), 85–88. doi:10.9790/9622-0706048588

Shah, V., & De Veciana, G. (2015). High-performance centralized content delivery infrastructure: Models and asymptotics. *IEEE/ACM Transactions on Networking, 23*, 1674–1687. doi:10.1109/TNET.2015.2461132

Shaw, J. (2018). How can research mediators better mediate? The importance of inward-looking processes. *Evidence and Policy, 14*, 143–153. doi:10.1332/174426416X14788873367067

Shepperd, M., Hall, T., & Bowes, D. (2018). Authors' reply to "Comments on 'Researcher bias: The use of machine learning in software defect prediction.'" *IEEE Transactions on Software Engineering, 44*, 1129–1131. doi:10.1109/TSE.2017.2731308

Shiau, S. J. H., Huang, C. Y., Yang, C. L., & Juang, J. N. (2018). A derivation of factors influencing the innovation diffusion of the OpenStreetMap in STEM education. *Sustainability, 10*(10), 1–29. doi:10.3390/su10103447

Shin, G., & Hall, J. L. (2018). Exploring the influence of federal welfare expenditures on state-level new economy development performance: Drawing from the diffusion of innovation theory. *Economic Development Quarterly, 32*, 242–256. doi:10.1177/0891242418778115

Siboni, S., Sachidananda, V., Meidan, Y., Bohadana, M., Mathov, Y., Bhairav, S., . . . Elovici, Y. (2019). Security testbed for Internet-of-Things devices. *IEEE Transactions on Reliability*, *68*, 23–44. doi:10.1109/TR.2018.2864536

Sicari, S., Rizzardi, A., Grieco, L. A., & Porisini, A. C. (2015). Security, privacy and trust in Internet of things: The road ahead. *Computer Networks*, *76*, 146–164. doi:10.1016/j.comnet.2014.11.008

Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. (2017). Dynamic policies in Internet of Things: Enforcement and synchronization. *IEEE Internet of Things Journal, 4*, 2228–2238. doi:10.1109/JIOT.2017.2749604

Siegel, J., & Sarma, S. (2019). A cognitive protection system for the Internet of Things. *IEEE Security and Privacy*, *17*(3), 40–48. doi:10.1109/MSEC.2018.2884860

Sieger, P., & Monsen, E. (2015). Founder, academic, or employee? A nuanced study of career choice intentions. *Journal of Small Business Management, 53*, 30–57. doi:10.1111/jsbm.12181

Siegner, M., Hagerman, S., & Kozak, R. (2018). Going deeper with documents: A systematic review of the application of extant texts in social research on forests. *Forest Policy and Economics*, *92*), 128–135. doi:10.1016/j.forpol.2018.05.001

Sinaga, N. (2018). Authority of military police of the Indonesian Air Force in handling national airspace boundaries. *Central European Journal of International and Security Studies*, *12*(4), 111–126. Retrieved from http://www.cejiss.org/

Singh, J., Millard, C., Reed, C., Cobbe, J., & Crowcroft, J. (2018). Accountability in the IoT: Systems, law, and ways forward. *Computer*, *51*(7), 54–65. doi:10.1109/MC.2018.3011052

Sivanathan, A., Habibi Gharakheili, H., & Sivaraman, V. (2020). Managing IoT cyber-security using programmable telemetry and machine learning. *IEEE Transactions on Network and Service Management*, *17*, 60–74. doi:10.1109/TNSM.2020.2971213

Smith, C. (2017). Preventing unintended disclosure of personally identifiable data following anonymisation. *Studies in Health Technology and Informatics*, *235*, 313–317. doi:10.3233/978-1-61499-753-5-313

Solangi, Z. A., Solangi, Y. A., Chandio, S., Aziz, M. B. S. A., Bin Hamzah, M. S., & Shah, A. (2018). The future of data privacy and security concerns in Internet of Things. *2018 IEEE International Conference on Innovative Research and Development*, pp. 1–4. doi:10.1109/ICIRD.2018.8376320

Son, I., Kim, J., Park, G., & Kim, S. (2018). The impact of innovative technology exploration on firm value sustainability: The case of part supplier management. *Sustainability, 10*(10), 3632. doi:10.3390/su10103632

