5-14-2024

Exploring Security Strategies to Enable the Adoption of Internet of Things Devices in the Manufacturing Sector

Joy Chamoun
Walden University

Walden University

College of Management and Human Potential

This is to certify that the doctoral study by

Joy Chamoun

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. Alan Dawson, Committee Chairperson, Information Technology Faculty
Dr. Cheryl Waters, Committee Member, Information Technology Faculty

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

Walden University
2024

Abstract

Exploring Security Strategies to Enable the Adoption of Internet of Things Devices in the Manufacturing Sector

by

Joy Chamoun

MS, Bellevue University, 2018

BS, The Open University, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

May 2024

Abstract

Many information technology (IT) leaders lack the strategies to protect IoT devices from information security threats in the manufacturing sector, which puts IoT devices and modern manufacturing systems at risk of external threats and introduces security risks to organizations and workers. Grounded in the diffusion of innovation (DOI) theory, the purpose of this qualitative multiple-case study was to determine strategies that IT leaders use to implement security for IoT devices in the manufacturing sector. The participants were three IT leaders from three separate manufacturing facilities in the Los Angeles area of the United States. The data were collected from semistructured interviews and organizational public documents. The data were analyzed using methodological triangulation to identify codes and themes. The three major themes that emerged were (a) authentication and access control, (b) data privacy and confidentiality, and (c) device and network security. A key recommendation for IT leaders is to use a defense-in-depth approach in which a series of defensive mechanisms are layered to protect IoT devices. The implications for positive social change include the potential for improving the organization's quality of goods and employees' safety.

Exploring Security Strategies to Enable the Adoption of Internet of Things Devices in the Manufacturing Sector

by

Joy Chamoun

MS, Bellevue University, 2018

BS, The Open University, 2011

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

May 2024

Table of Contents

List of Tables

Section 1: Foundation of the Study

Manufacturers face significant security risks when collecting data through Internet of Things (IoT) devices. IoT opens a wide range of new cyberattacks to the manufacturing sector. Security risks might appear at all stages of production, from data collection and processing to managing and controlling machinery and robotic devices.

Background of the Problem

Smart manufacturing has gained considerable interest recently both for academic research and industrial developments. Smart manufacturing is an integrator of different types of information technology (IT), such as IoT devices and AI, aiming to achieve digital transformations over traditional manufacturing processes. The cooperation between computer numerical control, robotics arms, and IoT technology has enhanced supply chain operations and streamlined industry processes more efficiently and cost-effectively.

IoT devices are one of the main key technologies and fields related to Industry 4.0 (Yamao & Lescano, 2020). Industry 4.0 aims to enable autonomous decision-making processes, monitor assets and operations in real-time, and promote equally real-time connected value creation networks through stakeholders' early involvement. While IoT devices benefit the manufacturing industry, they can also introduce blind spots and security risks to the organizations and the workers (Rana & Dahotre, 2021). A criminal attack, inadequate cloud security, IT security failure, or the IoT devices' vulnerability could lead to a data breach if data held within the devices are not adequately secured. It

can also lead to work injuries, economic losses for customers, and damage to the manufacturer's brand and reputation.

According to security company researchers, hackers could target smart manufacturing with new and unconventional cyberattacks designed to exploit vulnerabilities in IoT devices that are connected to the organizations' network to access other systems on the same network. IoT is an essential component of industrial transformation efforts across the globe, and yet, manufacturers are ignoring the importance of keeping these devices secured. This study explored strategies that IT leaders use to implement security for IoT devices in the manufacturing sector.

Problem Statement

IoT devices are built without any security considerations (Mohamad et al., 2019). Eighty percent of IoT firmware relies on libraries that have known vulnerabilities (Neshenko et al. 2019). The general IT problem is that IoT devices in the manufacturing sector are vulnerable to security threats. The specific IT problem is that some IT leaders lack strategies to protect IoT devices from information security threats in the manufacturing sector.

Purpose Statement

The purpose of this qualitative multiple-case study was to determine strategies that IT leaders use to implement security for IoT devices in the manufacturing sector. The target population includes IT leaders of aerospace and defense manufacturing facilities in Southeast Los Angeles who have strategies to secure these devices from cyberattacks.

The social impact is that this study may have a positive effect on the employees' safety in the manufacturing environment and might also have a social impact on the quality of the goods that are delivered to the consumers. IoT devices can track working conditions such as detecting hazardous material leakage, which can prevent potential work injuries. Furthermore, IoT sensors can determine whether the manufactured products have been exposed to pressures, temperatures, and other conditions that may render the product unsafe for use or consumption.

Nature of the Study

I chose the qualitative methodology as the research method for this study. A qualitative approach is a way of thinking about conducting qualitative research. It describes the purpose of qualitative research, the role of the researcher, and the method of data analysis (Trochim, n.d.). It is suitable for this study because my research focuses on the quality of the strategies used by the organization in securely implementing IoT. I did not choose the quantitative method because it is limited in its pursuit of statistical relationships, which can lead to overlooking broader relationships. Likewise, I did not choose the mixed method because it also uses statistical data, which is hard to gather since I used observations and interviewing IT leaders. Harvey (2021) discussed how he was able to identify organizational, security, and technical deficiencies by conducting a qualitative interview with participants that he would not have realized had he used a quantitative questionnaire.

The five qualitative approaches are biography, ethnography, phenomenology, grounded theory, and case study. The most appropriate approach for the IT problem that I

addressed for my doctoral research is the case study. Case study research is the most common qualitative method used in information systems. It enables the researcher to study information systems in their natural settings and generate theories from practice. Case study research can be critical, positivist, or interpretive, depending on the researcher's underlying philosophical expectations (Myers, 2004). A case study was the most suitable design because of the ability to perform an in-depth investigation and analysis of the problem.

I did not consider ethnography or grounded theory, because ethnographic research comes from the discipline of cultural anthropology, where the researcher is required to spend a significant amount of time in the field. This approach can be used to study the development of information systems and IT management aspects. Grounded theory is a research method that pursues to develop a theory that is grounded in data systematically gathered and analyzed. Grounded theory approaches are common in the information system research literature because it is particularly useful in developing context-based, explanation of the phenomenon, and process-oriented descriptions. Addressing the perception of the participant about the phenomena is not necessary to conduct the research (Murray, 2020).

The least appropriate approaches for my research are biography and phenomenology. Biography focuses on exploring an individual's life, whereas phenomenology focuses on understanding the essence of the experience. Some of the disadvantages of these approaches are subjectivity and bias. It is very challenging to

establish the reliability and validity of the approaches, which makes subjective research difficult.

Research Question

What strategies are used by IT leaders to implement security for IoT devices in the manufacturing sector?

Interview/Survey Questions

1. How many years of experience do you have in implementing cybersecurity technical controls?
2. What strategies have you used to secure IoT devices?
3. What problems or road blocks did you encounter when implementing these strategies?
4. Which of those strategies worked well, and why?
5. How did regulations affect your choice of strategies?
6. What steps have you taken before implanting your controls?
7. How do you measure IoT risks on the organization?
8. How do you assess the effectiveness of the strategies used to secure IoT devices in your manufacturing environment?
9. How do you ensure the continued security of IoT devices in your manufacturing environment?

Conceptual Framework

The theoretical perspective that will guide my research is the diffusion of innovation (DOI) theory, developed by E. M. Rogers (1962). DOI explains the degree to

which an innovation is seen as better than the idea. There are five main factors that influence adoption of an innovation: relative advantage, compatibility, complexity, trialability, and observability. One of the DOI core advantages is its applicability. It can be applied across multiple disciplines. However, it does not consider an individual's resources or social support to adopt the new behavior. Researchers have used the DOI theory to explain the adoption of innovative technology in different sectors. DOI helps explain why and how technologies spread through cultures (Sundstrom, 2016).

Rogers developed DOI theory in 1962, and researchers have extensively employed it to investigate IT innovation at both individual and organizational levels (Tu, 2018). Rogers asserted that the five innovation attributes (i.e., relative advantage, compatibility, complexity, trialability, and observability) could elucidate 49%–87% of innovation adoption. Each attribute, along with its subdimensions, impacts adoption in varied ways (Savoury and Burchell, 2021).

The DOI theory provides a framework for understanding how new technologies are adopted over time. In the context of IoT security, the theory can be used to understand how new security technologies and strategies are adopted and understand the factors that influence the adoption pattern. IT leaders can use the DOI theory to understand the different adoption factors and to develop strategies that will be effective and appealing that are more likely to be adopted and followed by all stakeholders.

Definition of Terms

Internet of Things (IoT): A system of interrelated computing devices that are provided with the ability to transfer data over a network without requiring human-to-human interaction.

Intrusion detection system: A monitoring system that detects suspicious activities or malicious activities or policy violations and generates alerts when they are detected. Any intrusion activity or violation is typically reported either to security operations center (SOC) analyst to investigate the issue and take actions to remediate the threat.

Cipher: A cipher is an algorithm for performing encryption or decryption by following defined steps. To encipher or encode is to convert information into cipher or code (Agyemang et al., 202).

Machine learning (ML): One of the artificial intelligence techniques which trains systems using different algorithms and helps them learn from their experience (Tahsien et al., 2020).

Denial of service (DoS): A cyberattack in which the attacker seeks to a system or network resource unavailable to its intended users by disrupting services of a host connected to the internet.

Man-in-the-middle (MITM): An attack where the attacker intercepts and potentially modifies the communication between two parties who believe they are communicating directly with each other.