Soultatos, O., Spanoudakis, G., Fysarakis, K., Askoxylakis, I., Alexandris, G., Miaoudakis, A., & Nikolaos Petroulakis, E. (2018). Towards a security, privacy, dependability, interoperability framework for the Internet of Things. *2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks*, pp. 1–6. doi:10.1109/CAMAD.2018.8514937

Spearman, L., Norwood, D., & Waller, S. (2016). Does the cream rise to the top? NCAA Division I players' perceptions of meritocracy in baseball. *Journal of Contemporary Athletics, 10,* 119–137. Retrieved from https://novapublishers.com/shop/journal-of-contemporary-athletics/

Stahl, N., Lampi, J., & King, J. R. (2019). Expanding approaches for research: Mixed methods. *Journal of Developmental Education*, *42*(2), 28–31. Retrieved from https://ncde.appstate.edu/

Stahl, W., & Karger, J. (2016). Student data privacy, digital learning, and special education: Challenges at the intersection of policy and practice. *Journal of Special Education Leadership*, *29*(2), 79–88. Retrieved from https://www.casecec.org/journal

Stahlke, S. (2018). Expanding on notions of ethical risks to qualitative researchers. *International Journal of Qualitative Methods, 17*, 1–9. doi:10.1177/1609406918787309

Stephenson, R., Phelps, A., & Colburn, J. (2018). Diffusion of innovations and program implementation in areas of health behavior / education / promotion. *Physical Activity, and Physical Education, 10*(1), 3-11. Retrieved from http://ichpersd.org/index.php/journal/journal-of-ichpermsd

Stewart, H., Gapp, R., & Harwood, I. (2017). Exploring the alchemy of qualitative management research: Seeking. *Qualitative Report*, *22*, 1–19. Retrieved from http://nsuworks.nova.edu/tqr

Strickland, W., Pirret, A., & Takerei, S. (2019). Patient and/or family activated rapid response service: Patients' perceptions of deterioration and need for a service. *Intensive and Critical Care Nursing*, *51*, 20–26. doi:10.1016/j.iccn.2018.11.007

Strömberg, H., Rexfelt, O., Karlsson, I. C. M. A., & Sochor, J. (2016). Trying on change—Trialability as a change moderator for sustainable travel behaviour. *Travel Behaviour and Society, 4,* 60–68. doi:10.1016/j.tbs.2016.01.002

Su, Y. S., Ding, T. J., Lue, J. H., Lai, C. F., & Su, C. N. (2017). Applying big data analysis technique to students' learning behavior and learning resource recommendation in a MOOCs course. *Proceedings of the 2017 IEEE International Conference on Applied System Innovation: Applied System Innovation for Modern Technology,* pp. 1229–1230. doi:10.1109/ICASI.2017.7988114

Subahi, A., & Theodorakopoulos, G. (2018). Ensuring compliance of IoT devices with their privacy policy agreement. *Proceedings—2018 IEEE 6th International Conference on Future Internet of Things and Cloud*, pp. 100–107. doi:10.1109/FiCloud.2018.00022

Suduc, A.-M., Bizoi, M., & Gorghiu, G. (2018). A survey on IoT in education. *Revista Romaneasca Pentru Educatie Multidimensionala, 10*(3), 103–111. doi:10.18662/rrem/66

Suharta, I. G. P., & Suarjan, I. M. (2018). A case study on mathematical literacy of prospective elementary school teachers. *International Journal of Instruction, 11*, 413–424. doi:10.12973/iji.2018.11228a

Sullivan, C. (2018). GDPR Regulation of AI and Deep Learning in the Context of IoT Data Processing--A Risky Strategy. *Journal of Internet Law*, *22*(6), 1–23

Sun, C. (2020). Research on investment decision-making model from the perspective of "Internet of Things + Big data." *Future Generation Computer Systems, 107*, 286–292. doi:10.1016/j.future.2020.02.003

Sundstrom, B. (2016). Mothers "Google it up:" Extending communication channel behavior in diffusion of innovations theory. *Health Communication, 31*, 91–101. doi:10.1080/10410236.2014.936339

Syal, A. S., & Gupta, A. (2018). Internet of Things: Review on security of novel technology. *Proceedings of the 2017 International Conference on Smart Technology for Smart Nation*, pp. 1405–1410. doi:10.1109/SmartTechCon.2017.8358596

Tabrizi, S. S., & Ibrahim, D. (2016). Security of the Internet of Things: An overview. *ACM International Conference Proceeding Series, 22*, 146–150. doi:10.1145/3023924.3023943

Taguchi, N. (2018). Description and explanation of pragmatic development: Quantitative, qualitative, and mixed methods research. *System, 75*, 23–32. doi:10.1016/j.system.2018.03.010

Taib, S. M., De Coster, R., & Nyamu, J. (2017). Innovation diffusion of wearable mobile computing: Pervasive computing perspective. *International Conference on Information Society,* pp. 97–101. doi:10.1109/i-Society.2016.7854185

Tan, P., Wu, H., Li, P., & Xu, H. (2018). Teaching management system with applications of RFID and IoT technology. *Education Sciences, 8*, 26. doi:10.3390/educsci8010026

Tankard, C. (2015). The security issues of the Internet of Things. *Computer Fraud & Security, 2015*(9), 11–14. doi:10.1016/S1361-3723(15)30084-1

Tanye, H. A. (2017). Perceived attributes of innovation: Perceived security as an additional attribute to Roger’s diffusion of innovation theory. *International Journal of Multicultural and Multireligious Understanding, 3*(6), 6–18. doi:10.18415/ijmmu.v3i6.56

Teixeira da Silva, J. A. (2017). Are pseudonyms ethical in (science) publishing? Neuroskeptic as a case study. *Science and Engineering Ethics, 23*, 1807–1810. doi:10.1007/s11948-016-9825-7

Thibaud, M., Chi, H., Zhou, W., & Piramuthu, S. (2018). Internet of Things (IoT) in high-risk environment, health and safety (EHS) industries: A comprehensive review. *Decision Support Systems, 108*, 79–95. doi:10.1016/j.dss.2018.02.005

Thiele, T., Pope, D., Singleton, A., & Stanistreet, D. (2018). Exploring the use of mixed methods in research and evaluation of widening participation interventions: guidance for practitioners. *Widening Participation and Lifelong Learning, 20*(4), 7–38. doi:10.5456/wpll.20a.7

Thomas, M., Costa, D., & Oliveira, T. (2016). Assessing the role of IT-enabled process virtualization on green IT adoption. *Information Systems Frontiers*, *18,* 693–710. doi:10.1007/s10796-015-9556-3

Thompson, R. (2019). A qualitative phenomenological study of emotional and cultural intelligence of international students in the United States of America. *Journal of International Students*, *8*, 1220–1255. doi:10.32674/jis.v8i2.144

Thompson Long, B., & Hall, T. (2018). Educational narrative inquiry through design-based research: designing digital storytelling to make alternative knowledge visible and actionable. *Irish Educational Studies, 37*, 205–225. doi:10.1080/03323315.2018.1465836

Thongsri, N., Shen, L., Bao, Y., & Alharbi, I. M. (2018). Integrating UTAUT and UGT to explain behavioural intention to use M-learning: A developing country’s perspective. *Journal of Systems and Information Technology, 20*, 278–297. doi:10.1108/JSIT-11-2017-0107

Tian, H., Nan, F., Chang, C. C., Huang, Y., Lu, J., & Du, Y. (2019). Privacy-preserving public auditing for secure data storage in fog-to-cloud computing. *Journal of Network and Computer Applications*, *127*, 59–69. doi:10.1016/j.jnca.2018.12.004

Tomko, M. E., Linsey, J., Nagel, R., & Alemán, M. W. (2017). Exploring meaning-making and innovation in makerspaces: An ethnographic study of student and faculty perspectives. *Proceedings—Frontiers in Education Conference,* pp. 1–9. doi:10.1109/FIE.2017.8190580

Torre, I., Sanchez, O. R., Koceva, F., & Adorni, G. (2018). Supporting users to take informed decisions on privacy settings of personal devices. *Personal and Ubiquitous Computing*, *22*, 345–364. doi:10.1007/s00779-017-1068-3

Tran, V. T., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology*, *80*, 88–96. doi:10.1016/j.jclinepi.2016.07.014