Service set identifier (SSID): An identifier associated with an 802.11 wireless local area network (WLAN). Devices utilize case-sensitive identifiers to recognize and connect to wireless networks.

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are statements that are considered true, even though they have not been scientifically tested. There are two types of assumptions in research papers: explicit and implicit. Assumptions are vital to research success (Oden, n.d.). My first assumption for this study was that the participants have experience in implementing security strategies for IoT devices. My second assumption was that the participants would interpret the questions accurately and answer honestly. My last assumption was the participants chosen sufficiently represented the overall IT leaders in the manufacturing sector.

Limitations

Research limitations are characteristics of design or methodology that impact the interpretation of the findings (University of Southern California, n.d.). This study has limitations that should be acknowledged. This study was limited to three participants in the manufacturing sector, and as such, this limitation may influence the case study. Another limitation was that self-reported data are limited by the fact that they can hardly be independently verified. The data may contain potential sources of bias that should be noted as limitations, such as selective memory, telescoping, attribution, and exaggeration.

Delimitations

Delimitations refer to the boundaries of the research dissertation in which the researcher specifies what to include and what to exclude. Theofanidis and Fountouki (2018) explained that delimitations are set so that the study's aims and objectives do not become impossible to achieve. The first delimiter was that all the participants had IT leadership responsibilities in a manufacturing environment. The second delimiter was the selection of manufacturing organizations located in the Los Angeles area of the United States. The final delimiter was collecting data using semistructured interview questions.

Significance of the Study

IoT devices can perform a range of activities but are primarily used in manufacturing to collect data and perform specific actions. These smart devices are integrated with sensors and software to connect and exchange data within the network. It provides valuable real-time data that allows manufacturers or operators to make informed decisions (Peranzo, 2020). This study aimed to explore the strategies being used by IT leaders to implement IoT in the manufacturing sectors securely. The results of this study may shed light on some insights on the best security strategies that manufacturers can use to protect the confidentiality, privacy, and availability of their assets. IoT devices provide an improvement of the productivity of the operation by improving visibility, processes, and actions.

The study can significantly contribute to a positive social change by promoting the importance of securing IoT in the manufacturing sector. Securing IoT devices within the manufacturing sector might ensure safer customer information, increase the

productivity of the business, and improve the quality of the products which will increase customer satisfaction and trust that leads to higher revenue.

A Review of the Professional and Academic Literature

In the literature review, I provide a comprehensive overview of the existing knowledge and ideas related to the research question: What strategies are used by IT leaders to implement security for IoT devices in the manufacturing sector? I explored security strategies using the five characteristics of the DOI theory. I identified key concepts to build a solid foundation for this research. The literature focused on four key areas (a) DOI theory, (b) IoT, (c) IoT security issues, (d) IoT security strategies. In total, I considered 177 articles for review, of which 149 (84%) were peer-reviewed and published within 5 years of my anticipated graduation date. I derived the literature articles from sources such as Google Scholar, Walden University Library, ProQuest, IEEE Xplore Digital Library, ScienceDirect, ACM, EBSCO, and Ulrich's database. Here are some of the keywords I used to conduct the searches: IoT, IoT security issues, IoT security strategies, diffusion of innovation theory, DOI characteristics, IoT supply chain, IoT in manufacturing, Industry 4.0, machine learning, Big Data, blockchain, IoT architect, IoT layers, sensing layer, network layer, application layer.

DOI Theory

DOI Defined

Rogers's DOI theory explains how new ideas or innovations are adopted. Diffusion is a social process in which an innovation or idea is communicated over time. According to Rogers (1976), there are five steps for the adoption of innovation explicitly:

knowledge, persuasion, decision, implementation, and confirmation. The decision to adopt an innovation is a process that involves interactions between the individual and attributes of the innovation, as well as factors such as situational and contextual. Needs and motivations differ among people according to their degree of innovativeness (Dearing et al., 2018). The main players in the theory are innovators, early adopters, early majority, late majority, and laggards. According to Rogers (2003), the sequence of adopter groups flowing from innovators to laggards is most likely to succeed for innovations with potentially superior performance over existing products. This theory proposes that the innovation's attributes or characteristics can be measured by five aspects: relative advantage, compatibility, complexity, trialability, and observability (Yuen et al., 2021). Rogers (2003) noted that individuals' insights into these characteristics predict the rate of adoption. Also, Rogers indicated that consumers become aware of a new product but lack related information at first. But if the consumer is interested in this new product, then they evaluate whether to use it based on the available information (Mazhar et al., 2021). Combining an innovation-supporting culture with employees with an innovative mindset gives organizations the capability of getting the maximum benefit that lies ahead.

Although innovations are important aspects of technological progress, diffusion plays a critical role as it has social and economic impact since innovations must spread across society in order to have such influence (Woo & Magee, 2022). DOI theory is an extensive social and psychological theory that aims to help predict how people make decisions when adopting a new idea or innovation; as such, the adoption of an innovation

can be fully understood by taking the social system into consideration. Including social influence as an antecedent will better help understand the users' adoption behavior toward innovation (Min et al., 2019).

The DOI theory is useful to extract the advancement of IoT adoption. The recent advances in IoT and their widespread adoption and diffusion have helped facilitate monitoring and quality control. But this created other security issues as the security protocols that applied to a traditional computer network do work efficiently on IoT infrastructure. While there have been many academic studies concerning IoT security, there are still lack of consistent approaches to security risks inherent in deployment of IoT solutions (Boyes et al., 2018).

The five characteristics of the DOI theory played critical roles in this study as I used them to explore the lock of security strategies to protect IoT devices from information security threats in the manufacturing sector. I am using the DOI theory's five characteristics to remind the implementers of the security concerns and the complexity and reliability issues that can disrupt the implementation and negatively affect the rate of adoption. During this study, the information gathered and the solutions provided might help IT leaders in the manufacturing sector with the foundation needed to implement security strategies to protect IoT devices from information security threats.

The diffusion and acceptance of new ideas may regulate the success of a security adoption. IoT manufacturers need to focus more on privacy and security issues. Bartlett (2020) discussed the security aspects of IoT across diverse security parameters; the IoT

network system serves as a vulnerable component. Common flaws in IoT security, identified across all device types, encompass issues of privacy and security.

Relative Advantage

Relative advantage is the first attribute of innovations, is the strongest predictor of the rate of adoption of an innovation and a leading factor that determines the users' intention of adoption. Rogers (2003) defined relative advantage as the extent to which an innovation is perceived to offer greater benefits than its predecessor. In order to affect the rate of adoption, it should be seen as better than the idea or product it replaces. Relative advantage is measured in terms of economics, satisfaction, convenience, and social prestige. However, the individual's perception of the advantages determines the rate of adoption even if an innovation is objectively advantageous (Rogers, 1983).

Innovations must compete with others looking to serve a similar purpose. People adopt new innovations when they are believed to be more useful due to their efficiency or effectiveness (Min et al., 2019). Ho (2022) argues that low cost is also a relative advantage that targets a market group that is looking for a relatively economical solution. To make relative advantage more effective and increase the rate of adopting innovations, financial payment incentive can be used to support society in adopting an innovation.

Relative Advantage and IoT Security

The concept of relative advantage elucidates how a given society perceives the benefits of IoT technology compared to the technologies it replaces (Rogers, 2003). People measure an innovation based on what matters the most to them; it could be economic advantage to some and satisfaction or social prestige to others. The relative

advantage attribute might be considered the same as perceived usefulness construct of the Technology Acceptance Model (TAM), referring to the degree to which a person believes using a particular system will improve his/her job performance in completing tasks (Mokwena & Hlebela, 2018). Perceived usefulness has positive effects on the users' attitude, behavioral intention, and satisfaction of using IoT (Yang, 2021). The relative advantage is the amount by which the innovation improves upon previous conditions.

The cost-effectiveness of IoT devices and their ability to connect in real time has made the technology highly attractive to many industry sectors. IoT facilitates radical advantages by automation and optimization of manual tasks. The reduction of hardware costs and the use of data generated by IoT is considered the main drivers of investment (Metallo et al., 2018). IoT can improve security by interconnecting systems and ensuring transparency. Information sharing is a secure way of monitoring connected devices (Omolara et al., 2022). The data that IoT devices generate is often what creates the relative advantage; however, cyber-risk exposure is part of the customers' perception of security and reliability which also affects the relative advantage of IoT (Jalali et al., 2019). IoT is useful when it comes to improving security for manufacturing companies in areas such as vehicle and asset tracking, air quality management, security access control, and risk measurement for radiation gases (Sivathanu, 2019). Tsai and Tiwasing (2021) suggested that relative advantage has positive effects on the users' attitudes toward the adoption of smart lockers.

Compatibility

Compatibility, the second characteristic of DOI, refers to the degree to which an innovation is recognized as consistent with user's previous experiences. Rogers (2003) defined compatibility as the extent to which an innovation is perceived to be consistent with current values, experiences, and the expectations of potential adopters. In other words, it refers to the extent to which society perceives that innovation aligns effectively with traditional knowledge (Al-Rahmi et al., 2021). It entails that new innovation must be consistent with existing norms and prior experiences of potential adaptors (Okoli & Tewari, 2021).

A high level of compatibility suggests that an innovation is perceived as less uncertain by its potential adopters (Rogers, 1983). An innovation that is considered compatible with the organization's norms may be adopted faster than an innovation that is incompatible. Wang et al. (2020) found that compatibility influences users' intentions to adopt technology. Compatibility's perceived usefulness and ease of use have significant effects on the adoption of technology (Nikou, 2019).