Tran, V. T., Porcher, R., Tran, V. C., & Ravaud, P. (2017). Predicting data saturation in qualitative surveys with mathematical models from ecological research. *Journal of Clinical Epidemiology*, *82*, 71-78.e2. doi:10.1016/j.jclinepi.2016.10.001

Triantafyllou, A., Sarigiannidis, P., & Lagkas, T. D. (2018). Network protocols, schemes, and mechanisms for Internet of Things (IoT): Features, open challenges, and trends. *Wireless Communications and Mobile Computing, 2018*. doi:10.1155/2018/5349894

Tristani, L., Tomasone, J., Fraser-thomas, J., & Bassett-gunter, R. (2020). Examining factors related to teachers’ decisions to adopt teacher-training resources for inclusive physical education. *Canadian Journal of Education, 43*(2), 367-396. Retrieved from https://cje-rce.ca/

Turcotte-Tremblay, A. M., & Mc Sween-Cadieux, E. (2018). A reflection on the challenge of protecting confidentiality of participants while disseminating research results locally. *BMC Medical Ethics, 19*(Suppl 1). doi:10.1186/s12910-018-0279-0

Tyagi, S., Kumar, D., & Kumar, S. (2017). Understanding the nittygrities of software reliability and its testing procedures: A different approach. *Journal of Information and Optimization Sciences, 38*, 971–988. doi:10.1080/02522667.2017.1372144

Ullah, I., Ahmad, R., & Kim, D. H. (2018). A prediction mechanism of energy consumption in residential buildings using hidden Markov model. *Energies, 11*(2), 1–21. doi:10.3390/en11020358

Vargo, S. L., Akaka, M. A., & Wieland, H. (2020). Rethinking the process of diffusion in innovation: A service-ecosystems and institutional perspective. *Journal of Business Research, 116*(February), 526–534. doi:10.1016/j.jbusres.2020.01.038

Varkonyi, G. G., Kertesz, A., & Varadi, S. (2019). Privacy-awareness of users in our cloudy smart world. *2019 Fourth International Conference on Fog and Mobile Edge Computing*, pp. 189–196. doi:10.1109/fmec.2019.8795310

Varpio, L., Ajjawi, R., Monrouxe, L. V., O'Brien, B. C., & Rees, C. E. (2017). Shedding the cobra effect: Problematising thematic emergence, triangulation, saturation and member checking. *Medical Education, 51*, 40–50. doi:10.1111/medu.13124

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterising and justifying sample size sufficiency in interview-based studies: Systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology, 18,* 1–19. doi:10.1186/s12874-018-0594-7

Venkatesh, V., Morris, G. M., Davis, B. G., & Davis, D. F. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*, 425. doi:10.2307/30036540

Verma, P., & Sood, S. K. (2018). Internet of Things-based student performance evaluation framework. *Behaviour & Information Technology, 37*, 102–119. doi:10.1080/0144929X.2017.1407824

Villari, M., Fazio, M., Dustdar, S., Rana, O., Chen, L., & Ranjan, R. (2017). Software defined membrane: Policy-driven edge and Internet of Things security. *IEEE Cloud Computing, 4*(4), 92–99. doi:10.1109/MCC.2017.3791014

Vojtovič, S., Navickas, V., & Gruzauskas, V. (2016). Journal of Security and Sustainability Issues Volume 4 Number 3. *Journal of Security and Sustainability Issues, 5*(2), 489–499. doi:10.9770/jssi.2016.5.3(4)

Wadams, M., & Park, T. (2018). Qualitative research in correctional settings: Researcher bias, Western ideological influences, and social justice. *Journal of Forensic Nursing, 14*(2), 72–79. doi:10.1097/JFN.0000000000000199

Waheed, M., Kaur, K., Ain, N., & Sanni, S. A. (2015). Emotional attachment and multidimensional self-efficacy: Extension of innovation diffusion theory in the context of eBook reader. *Behaviour and Information Technology, 34*, 1147–1159. doi:10.1080/0144929X.2015.1004648

Wang, X., Shi, W., Xiang, Y., & Li, J. (2016). Efficient network security policy enforcement with policy space analysis. *IEEE/ACM Transactions on Networking, 24*, 2926–2938. doi:10.1109/TNET.2015.2502402