Compatibility and IoT Security

The deployment of IoT poses some critical concerns due to the lack of industry standards due to compatibility issues (Latif et al., 2022). IoT devices are often designed with conventional architecture and design patterns that are not specific to IoT, making them not compatible with other devices on the network, and harder to maintain and secure (Washizaki et al., 2020). IoT devices in organizations can handle different kinds of data which causes another critical issue for the compatibility of the devices. Suman et al.

(2019) suggested verifying the compatibility of the devices prior to any implementation by using rule-based methods such as Semantic Web Rule Language (SWRL). Ensuring the compatibility between IoT devices is crucial since IoT-based services are enabled by connecting smart objects in the network (Shin et al., 2018). Yuen et al. (2021) discussed how compatibility is one of the most influential characteristics on IoT acceptance and adoption. To improve compatibility with previous IoT models, Ivica et al. (2021) proposed a multithreaded microcontroller to collect data from sensors. This will ensure long-term security by having a dedicated protocol that eliminates the need for device configuration outside the vicinity of the device. Sarac et al. (2021) discussed how adding a simple interface to an IoT device's security gateway architecture can provide security compatibility, decentralization, and authentication with the IoT remote service. IT leaders should have a mechanism to check the compatibility of IoT devices with their organization's security policies prior to any installation. Hamza et al. (2022) discuss how manufacturer usage description, an Internet Engineering Task Force (IETF) standard, can help manufacturing organizations in ensuring compatibility of the IoT devices with their organization security policies.

Complexity

The third attribute of DOI is complexity and refers to the degree to which an innovation can be considered as easy or difficult to understand and/or use (Rogers, 1983). Al-Rahmi et al. (2019) referred to the degree of effort viewed by the learner that affects their learning performance. In other words, the complexity of an innovation is negatively associated with its degree of adoption (Yilmaz & Olgan, 2020). The lack of ease of use

can negatively affect innovation adoption. If using an innovation requires a lot of effort from adopters to develop a new skill, this may lead to resistance. An innovation will spread rapidly when the inventor reinvents an innovation to become simpler and to the adopters to learn it (kewena & Hlebela, 2018). The complexity of innovation might lead its target customers to misunderstand its function (Min et al., 2019). Complexity exhibits an inverse correlation with perceived usefulness (Hardgrave et al., 2003). The complexity of a new technology and the barriers to its adoption increase with the amount of new knowledge individuals need to understand in order to use it (Saberi et al., 2019).

Tornatzky and Klein (1982) found that complexity is one of the major factors that influence the adoption of a range of innovations. A similar finding was also made by Al-Jabri and Sohail (2012) when evaluating the factors that drive the use of mobile phones. Innovations that have low complexity, high advantage, high compatibility, high trialability, and high observability are likely to succeed (Rogers, 2003). The complexity of technology is an important standard to measure innovation quality (Jin et al., 2022).

Complexity of IoT Security

The effect of perceived ease of use on IoT adoption can be arguable in a lot of cases (Yang, 2021). The heterogeneous nature of IoT devices raises the degree of complexity of the security requirements, which increases the risk on the organizations (Jing et al., 2014). The development of IoT will increase the complexity of the security system (Soewito & Marcellinus, 2021). The security for IoT is more complex than for usual systems, because of the limitation of processor, memory, and energy in IoT devices (Kaedi & Ghaznavi-Ghoushchi, 2018). The complexity of large-scale IoT systems

introduces numerous security vulnerabilities and design challenges, given IoT's crucial role in supporting diverse applications by connecting heterogeneous devices, machines, and industry processes (Fang & Wang, 2020). As the IoT systems are getting larger due to the tremendous increase of connected devices, there is a need for reducing complexity to better detect attacks (Dibaei et al., 2020).

Due to the complexity of the IoT, it is hard to create procedures for security detection and threat awareness in it. There are still a lot of challenges to build a secure complex IoT systems (Shuqin et al., 2021). Apart from the complex security challenges of IoT, the heterogeneous data transfer between IoT devices further aggravates its structural complexity (Song et al., 2020). IoT systems working across multiple layers makes them complex and harder to secure because vulnerability across these layers can lead to system breach or failure (Fang et al., 2021). Lack of standardization and the limited control over the built-in security features of IoT devices can be problematic to IT leaders, as it increases the operational costs because it requires the involvement of different experts and tools in order to manage, monitor, and secure heterogeneous devices (Roe et al., 2022).

Trialability

The fourth attribute of DOI is trialability, which refers to allowing technology to be experimented before its permanent adoption (Rogers, 2003). In other words, it is the degree to which potential adopters perceive that they can experiment with the innovation prior to committing to it (Moore & Benbasat, 1991). Trialability helps the users with the anticipation of innovation by gaining more exposure into the solution. Adoption is a

learning experience, and the more the user can learn about the innovation, the more likely they are to adopt (Arvidsson, 2014). According to Rogers (1983), as the users gain more insight, the levels of uncertainty will decrease and the importance of trialability will decline. Earlier users see the trialability attribute of innovations as more essential than later users. If the users are given the opportunity to experiment with the innovation, the likelihood of adopting will increase. The larger the scope of the trial, the more likely of adoption (Lee et al., 2011). Users tend to try the innovation before considering adopting it tend to have less uncertainty (Al-Rahmi et al., 2019), which further enhances the adoption and use (Yang, 2021). Also, it reduces the risk of adoption, which encourages its diffusion (Shin, 2019).

Trialability of IoT Security

Trialability is the degree to which users trust the likelihood of experiencing technology before deciding on the adoption. An innovation that is triable provides little to no doubt to the users (Al-Rahmi et al., 2021). Trialability positively influences the perception of security. The ability to try an innovation before adoption can help the user to overcome security concerns (Johnson et al., 2018). Customer expectations regarding IoT have started to transition from being focused solely on products to emphasizing more experiential aspects. As users gain experience with IoT, they become more familiar with its security features and limitations. IoT systems are complex, which makes it complicated for potential adopters to understand their benefits without trying them before (Sorri et al., 2022). Given that innovations necessitate investment in resources, time, and energy, those that are tested prior to implementation are readily embraced (Tortorella et

al., 2021). IT leaders should first pursue testing an IoT security solution to see how it can benefit the organization and then make a favorable decision towards using it, as it takes time and effort to experience the solution and its benefits.

Observability

The fifth and last characteristic of DOI is observability. It is defined as "the degree to which the results of an innovation are visible to others" (Rogers, 2003). The tangible results provided by innovation can be a significant predictor of technology adoption. Not everyone adopts an innovation immediately; some potential and later adaptors rely on seeing early adopters using innovation. If potential adopters do not see an innovation used by others, they are less likely to adopt it themselves (Menzli et al., 2022). Consumers are more likely to adopt new innovations when seeing their benefits (Min et al., 2019). When an individual witnesses the beneficial impacts of a technology, they are more inclined to utilize it (Rogers, 1995). Impacts of an innovation that are unobservable are difficult to comprehend (Warner et al., 2020). The more positive outcomes innovation provides, the higher the chance of adoption (Tortorella et al., 2021). Observability has a significant positive impact on perceived usefulness (Lee et al., 2011). Al-Rahmi et al. (2019) mentioned that users' attitude toward using innovation is highly influenced by observability. Rogers (2003) suggests that the observability of successes can positively support an innovation uptake.

Observability of IoT Security

In their review, Wamba et al. (2013) found that DOI theory is the most popular approach when studying IoT adoption. Rogers (1995) emphasized that DOI hinges on

human capital, observing that the adopters are approximately distributed over time. Perceived security can be influenced by users' observations during system trials. Users must attribute their performance to using IoT in order for it to gain acceptance and adoption (Yang, 2021). Security is a significant challenge for customers adopting IoT, as these devices lack a graphical user interface for users to learn about any infection and take remediation actions. The main objective of IoT security is to protect the privacy of the customers and their data integrity, confidentiality, and availability (Litoussi et al., 2020). There are multiple promising security solutions being adopted in the IoT domain to reduce and mitigate threats (Barbareschi et al., 2021). Cirne et al. (2022) suggests promoting the adoption of security measures using IoT devices and systems certification. It was observed that malicious chipsets and electronic components are inserted into devices during manufacturing to compromise the integrity of the IoT devices (Rondon et al., 2022). The level of IoT devices security indicates that malicious acts by hackers are not successful and privacy is the key to increasing the adoption of an innovation. (Padyab et al., 2019). While the adoption process of IoT has been an ongoing phenomenon over the past few years, organizations still need to adjust to successfully secure their IoT devices.

The five characteristics of the DOI theory influenced this study. The innovations that have these five characteristics are more likely to succeed over innovations that do not. These characteristics served as a framework to understand security strategies to enable the adoption of IoT devices in the manufacturing sector. Adoption is the process of selecting a technology for the organization and implementing it for use by its

employees (Damanpour et al., 2018). One of the main reasons for adoption and diffusion can be traced back to the simplicity of the solution. It is the IT leaders' responsibility to select the proper solutions for their organizations. Having a great solution yet very complex to implement might not be the right choice.

The DOI theory is concerned with how innovations such as security strategies are diffused over time. When an organization determines to adopt an innovation, it enters the intention stage of the DOI theory. As the organization becomes more knowledgeable and gains more experience through the intention stage, it enters the next stage which is called the adoption stage (Martins et al., 2016). With the help of the five characteristics of DOI theory, IT leaders can assess the likelihood of success or failure of the solutions.

Cyber security is considered to be one of the most important issues related to IoT in the manufacturing sector. IoT devices are an attractive target to hackers because they are less secure, might contain confidential information, and have a huge impact on the operation of the organization (Cangea, 2019). IT leaders in the manufacturing sector will be the ultimate beneficiaries of the solutions and strategies identified in this study, as they will become informed of the recent IoT security issues and their solutions that could be used to enable the adoption of IoT devices in the manufacturing sector.

IT leaders should consider the five characteristics of the DOI theory when setting up IoT security strategies. IT leaders should consider factors such as the visibility of security measures, the level of transparency in the implementation process, the level of technical expertise requires, the level of ongoing maintenance required, the compatibility of security measures with existing devices, and the ease of integration with existing

systems. Furthermore, IoT security strategies must provide opportunities for trial and experimentation to encourage adoption and demonstrate the benefits of IoT security in terms of cost savings, improving efficiency, and enhancing data protection.

Analysis of Contrasting Theories

In addition to DOI, I reviewed other theories that are related to information security and technology:

Technology Threat Avoidance Theory (TTAT). Liang and Xue (2009) developed TTAT by synthesizing literature from diverse areas, including information systems and risk analysis. TTAT explains how and why individual IT users engage in threat avoidance behaviors. It provides a framework at the user level instead of at the organizational level. TTAT assumes that when employees notice that an IT threat exists, they will be motivated to avoid it by taking safeguarding measures actively.

The theory posits that IT threat prevention behavior can be represented by a cybernetic process. The users aim to enlarge the distance between their current security state and the undesired end state. Furthermore, users appraise if the IT threat exists and to what degree it exists. Then they agree on methods and actions to help prevent the threat. TTAT proposes that users consider the following factors to assess the extent of threat avoidance: the usefulness of the safeguarding measure, the costs of the measure, and users' capability in applying the measure (carpenter et al., 2019).

TTAT can assist IT leaders in raising security awareness by providing guidelines for IT practices and educating employees about IT threats (Chen & Liang, 2019). I chose

DOI over TTAT because TTAT focuses on educating why users actively and passively respond to IT threats and, as such, it is not the focus of my research.

Technology Acceptance Model (TAM). Davis developed TAM in 1986 based on the Theory of Reasoned Action (TRA) and the Theory of Planned Behavior (TPB). In TAM there are two factors that affect an individual's attitude towards using the technology: perceived usefulness (PU), and perceived ease of use (PEOU) (Davis, 1986). PU refers to the beliefs of a user that using this product or technology will improve his job performance. Whereas PEOU refers to the degree to which learning the product or technology will require minimum effort. In other words, TAM emphasizes the perceptions of the potential user. The creator might believe its product is useful and user-friendly, however, if the potential users do not share the same belief, they might not accept the product (Mezhuyev et al., 2019).

David developed the model for testing the acceptance of new information system by users. TAM helps explain why users adopt or do not adopt a particular information system. While TAM has been criticized on a number of grounds, it serves as a useful general framework, and it has been applied by many researchers to different domains outside information system. TAM is very similar to DOI when it comes to attempting to understand acceptance and diffusion of technology. However, TAM does not include characteristics such as complexity and compatibility which are critical for the manufacturing environment and IoT. As such, DOI is better suited for my research than TAM.

Internet of Things

IoT Defined

IoT is defined as the network or things empowered with limited computation, storage, and communication capabilities as well as embedded with electronics, software, and network connectivity that enables these objects to collect, process, and exchange data. IoT devices are connected to the internet, machine to machine, and machine to humans (Al Reshan, 2021). IoT is closely related to operational technology (OT) and IT. The term *OT* comprises the technology related to managing, monitoring, and controlling industrial control systems from manufacturing to transportation and utilities (Lindstrom et al., 2019). Whereas the term *IT* is used for data-centric computing. With the IT and OT convergence, IoT has emerged as the unifying umbrella (Alsheikh et al., 2022). IoT is a collection of multiple converging technologies that enable real-world objects with speech, vision, hearing, and/or touch capabilities to perform repetitive jobs accurately (Trappey et al., 2021). IoT is a computing concept with three pillards: identifiability, communication, and interaction, in which the internet-enabled physical objects are in full communication with each other to gain greater value through exchanging data (Cui et al., 2021).

Most of the early IoT devices were created by simply equipping them with existing objects such as sensors and tag readers to facilitate the collection of information (Lu et al., 2018). IoT extends the capability of objects referred to as “things” to connect to the internet. Things are split into three categories. Smart things are physical objects such as watches enriched with communication and processing capabilities. Sensor things

are objects that perform sensing and/or actuating functions. And gateway things are objects that possess lightweight processing capabilities such as Raspberry Pi (Alkhabbas et al., 2019). A typical IoT infrastructure consists of multiple low-processing electronic devices connected to each other and the internet (Bigini et al., 2020). IoT represents the transition from a computer network to a network of objects.

The uses of IoT devices have been growing exponentially in the last decade, especially in the manufacturing industry due to the intense market competition which forces traditional manufacturers to continuously reform IoT technology in order to stay competitive (Liu et al., 2022c). Huang et al. (2019) discuss how IoT has made it easy for manufacturers to obtain production data in real-time which facilitates production management and optimize decision. IoT is considered the next technological mega-trend connecting billions of devices from home equipment to industrial equipment to the internet across multiple sectors (Hamza et al., 2022).

IoT plays an important role in the era of Industry 4.0 (Cavalieri et al., 2022). Industry 4.0 initiatives place emphasis on IT-based manufacturing. Its concepts are to link machines and systems in order to communicate in real-time and increase efficiency (Trappey et al., 2021). It has transformed manufacturing to be more productive, adaptable, and marketable. The rapid advancement of IoT has provided manufacturers with the ability to monitor operation processes and automate fault detection and predictive maintenance systems (Liu et al., 2022a). Smart manufacturing enhances efficiency, quality, and reliability in delivering new services and products to customers,

all facilitated by IoT and predictive maintenance with the leveraging condition monitoring to detect anomalies (Compare, et al., 2020).

Fetah et al. (2022) highlight the opportunities that IoT brings for solving most of today's problems, from transportation, smart cities, agriculture, healthcare, and manufacturing. IoT aims at improving life quality for the users and supporting general purpose operations (Akpakwu et al., 2017). It is capable of handling production in an efficient way and is less prone to disruption due to its capability of predictive maintenance (Aly et al., 2021). IoT integration improves manual systems and provides productivity insight (Bataineh et al., 2022). Manufacturers have found that effective supply chain management is crucial for the business. IoT systems are being implemented to effectively drive supply chain and predict the future market, also to improve workplace safety. The supply chain has become more and more complex, which makes traceability and integrity harder to ensure. Bala and Kaur (2022) suggest incorporating IoT with Blockchain technology to provide more reliability, security, transability, and cost efficiency into the supply chain. Manufactures can dramatically reduce safety related incidents by adopting IoT technologies. It can be used to monitor and manage different types of hazards, safety of plants, and safety of workers (Gnoni et al., 2020).

Walas and Redchuk (2021) explored the work regarding IoT and Artificial Intelligence under Industry 4.0. ML is considered to be one of the most suitable examples to provide embedded intelligence in IoT devices. ML can help IoT devices to make decisions or behave based on the knowledge and the data collected from the machines to tackle certain problems. IoT is the enabler technology to help in behavior pattern sensing

and controlling, as well as in data-driven decision-making. The big volumes of data collected by IoT devices can be used by intelligent tools for real time decision making (Bala & Kaur, 2022).

The huge scale of IoT networks and type of data collected by these devices brings new challenges such as management of these devices, security, and privacy. The fact that IoT devices are connected to the internet and use enabling technologies such as Cloud Computing (CC) and Software Defined Networking (SDN), increases the landscape of threats. The heterogeneity of IoT and data collected creates compatibility challenges due to hardware and software components. IoT devices don't use the same operating systems and do not have the same peripherals or use the same protocols. Additionally, it is hard to process and manage different types of data generate from diverse IoT applications (Hussain et al., 2020). Organizations are struggling in finding the right solutions to secure their IoT network. As IoT devices run on lightweight operating system, which makes it difficult to find security patches for many of the vulnerabilities (George & Thampi, 2022). The sensing and actuating objects in IoT generate mass amount of data (Alazab et al., 2022). Furthermore, IoT devices can be accessed from anywhere, which makes them more vulnerable to attacks. As IoT carries more and more private and valuable information, the impact of attacks is getting higher (Tahsien et al., 2020).

IoT Architecture

IoT architectures vary significantly depending on the solution that is to be implemented. Different architects have been used for IoT, such as three-layer or basic IoT architecture, four-layer, middle-ware-based architecture, service-oriented

architecture, and five-layer (Mrabet et al., 2020). The most basic and widely accepted format is the three-layer architecture: Perception, network, and application.

The perception or sensing layer is the first layer of IoT architecture. It is mainly divided into sensing and identification technologies, where the sensors and connected devices come into play as they collect data and information from the environment (Al Reshan, 2021). The components of the sensing layer mainly consist of sensor technologies such as Quick Response (QR) code, Radio-Frequency Identification (RFID), Wireless Sensor and Actuator Network (WSAN), and Wireless Body Area Network (WBAN). Sensors can be used to monitor and detect events or changes in its environment before relaying the information to the network layer and the application layer.