Wang, X., Yuen, K. F., Wong, Y. D., & Teo, C. C. (2018). An innovation diffusion perspective of e-consumers' initial adoption of self-collection service via automated parcel station. *International Journal of Logistics Management, 29,* 237–260. doi:10.1108/IJLM-12-2016-0302

Wang, Y. S., Li, H. T., Li, C. R., & Zhang, D. Z. (2016). Factors affecting hotels' adoption of mobile reservation systems: A technology-organization-environment framework. *Tourism Management, 53,* 163–172. doi:10.1016/j.tourman.2015.09.021

Wang, Z., Zhang, Y., Tian, Z., Ruan, Q., Liu, T., Wang, H., . . . Shi, W. (2019). Automated vulnerability discovery and exploitation in the Internet of Things. *Sensors, 19*(15), 3362 doi:10.3390/s19153362

Weber, R. H. (2015). Internet of Things: Privacy issues revisited. *Computer Law and Security Review, 31*(5), 618-627. doi:10.1016/j.clsr.2015.07.002

Williams, M., & Moser, T. (2019). The art of coding and thematic exploration in qualitative research. *International Management Review, 15*, 45–56. Retrieved from http://www.imrjournal.org/

Wirtz, A. L., Mehta, S. H., Latkin, C., Zelaya, C. E., Galai, N., Peryshkina, A., . . . Beyrer, C. (2016). Comparison of respondent driven sampling estimators to determine HIV prevalence and population characteristics among men who have sex with men in Moscow, Russia. *PLoS ONE, 11*(6), 1–16. doi:10.1371/journal.pone.0155519

Wiseman, N., Rossmann, C., & Harris, N. (2019). A systematic review of data collection techniques used to measure preschool children's knowledge of and preference for physical activity. *International Journal of Environmental Research and Public Health*, *16*(6), 964. doi:10.3390/ijerph16060964

Wortmann, F., & Flüchter, K. (2015). Internet of Things: Technology and value added. *Business and Information Systems Engineering, 57*, 221–224. doi:10.1007/s12599-015-0383-3

Wu, W., Zhai, X., & Zhao, Y. (2018). On minimizing sensing time via data sharing in collaborative Internet of Things. *IEEE Access, 6*, 41633–41642. doi:10.1109/ACCESS.2018.2859357

Xing, L., Tannous, M., Vokkarane, V. M., Wang, H., & Guo, J. (2017). Reliability modeling of mesh storage area networks for Internet of Things. *IEEE Internet of Things Journal, 4*, 2047–2057. doi:10.1109/JIOT.2017.2749375

Xu, K., Qu, Y., & Yang, K. (2016). A tutorial on the internet of things: From a heterogeneous network integration perspective. *IEEE Network, 30*(2), 102-108. doi:10.1109/MNET.2016.7437031

Xu, S., Yang, G., Mu, Y., & Liu, X. (2019). A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance. *Future Generation Computer Systems*, *97*, 284–294. doi:10.1016/j.future.2019.02.051

Yang, A., Zhang, C., Chen, Y., Zhuansun, Y., & Liu, H. (2020). Security and privacy of smart home systems based on the Internet of Things and stereo matching algorithms. *IEEE Internet of Things Journal*, *7*, 2521–2530. doi:10.1109/JIOT.2019.2946214

Yang, C.-Y., Huang, C.-T., Wang, Y.-P., Chen, Y.-W., & Wang, S.-J. (n.d.). *File changes with security proof stored in cloud service systems.* doi:10.1007/s00779-017-1090-5

Yang, K., Han, Q., Li, H., Zheng, K., Su, Z., & Shen, X. (2017). An efficient and fine-grained big data access control scheme with privacy-preserving policy. *IEEE Internet of Things Journal*, *4*, 563–571. doi:10.1109/JIOT.2016.2571718

Yang, K., Li, Q., & Sun, L. (2019). Towards automatic fingerprinting of IoT devices in the cyberspace. *Computer Networks*, *148*, 318–327. doi:10.1016/j.comnet.2018.11.013

Yeong, M. L., Ismail, R., Ismail, N. H., & Hamzah, M. I. (2018). Interview protocol refinement: Fine-tuning qualitative research interview questions for multi-racial populations in Malaysia. *Qualitative Report*, *23*, 2700–2713. Retrieved from https://nsuworks.nova.edu/tqr/

Yin, C., Xi, J., Sun, R., & Wang, J. (2018). Location privacy protection based on differential privacy strategy for big data in industrial Internet of Things. *IEEE*

Transactions on Industrial Informatics, *14*, 3628–3636. doi:10.1109/TII.2017.2773646

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). Thousand Oaks, CA: Sage.