QR code is a two-dimensional barcode that can contain information about a product or item. The QR code sensor extracts the information from the presented two-dimensional barcode. It mainly consists of position detection, format, and data information. The QR code finds extensive application in automated storage and retrieval systems, as well as in mobile payment solutions (Li et al., 2022). RFID uses electromagnetic fields to identify and track tags that can be attached to objects. RFID can be categorized as passive and active. Passive RFID does not need to require power, whereas active requires some sort of power. With the help of RFID, manufacturers can increase the accuracy of product tracking and improve their productivity (Rungruengkultorn & Boonsiri, 2022). A WSAN is a group of sensors and actuators that gather information about their environment. WSAN can provide peer-to-peer high radio coverage and higher processing for the data coming from the sensors (Filho et al., 2018).

WBAN is defined as a set of sensors implemented in or on patients' bodies to monitor health parameters such as temperature, glucose level, blood pressure, and even physiological signals (Samanta & Nguyen, 2022). The perception layer might also handle modulation and demodulation, encryption and decryption, and frequency selection. Some of the challenges of this layer are security, interoperability, and energy utilization.

The second IoT architecture layer is the network layer. It is a collection of different communication technologies whose main job is routing and transferring the data that is collected by the sensing layer to the application layer. The network layer connects the sensors, smart objects, servers, and network devices altogether through network technologies and protocols (Tahsein et al., 2020). The connections between different objects can be divided into two types: interlinks and intralinks. Interlinks is any type of communication between devices, while the intralinks is the type of communication with the infrastructure and/or the cloud (Chen et al., 2020). Some of the technologies used in this layer are Wi-Fi, ZigBee, Cellular, Bluetooth, LoRa, and Halow.

Wi-Fi is one of the most common and robust wireless technology. Wi-Fi protocols focus on optimizing bandwidth and transmission rate. However, Wi-Fi might not be the ideal solution as it consumes more energy than the other wireless technologies (Lee et al., 2022). Smart factory is one of the key concepts within Industry 4.0, which requires intelligent systems that are fully connected to all manufacturing devices. Cellular technology such as 5G play a key role in the improving communication and the implementation of Industry 4.0 (Saafi et al., 2021). 5G networks have been designed to support complex environments including IoT in an industrial setup (Candal-Ventureira et

al., 2021). Bluetooth provides a low-energy solution for short-range transmission and has become one of the predominant technologies for connecting IoT. However, Bluetooth has many security vulnerabilities (Angela et al., 2018). Security, power utilization, and availability are some of the network layer challenging issues.

The application layer is the third layer and is what the user interacts with to access data that is collected by the sensors. This layer aggregated data and presents smart services to help users identify current trends and make the right decisions (Al Reshan, 2021). Various application protocols are developed specifically for this layer to meet the IoT requirement in terms of low processing and power consumption, such as Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol (CoAP), and Data Distribution Service (DDS).

IoT has driven the efforts of digital transformation. MQTT is a protocol used by IoT devices and low bandwidth networks. It was originally developed as a solution to monitor multiple stations and oil pipelines in remote areas with low-reliability connections (Mazur et al., 2022). CoAP is a bandwidth-efficient protocol with a reduced overhead packet that is designed for data transmission between the application layer and the sensing layer (Makarem et al., 2022). DDS protocol provides a standard data-centric programming model for distributed systems (Tekinerdogan et al., 2018). Some of the application layer challenges are privacy and security of user data, compliance with regulations, and data management (Iqbal et al., 2020). The biggest and most common challenging factor across all IoT layers is security.

IoT Security Issues

IoT has revolutionized the way many industries operate. However, security challenges act as a barrier to the adoption and diffusion of IoT. The type of data collected by IoT devices in manufacturing, infrastructure, and medical sectors has further security ramifications (Roe et al., 2022). In a lot of situations, IoT could have life-threatening effects if it is not properly secured. Hackers could take advantage of vulnerabilities in IoT devices to disrupt services such as water and electricity supply, harm nuclear power plants, and even shut down hospitals, leaving thousands, if not millions, of people without access to resources or medical care.

The lack of standardization of IoT technologies with intrinsic vulnerabilities and the increase of interconnectivity increases the security risk. As the size of the IoT network exponentially increases, the security issues of IoT come to light (Hamza et al., 2022). IoT devices lack memory and processing power, limiting the security measurements that can be implemented and system updates. The constraints in the capacity of processing and power lead to the limited ability to run some cryptographic protocols. Cryptography is a security mechanism that protects information and communication through the use of codes. Using weak cryptographic protocols puts the data stored in the sensor network at risk. Industry 4.0 IoT devices handle large volumes of sensitive data, making them a target for many attackers (Velliangiri et al., 2022).

The heterogeneous nature of IoT makes it hard to implement one integrated security solution for all the devices on the network. Furthermore, the lack of security consideration when designing and manufacturing IoT devices causes major security

issues. Manufacturers tend to focus on the features of their products and making them appealing to customers, which makes security less priority for them. Hogewoning (2018) states that expecting manufacturers to produce IoT devices completely free of bugs is unrealistic. Many IoT devices are shipped directly from the factory with outdated pre-installed software that is missing critical security patches. Alsheikh et al. (2022) discussed how hackers use search engines like Shodan, Zoomeye, and Censys to find vulnerable IoT devices such as power plants, traffic lights, surveillance cameras, and even medical devices. As a result, IoT continues to be a viable and popular target for malicious actors. In sum, IoT is not sufficiently regulated to maintain the security of information, and in the wrong hands, it can cause extreme damage to the users (Hu et al., 2018).

IoT became a playground for security attacks ranging from simple hacks for home devices to well-coordinated hacks targeting sectors, industries, and even governments. The environment that IoT operates in might pose additional security challenges (Hussain et al., 2020). The network structure is similar across all industries; however, there is more risk of widespread disruption from third-party threats in the manufacturing industry due to the OT convergence. Yet, many manufacturing organizations are behind when it comes to security. Heritage (2019) highlighted that regular patching is still highly problematic because of the long replacement cycles of OT devices in manufacturers that prioritizes uptime above cyber risk.

There are two main types of attacks: active attacks and passive attacks. In a passive attack, the attacker monitors and observes the data or systems without modifying

them. The victim does not know about its occurrence as it does not impact the system's resources. Eavesdropping and traffic analysis are good examples of passive attacks that can be used through an IoT network. In an active attack, the attacker alters the data and directly impacts the system's resources. Active attacks such as DoS, MITM, and data tampering threaten the integrity and accessibility of IoT (Tahsien et al., 2020). A new type of attack has recently emerged based due to technological advances. This new type is called a smart attack, which is less dependent on human actors and more reactive to countermeasures. ML-based smart attacks have drastically changed the threat landscape. Attackers can use open-source frameworks such as Open Ai-Gym and Tensorflow to create ML-based attacks with little knowledge of ML (Bout et al., 2022).

IoT has been expanding exponentially over the last few years, so the threats are emerging at the same rate as IoT expansion. The compromised IoT devices are the primary sources from where the attacker initiates their attacks. Almost every layer of the IoT architecture is vulnerable to attacks. The sensors collect data directly and are the most vulnerable interface of the IoT architecture, which makes sensing layer threats the most significant. Attackers take advantage of sensors' vulnerabilities to inject malicious code and capture sensitive data (Al Reshan, 2021).

Some threats at the perception layer are eavesdropping, battery drainage attacks, node cloning, tampering, and RF jamming attacks. Eavesdropping attacks can pose a challenging threat to the privacy of IoT devices. It uses malicious devices to connect to IoT devices for passive sniffing of traffic to gain confidential information, which consequently affects basic user rights (Anajemba et al., 2022). Most IoT devices are

resource constraints, especially those that use the battery as the main power source. A drainage battery attack or sleep deficiency attack occurs when the attacker sends many request messages to the IoT device to prevent it from entering sleep or energy-saving mode and drain its battery (Kumar et al., 2020).

Due to the lack of standardization in IoT, the manufacturer can easily forge and duplicate IoT devices. An insider attacker can clone or swap a legitimate device with modified devices with overwritten parameters or firmware that perform different attacks (Iqbal et al., 2020). Tampering attacks are continuously increasing against IoT devices. Attackers violate the integrity of IoT by tampering with its hardware features and gaining access to it (Mastorakis et a., 2021). Wireless communications are vulnerable to a wide range of attacks that are hard to detect. RF jamming is another attack that can be conducted on the sensing layer; it can overload the wireless medium leading to packet losses (Kosmanos et al., 2021).

The network layer is another area of security concern. Its job is to get the network packets from the sources to the destination. However, it is still susceptible to many attacks as it connects different LANs together. The attacks target the communication aspects and exploit the resource constraints of IoT devices, and the lack of sophisticated authentication methods used (Hussain et al., 2020). Many attacks that can be used on the perception layer can also be used on the network layer. The less secure wireless protocols used in IoT, such as ZigBee, SigFox, 802.11X, and LoRa are also vulnerable to attacks like DoS and Spoofing (Mazhar et al., 2021).

Eavesdropping on the network can pose a challenging threat to IoT privacy. The more IoT devices generate private information, the more subtle it is to eavesdropping and other network attacks (Anajemba et al., 2022). Attackers can modify and resend network packets to poison network traffic. Spoofing happens when attackers disguise themselves as trusted sources to access confidential information. Spoofing can cause severe damage to time dependent IoT devices, such as robotic arms, in the manufacturing sector (Khan et al., 2022). Sybil attack is performed using IoT devices with multiple fake identities to outnumber the real network nodes and compromise the IoT devices' effectiveness (Arshad et al., 2021).

Flooding attacks are one of the most common types of attacks that target the IoT network. Flooding attacks reduce the speed of traffic flowing to and from IoT nodes by occupying the Domain Name System (DNS) (Mahjabin et al., 2022). The sinkhole is another attack in which data traffic is lured and redirected to go through a malicious node (Fahad et al., 2019). This attack makes it possible to conduct other attacks, such as selective forwarding, that affect the communications between devices by reducing network traffic or corrupting data packets (Tournier et al., 2021). A wormhole is also one of the routing attacks that can cause serious damage if combined with other attacks. It aims to give the attacker advantages over the other nodes' traffic (Kaliyar et al., 2020).

Operating systems are similar to traditional network devices, whereas, in the IoT ecosystem, operating systems are very customized and diversified due to a lack of standardizations. IoT operating systems suffer from errors that lead to security vulnerabilities (Al-Boghdady et al., 2021). The resource constraint of IoT devices refrains

from implementing a lot of application-based security, such as software updates, security patches, and access control. Gaining unauthorized access to IoT devices is becoming easier than ever due to the default passwords across many applications. Developers intentionally implement insecure APIs for remote access (Iqbal et al., 2020).

The vulnerabilities of software used in IoT can be a great cause of a compromised system (Mazhar et al., 2021). A lot of application developers focus on the effectiveness of the IoT product rather than on its security due to the limited timeline and budget. IoT applications are relatively lucrative targets and can be compromised without much effort. Some of the attacks on the application layer include but are not limited to, malware attacks, DoS, buffer overflow attacks, SQL Injection, Cross Site Scripting (XSS), and side-channel attacks. A common theme in application attacks is exploiting vulnerabilities and using them to inject and execute malicious code and gather confidential information (Xu et al., 2018).

A buffer overflow is one of the most used attacks on the application layer. It enables the attacker to inject more data than the buffer allows (Teixeira et al., 2019). One of the known database attacks is SQL injection. Although this attack is commonly used to target web applications, it can target any database whether it is on servers or IoT devices (Bedeković et al., 2022). Cybercriminals can modify or delete any data in the database tables by exploiting vulnerabilities through specially prepared data input (Kasim, 2021). IoT is also susceptible to XSS attacks, where attackers inject malicious scripts into the web application displayed to different users (Mokbal et al., 2021). In the manufacturing sector and in many cases, IoT devices are placed in relatively open areas accessible by

many people, making them an easy target for side-channel attacks (Peng et al., 2021). A side-channel attack defeats traditional cryptography during application execution by revealing passwords from memory (Salehi et al., 2022).

IoT Security Solutions

Undoubtedly one of the main issues of IoT is security. It is important to address security concerns to protect the confidentiality, integrity, and availability (CIA) triad of IoT devices (Al Reshan, 2021). Confidentiality ensures that access is granted to only authorized users. It concerns protecting the customer's sensitive information from unauthorized disclosure. A failure in confidentiality can cause serious financial and reputation damage to the organization, especially lately with all the regulations and laws, such as Health Insurance Portability and Accountability Act (HIPPA), Payment Card Industry Data Security Standard (PCI-DSS), California Consumer Privacy Act (CCPA), and Gramm-Leach-Bliley Act (GLBA). Implementing adequate Identity and Access Management (IAM) combined with encryption, multi-factor authentication (MFA), and data loss prevention (DLP) solutions can protect the confidentiality of the IoT systems and data (Wang & Mu, 2021).

Integrity, on the other hand, involves maintaining the accuracy and trustworthiness of data at rest and in transit. It also ensures that only authentic and authorized users change the data. Integrity can be protected using appropriate cryptography and data manipulation prevention solutions (Halabi & Bellaiche, 2018). Availability describes the ability of the data and service to be accessible for the users at any time. It is crucial to maintain the availability of IoT devices in sectors such as

utilities, manufacturing, and medical, where IoT provides critical services that require high levels of availability with minimum to no interruption (Lopez-Pena et al., 2020). IoT system availability can be improved by implementing security measures to mitigate threats like malware and DoS (Shen et al., 2022).

Cryptographic solutions help protect the IoT from outside threats and prevent the disclosure of confidential information to any unauthorized entity (Vijavakumara et al., 2020). Cryptography techniques applied to the network layer can secure data during communication through public channels (Pal et al., 2022). Yu et al. (2019) proposed using a data leakage prevention model based on graph fusion that can be deployed for IoT. IAM enables efficient resource discovery and facilitates the management of IoT and users. IT managers can control and access these resources using access control mechanisms to protect them from unauthorized access (Nath & Nath, 2022).

Intrusion detection and prevention systems (IPS) act as a line of defense against outside attacks, such as malware and DoS attempting to exploit vulnerabilities in IoT devices. There are two types of IPS, host-based and network-based. Due to the resource constraints of IoT devices, network based IPS is the better option (Agyemang et al., 2020). IPS is an efficient security technique that identifies and prevents attacks by analyzing data traffic. It is a greater countermeasure to the MITM attack. However, many existing IPS have high computational costs and cannot handle zero-day wireless intrusions in IoT. Davahli et al. (2020) provide a lightweight anomaly detection model called LIDS for wireless sensor networks (WSNs) in IoT.

The resource limitations of IT can also be challenging when implementing encryption, as generic algorithms cannot be used. There is a trivial need for lightweight cryptographic algorithms with a balance between security computing resource consumption, such as mCrypton and SEA (Ning et al., 2020). Securing IoT devices requires innovation at the processor level using software libraries and dedicated security hardware, as some threats cannot be defeated by just using software solutions (El Hadj Youssef et al., 2022).

Various solutions have been proposed to overcome security issues at the perception and network layers. Liu et al. (2022b) proposed a lightweight transmission mechanism to secure data exchange in IoT networks from eavesdropping attacks. Li et al. (2022) designed a novel authentication model to tackle authentication issues in wireless IoT by utilizing blockchain. To tackle privacy concerns in cloudlet-assisted wireless networks, Yin et al. (2018a) explored an adapted offloading scheme for IoT. Noshouhi et al. (2022) proposed a lightweight security solution for the detection of wireless spoofing attacks in 5G mmWave used in IoT networks.

DDoS has become a significant threat to IoT devices. Some of the traditional countermeasures for DDoS, such as D-WARD, Ingress/Egress filtering, Hop Count Filtering, and SYN-Cookies, are applied at the gateways, routers, and entry points of the networks (Mrabet et al., 2020). However, due to the different architectures of IoT, it is hard to devise a unified mechanism to combat DDoS attacks. Lee et al. (2021) suggested setting up a multi-level defense system with multi-hierarchical security equipment for communication protocols L2 and L7 to counter DDOS attacks on IoT devices. Abidoye

and Obagbuwa (2018) proposed a unique method called message analyzer scheme (MSA) to protect against DDoS attacks in WSNs, by adopting a hash function and encryption to ensure the authenticity and integrity of the data. There is limited research on how to improve the security of the IoT with software-defined networking (SDN). Yin et al. (2018b) proposed an algorithm for detecting and mitigating DDoS attacks with SDN by finding the real attacker within a short period and blocking the attacker at the source. Enabling technologies such as fog and cloud computing have also been used to improve the detection of DDoS attacks on IoT. Yan et al. (2018) presented a fog and cloud computing-based DDoS mitigation framework that uses SDN gateways to protect IoT nodes.

Authentication and access control mechanisms are some of the leading security requirements in IoT. However, they are also equally challenging to implement due to the resource constraints and the heterogeneity of IoT devices. IoT devices must be authenticated when joining the network to ensure the organization's security. Trusted authenticated devices or the gateway can facilitate the authentication of the new devices. Pham and Dang (2021) propose a lightweight authentication protocol based on elliptic curve cryptography (ECC) to achieve security in a distributed network as well as between devices while minimizing resource consumption. Access control mechanisms define the functions that implement the controls forced by the policy. Some of the well-known access controls that can be used to secure IoT devices are access control lists (ACL), extensible access control markup language (XACML), open authorization (OAuth), and user-managed access (UMA). Ouaddah et al. (2017) highlighted the advantages and

challenges of existing access control solutions and their usability in the IoT domain. Drame-Maigne et al. (2021) proposed four architectures for access control and discussed the benefits of each to the IoT environment.

Due to the nature of the IoT environment, as explained earlier, verifying the integrity of the IoT devices on the network is essential. Lightweight Remote Attestation (RA) methods allow the IoT devices to authenticate themselves on the network. A hardware-based RA requires trusted hardware, such as Trusted Platform Modules (TPMs), to generate attestation results, whereas software-based RA requires no additional trusted hardware. However, it is less secure than hardware-based RA (Kumar et al., 2022). Shah et al. (2021) presented a novel lightweight continuous authentication protocol for IoT based on the Zero Trust Architecture (ZTA) approach from NIST Special Publication 800-207. ZTA is a manifestation of the key access control principle of the least privileged, where zero trust is the norm.

Malware and Malicious code injection are one of the most infamous attacks on IoT devices that exploit existing vulnerabilities. It is challenging to stay on top of different types of malwares and their detection techniques. There are two main types of detection techniques: static or code analysis and dynamic or behavioral analysis. Static is the process of analyzing the binary of malware without running. Whereas in dynamic, the analysis is performed while the malware runs on a host system or sandbox environment (Catalano et al., 2022). The traditional malware detection techniques are no longer effective against sophisticated malware that target IoT devices. Here are some of the dynamic analysis techniques: Anubis, Cuckoo, CWSandbox, and BareCLoud. Noor et al.