Yu, S., Wang, G., Liu, X., & Niu, J. (2018). Security and privacy in the age of the smart Internet of Things: An overview from a networking perspective. *IEEE Communications Magazine, 56*(9), 14–18. doi:10.1109/MCOM.2018.1701204

Yu, X., Tian, Z., Qiu, J., & Jiang, F. (2018). A data leakage prevention method based on the reduction of confidential and context terms for smart mobile devices. *Wireless Communications and Mobile Computing*, *2018*, 1–11. doi:10.1155/2018/5823439

Yuan, J. S., Lin, J., Alasad, Q., & Taheri, S. (2017). Ultra-low-power design and hardware security using emerging technologies for Internet of Things. *Electronics, 6*(3), 67. doi:10.3390/electronics6030067

Zahle, J. (2017). Privacy, Informed Consent, and Participant Observation. *Perspectives on Science*, *25*(4), 465–487. doi:10.1162/POSC

Zanello, G., Fu, X., Mohnen, P., & Ventresca, M. (2016). The creation and diffusion of innovation in developing countries: A systematic literature review. *Journal of Economic Surveys*, *30*, 884–912. doi:10.1111/joes.12126

Zhang, J., Chu, Z., Sankar, L., & Kosut, O. (2018). Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems? *IEEE Transactions on Power Systems*, *33*, 4775–4786. doi:10.1109/TPWRS.2018.2818746

Zhang, J., Duong, T. Q., Woods, R., & Marshall, A. (2017). Securing wireless communications of the Internet of Things from the physical layer, an overview. *Entropy*, *19*(8), 1–17. doi:10.3390/e19080420

Zhang, L., Qian, X., Lv, P., & Zhou, X. (2019). A novel recommendation algorithm based on diffusion of innovation theory. *Journal of Engineering Science and Technology Review*, *12*(6), 87–95. doi:10.25103/jestr.126.11

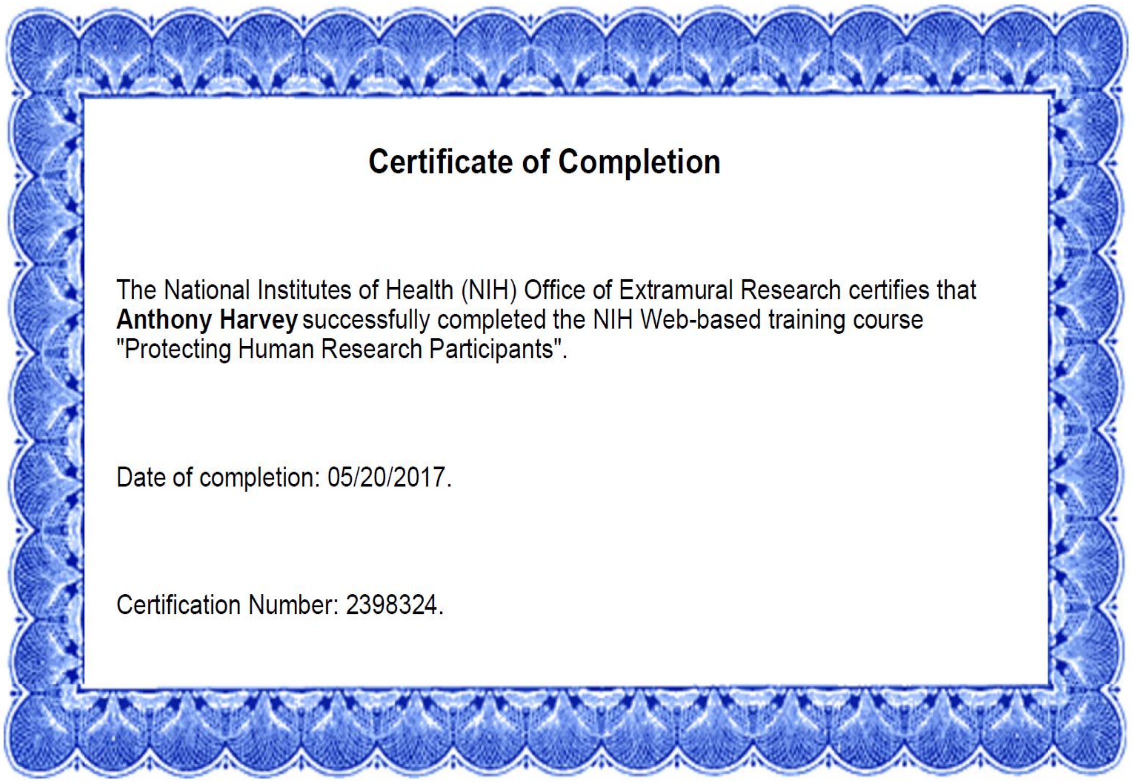
Zhang, Y., Szabo, C., & Sheng, Q. Z. (2016). Reduce or remove: Individual sensor reliability profiling and data cleaning. *Intelligent Data Analysis, 20*, 979–995. doi:10.3233/IDA-160853