(2018) presented a novel technique called AEMS based on a Cuckoo sandbox to detect malware evasive behavior. Masabo et al. (2018) compared techniques that can be used to detect polymorphic malware, such as topological features-based extraction, sequence classification detection, string matching, and substitution matrices, client-server-based detection, viral polymorphic malware detection, and hybrid clustering detection approach. Similarly, Maniriho et al. (2022) provided a comprehensive list of tools for performing dynamic analysis, memory analysis, and ML and deep learning techniques to detect malware. And Souri et al. (2018) presented a survey of malware detection approaches using data mining techniques. The authors categories the techniques into two: signature-based and behavior-based approaches.

Arshad et al. (2021) discussed the limitations and advantages of different Sybil attack countermeasures such as Cryptography, Received Signal Strength Indicator (RSSI), Trust, and AI. Whereas Kim et al. (2022) focused on the RSSI countermeasures in their article by proposing a Physical ID-based trust path routing (PITrust) scheme to improve detect and isolate Sybil attacks in Low-Power and Lossy Networks (RPL). Pu and Choo (2021) investigated Sybil attacks in IoT and proposed lightweight detection as a countermeasure. The mechanism is based on Bloom Filter and Physical Unclonable Function (PUF). Similarly, Kaliyar et al. (2020) discussed the significant security threats for RPL-based IoT and propose detection approaches against Sybil and Wormhole attacks by using Highest Rank Common Ancestor (HRCA) concept.

ML flexibility and the ability to evolve have been very beneficial in IoT security. It has been used in various tasks and applications, such as classification, fraud detection,

malware, intrusion detection, authentication, access control, and DDoS avoidance (Hussain et al., 2020). In this context, Esmalifalak et al. (2017) used ML techniques such as support vector machine (SVM) and principal component analysis (PCA) to detect stealthy attacks and isolate the tampered data from the normal data. Pajouh et al. (2018) proposed an RNN-based DL that uses LSTM structures to analyze IoT malware based on their OpCodes sequence. The authors train their models by using malware with three different configurations. Meidan et al. (2018) used autoencoders to detect and isolate anomalous network behavior, such as botnet attacks in IoT. However, this approach requires extensive training in order to detect any new malware.

Blockchain is another emerging technology that can be used to create a decentralized, reliable, and secure IoT environment (Shammar et al., 2021). Said (2022) proposed a lightweight Blockchain-Based Security scheme (LBSS) that enhances IoT devices' confidentiality, integrity, and availability. Bataineh et al. (2022) proposed an Enhanced Rich-Thin-Client architecture (ERTCA) solution to ensure data privacy and security while addressing the resource limitations of IoT devices.

Some of the essential steps for IoT security can be summarized as follows: security by design should be embedded into the IoT development rather than as an afterthought. Defense-in-depth and zero-trust approaches are equally important to the security of IoT devices. Authentication and access control mechanisms, ML, Blockchain, and cryptography technologies can be used to provide secure communication and protect against malware attacks. Lastly, the use of PUF can give a better countermeasure against hardware-based attacks (Alsheikh et al., 2022).

Relationship of This Study to Previous Research

Rogers's DOI theory is one of the most popular theories for studying adoption in information technologies. It has also been studied extensively to adopt innovation in various fields, such as marketing, agriculture, and education (Mehra et al., 2020). Researchers have used the DOI theory to explain the spread of innovations, as adoption is not necessarily based on innovations' effectiveness. Lu (2022) used DOI theory to understand IoT acceptance and adoption better. Researchers often use DOI theory in conjunction with other behavioral models like the Theory of Reasoned Action (TRA) and the Technology Adoption Model (TAM) (Pal et a., 2021). Using DOI theory, Nikou (2019) has investigated the effect of perceived consumer innovativeness and the perceived cost on the intention to adopt the technology.

The DOI theory is primarily based on the characteristics of the technology and how the users perceive innovation (Rogers, 2003). Al-Rahmi et al. (2021) assed the adoption of IT using the five DOI attributes: relative advantage, compatibility, complexity, trialability, and observability. Researchers have used the theory in an incredibly diverse range of applications. One of the most critical factors for diffusion is how well the innovations are communicated to different parts of society. The researchers appear to implement the DOI theory during the COVID-19 pandemic to assess the impact of IoT on social change and people's daily lives (Attié & Meyer-Waarden, 2022). DOI explains the diffusion process from start to finish from the user's attitudes (Rogers, 2003). Researchers have used the DOI theory to design studies that report user

experiences. Implementing the theory allowed a thorough analysis of the impact of IoT on patient safety (Yesmin et al., 2022).

Researchers have also applied the DOI theory to explain the adoption of technology within a firm. Want et al. (2021) illustrated the use of the DOI theory based three-stages from the view of manufacturing enterprises. Recently, industry 4.0 has diffused the digitalization of many functional areas in the manufacturing sector by bringing disruption innovation. Tortorella et al. (2021) illustrated the use of the DOI characteristics in integrating a maintenance management approach based on lean principles with industry 4.0.

Research has shown the most three factors that influence the adoption of innovation in an organization are the following: leadership attitude toward change, the complexity of the organization, and the external characteristics of the organization (Correia Simoes et al., 2020). The researchers indicated that attitudes are essential factors in the adoption of IoT healthcare products, and there is a correlation between perceived ease of use and perceived usefulness (Karahoca et al., 2018). Furthermore, Blut et al. (2021) used DOI to obtain a distinguished picture of technology adoption throughout the following adoption stages: early adopters, early majority, and late majority.

The DOI theory can be used to understand the different stages of IoT security strategies adoption. This information can be useful for IT leaders to develop strategies for promoting IoT technology and for individuals to make informed decisions about adopting IoT security strategies. Overall, the DOI theory provides a useful framework of

understanding the process of IoT adoption and identifying the factors that influence it, making it an appropriate theoretical framework for this study.

Transition and Summary

The literal review section provided insight into the current IoT security issues and their effect on the adoption in the manufacturing sector. Also, it highlighted some of the security solutions that IT leaders can use. Diffusion plays a vital role as it has a social and economic impact. The literature review focused on using the DOI theory and its five characteristics to extract the advancement of IoT adoption. DOI explains how an innovation gains momentum and diffuses through society over time. The characteristics of the DOI theory played critical roles in this study as I used them to explore the security strategies to protect IoT devices from information security threats in the manufacturing sector.

Relative advantage is the first characteristic of DOI and is the strongest predictor of an innovation's adoption rate. It is the amount by which the innovation improves upon previous conditions, and is measured in terms of economics, satisfaction, convenience, and social prestige. The second characteristic is compatibility, which entails that innovation must be consistent with existing norms. The third characteristic is complexity which refers to the degree to which an innovation is easy or hard to use. The fourth characteristic is trialability; it helps the users to gain more exposure to the solution before making a decision. The fifth and last characteristic is observability; it provides the potential adaptors an insight into the innovation's benefits. The following section thoroughly explains the purpose statement, research method, and design. It describes the

role of the researcher and the instrumentation and technique used to collect and analyze data. Also, it addresses the population from which the sample is drawn. Finally, it discusses the reliability and validity of the study.

Section 2: The Project

In this section, I explain in-depth the purpose statement, research method, and design. I define the role of the researcher, participant sampling, and ethical research. Additionally, I describe the instrumentation, tools, and technique that I used to collect, analyze, and organize the data. Lastly, the section covers the reliability and validity of the research study.

Purpose Statement

The purpose of this qualitative multiple-case study was to determine strategies that IT leaders use to implement security for IoT devices in the manufacturing sector. I also sought to highlight some of the security issues, threats, and attacks that IoT devices are currently facing and provide countermeasures technologies and solutions that could help protect against these attacks. The most significant trend affecting the manufacturing industry is the adoption of smart factories, which has exponentially increased the risk of cyberattacks. The target population includes IT leaders of aerospace and defense manufacturing facilities in Southeast Los Angeles who have implemented and tested strategies to secure IoT devices from cyberattacks.

This study may have a positive social impact on employees' safety in the manufacturing sector. It might also have a good impact on the quality of the goods produced by the factories and delivered to the consumers. IoT devices can track working conditions, such as detecting hazardous material leakage, which can prevent potential work injuries. Furthermore, IoT sensors can determine if the manufactured products have been exposed to pressures, temperatures, and other conditions that may render the

product unsafe for use or consumption. Ensuring the confidentiality, integrity, and availability of the IoT devices will increase the ability of the manufacturer to detect problems during all stages, starting from receiving the raw material to the end stage, where the products and goods are ready for delivery.

Role of the Researcher

My role as a researcher in this qualitative research was mainly to access the thoughts of study participants. Qualitative researchers discover individual experiences using inquiries that cannot always be analyzed using statistical techniques. I was the primary instrument in the interview and data collection process. I developed the interview questions to be open-ended and avoided wording that might influence answers. Furthermore, I analyzed and presented the findings of this study while attempting to minimize personal bias.

I have more than 15 years of IT and cybersecurity experience in multiple sectors, including manufacturing. During my career, I have implemented many cybersecurity strategies to protect organization assets from cyberattacks. Organizations tend to secure their systems and neglect securing their IoT devices, although they share the same internal network. The lack of security strategies to prevent cyberattacks that result from the implementation of IoT devices in the manufacturing sector is the main reason for this research study. My current background helped provide a foundation for this research.