Zheng, D., Wu, A., Zhang, Y., & Zhao, Q. (2018). Efficient and privacy-preserving medical data sharing in Internet of Things with limited computing power. *IEEE Access*, *6,* 28019–28027. doi:10.1109/ACCESS.2018.2840504

Zhou, R., Zhang, X., Du, X., Wang, X., Yang, G., & Guizani, M. (2018). File-centric multi-key aggregate keyword searchable encryption for industrial Internet of Things. *IEEE Transactions on Industrial Informatics, 14*, 3648–3658. doi:10.1109/TII.2018.2794442

Zutlevics, T. L. (2016). Could providing financial incentives to research participants be ultimately self-defeating? *Research Ethics*, *12*(3), 137–148. doi:10.1177/1747016115626756

Appendix A: Protecting Human Research Participants



Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Anthony Harvey** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 05/20/2017.

Certification Number: 2398324.

Appendix B: Interview Protocol

Interview Title: Exploring the Internet of Things Integration Strategies in Educational Institutions

A. I will introduce myself to the participant and thank them for agreeing to participate in the research study.

B. I will explain the reason for the study to the participants.

C. I will collect and verify the completion of the consent forms and answer any questions and concerns of the study participants.

D. I will remind the study participants that the interview will be recorded, and the recorded interview will remain strictly confidential.

E. I will turn on the recording device, identify the participants by their unique identifying code, and announce the date and time of the interview.

F. I will start the interview with the first question and continue through to the last question.

G. I will ask open-ended questions to extract maximum data from the participants to address the research question and understand their experiences.

H. End interview questions and ask if there is any other information they would like to share.

I. Inform the participant about the concept of member checking, which will be used to verify the accuracy of the initial interview.

J. Thank the participant for partaking in the study. Confirm the participant has contact information for any follow-up questions and concerns.

Appendix C: Interview Questions

A. Header

   a. Title : Interview with study participants

   b. Date : To-Be-Determined

   c. Venue : Office of the interviewee

   d. Interviewer: Anthony Harvey

   e. Interviewee: IT Administrators

B. Instructions for Interviewees.

C. Interview questions:

   a. Ice breaker

   b. What is the stage of IoT integration in your educational institution?

   c. What deployed connected devices in your institution do you classify as belonging to the IoT family?

   d. What security strategies do you adopt during the integration of IoT devices?

   e. How is your IT staff determining the use of security and reliability strategies during the integration of IoT devices?

   f. What strategies are you deploy to control compatibility issues that arise during the deployment of IoT devices?

   g. What methods are you using to confirm the viability of your IoT deployment?

h. How are you ensuring that stakeholders buy into the security strategies being used to integrate IoT devices?

i. How do you remain current regarding security strategies required to integrate IoT into your educational institution?

j. How do you ensure the continued security of IoT devices in your educational institution?

D. Thank the participant for participating in the interview.

E. Check with the participants to ensure that they have the interviewer’s contact information.

F. Complete logging the data related to the interview.