Given my experience in implementing security strategies in the manufacturing sector, my main responsibility in this study is to ensure unbiased results. Publication bias misleads researchers and diminishes public trust in the content of the paper (Dowdy et al.,

2022). Ellsworth (2021) suggested techniques to counteract bias in research. The distorted results that are generated from being biased will result in a wrong conclusion. There are three types of bias: information bias, selection bias, and confounding bias. Selection bias occurs when authors select results that they wish to report or publish (Moosa, 2019). Bias is a key concern that must be addressed when conducting studies (Belviso et al., 2022)

Reducing my disposition to interpret too quickly was critical to my role. I conducted the interviews properly by following the university requirements. First, I completed the appropriate training for protecting human research participants and received a certification of completion from the National Institutes of Health. Then, I selected participants that I had never worked with in my current or previous jobs and got approval from the Institutional Review Board (IRB) under approval number 12-06-23-1009294. Prior to conducting any interviews, I informed the participants about the interview process and protocol (see Appendix), and I got their consent to collect data. I used the same interview questions to ensure consistency, which reduced the potential for bias in the data collection process. I ceased interrupting the participants while speaking to avoid steering to the conversation that might lead to biased information and results. Furthermore, I abstained from providing my opinion on the topic to avoid influencing the interview.

Participants

Participant selection is an important phase in the research process. However, it is never a straightforward process. The mapping exercise starts by creating a list of

organizations that might have leaders and professional people with expertise that is potentially useful to the research (Hopkins & Schwanen, 2022). One of the most critical tasks relating to the qualitative research study lies in getting access to the participants that will serve as informants. Once access is granted, the researcher should find strategies to gain cooperation from the selected participants. Furthermore, prior to any interview, the researcher needs to take adequate measures to ensure the ethical protection of the participant.

The selection of participants for this study included IT and cybersecurity leaders from the manufacturing sector in the Southeast region of Los Angeles, United States. The criteria for selection were based on their experience as leaders in implementing security strategies for IoT devices. Although I used the purposive method for selecting participants, I ensured the selection was unbiased. I selected the participants based on their experience, avoiding any individuals I personally know. Purposive sampling is the process of selecting participants who might provide the researcher with the most valuable information. I used purposive selection instead of random selection because the quality of engagements is far more important than the number of engagements.

For this study, I used search engines to find manufacturing organizations and social media and email to reach out to participants. Finding participants with specific skill sets and experience in IoT security proved to be time-consuming. Some researchers use gatekeepers as a mediator to help them find participants. Naserrudin et al. (2022) explored the importance of gatekeepers in conducting research. The gatekeeper’s role may change during research, and within different organizational contexts, its main role is

to facilitate the research process and represent access for the researchers to reach their target participants. However, some gatekeepers may obstruct the research process (Naserrudin et al., 2022). They tend to be more influential in an emerging field (Alles, 2020).

Prior to conducting the interviews, I got approval from the organization's head of IT. And to adhere to the IRB requirements, I ensured all participants signed the consent form and received the necessary document related to the research. Furthermore, I got IRB approval to commence the recruitment and data collection process. The IRB is responsible for ensuring that all research complies with the university's ethical standards and U.S. federal regulations. The role of an IRB is to protect the welfare of human research subjects rather than judge the quality of research (Huh-Yoo et al., 2021). IRB protocols require researchers to address the three principles from *The Belmont Report* on research ethics with humans to determine if participants are treated ethically (Richie, 2021). IRB also ensures that appropriate safeguards are in place to protect participants (Roberts et al., 2018).

I assured the participants of complete confidentiality, and I ensured that participants' rights were upheld to the highest standard. Confidentiality pertains to protecting the participants' personally identifiable information. Building rapport early with the participants helped me gain their trust. I explained the nonmaterial benefits to be gained by participating and provided the participants with a synopsis of the interview. Lastly, I addressed any concerns they had related to the interview and data collection process.

Research Method and Design

Method

Research methods are techniques and strategies used in the data collection and analysis processes to understand the research study better. There are three main types of research methods: Quantitative, qualitative, and mixed methods. It is crucial for researchers to understand the difference between the methods and their advantages and disadvantages in order to select the most beneficial method for the research. All methods of research are valid, but certain research topics are more suited to one method than the other.

Researchers using the quantitative method seek to understand the correlational relationship between variables that are expressed in graphs and numbers to test theories and assumptions. Some of the common quantitative methods include observation, experiments, and surveys with closed-ended questions. The quantitative method can be used to describe an extensive collection of things much faster with more accurate results; however, it requires statistical training to analyze the collected data properly.

On the other hand, researchers use the qualitative method to understand events, experiences, opinions, or concepts by collecting and analyzing non-numerical data, such as text, audio, and video. The function of qualitative research is to understand human behavior, whereas the function of quantitative research is to explain human behavior (House, 2018).

The five qualitative approaches are biography, ethnography, phenomenology, grounded theory, and case study. The qualitative method is more flexible, can encourage

discussion, and can be conducted with a much smaller sample. However, it is not generalizable to broader populations. Another disadvantage of the qualitative method is it has a higher risk of research bias.

Researchers collect and analyze qualitative and quantitative data in mixed-method research to explore diverse perspectives. The main types of mixed method designs are parallel and nested, also called embedded, explanatory, exploratory, and triangulation. Mixed methods have the advantages of both methods, which can enrich the evidence and strengthen the research results. This hybrid research method is designed to answer research questions that are hard to answer by quantitative or qualitative methods alone. Mixed methods can be more complex and require extra resources, such as time, personnel, and money. Combining quantitative and qualitative methods does not always add up to the advantages of both methods and, in many cases, might cause problems (Timans et al., 2019).

Researchers should start by identifying the study aims to select the proper research method. My research study focuses on the quality of strategies organizations, and IT leaders use to securely implement IoT, making the qualitative methodology the most suitable research method for this study. I did not choose the quantitative method because it is limited in its pursuit of statistical relationships, which can lead to overlooking broader relationships. The results of quantitative research are numerical, which give fewer insights into thoughts and motivations than qualitative research. The other method that I did not choose is the mixed method because it also uses statistical data, which is hard to gather form interviewing IT leaders. Furthermore, quantitative and

mixed-method research requires a large sampling pool to accurately generalize the results.

Research Design

Research designs are strategies used by researchers to answer their research questions using empirical data. Their main function is to ensure that the evidence gathered will address the research problem. Choosing the right research design will also help in using the right kind of analysis for the gathered data and setting up the study for success. The top five qualitative research designs are phenomenology, ethnography, grounded theory, case study, and biography. While there are some commonalities between these methods, each of them has a different approach to supporting complex analysis (Whiffin et al., 2022).

Qualitative designs are mostly about gaining a detailed understanding of a specific phenomenon. The case study design focuses on gaining a holistic understanding of the case. The phenomenology design is used to explore the views of those who experienced a phenomenon to better understand it. Ethnography design allows the researcher to draw conclusions based on collecting data through observation and interviews. Ethnography is dynamic and maintains a balance between theoretical frames and practice (Cubellis et al., 2021). In a grounded theory study, the researcher collects and analyzes real-world data to discover new theories. And finally, biography design is concerned with the reconstruction of life history by focusing on a single life. Biography is based on memory-work and sharing lived experiences (Sofie et al., 2022).

Case study was the most appropriate approach for the IT problem I addressed for my doctoral research. Case study research is one of the most common qualitative methods used in information systems. It enables the researcher to study information systems in their natural settings and generate theories from practice. The case study approach adds to the transparency of the study (Czosnek et al., 2022). A case study was the most suitable design because of the ability to perform an in-depth investigation and analysis of the problem. It allowed me to closely examine the IoT security issues and strategies that might be beneficial to IT leaders in the manufacturing sector.

Ethnography and grounded theory designs are used to study information systems; However, I did not consider any of these designs. Ethnographic research comes from the discipline of cultural anthropology, where the researcher is required to spend a substantial amount of time in the field (Kelly, 2022). Another challenge is the difficulty in establishing trust and rapport with the participants, which can impact the quality and depth of the data collected. It requires time to build trust with the participants in order to get an honest discourse. Furthermore, the ethnographic researcher may face ethical challenges, such as protecting participant confidentiality. Grounded theory is a research design in which the researcher seeks to develop a theory grounded in data systematically gathered and analyzed (Siegel et al., 2022). Grounded theory tends to produce large amounts of data, which could be challenging for researchers who are not well-versed in the methodology, as it requires a high level of expertise in data analysis and interpretation. Also, I can be time-consuming and resource-intensive, requiring extensive analysis efforts.

The least appropriate approaches for my research are phenomenology and biography. Biography focuses on exploring an individual's life, whereas phenomenology focuses on understanding the essence of the experience. Biographical research has several disadvantages that can affect the quality and validity of the research findings. One major disadvantage is the subjectivity of the research (Gallagher et al., 2019). In a biography study, the researcher might write with persuasion in mind rather than to inform. Additionally, biographical research can be limited by the availability and accuracy of information. Phenomenology has several disadvantages that can impact the reliability and validity of the research findings. The subjectivity of the research is one of the major disadvantages of the phenomenology approach. The interpretation of experiences highly depends on the researcher's biases, perspectives, and cultural background (Urcia, 2021). Additionally, phenomenology can be time-consuming and resource-intensive, as it requires extensive reflection and interpretation of the collected data.

Population and Sampling

The population for this multiple case study is IT leaders working in three aerospace and defense manufacturing facilities in Southeast Los Angeles and have strategies to secure these devices from cyberattacks. Researchers can use either a fixed size or saturation sampling concepts. A predetermined sample, such as a fixed size, is not ideal in qualitative designs because it is not flexible as the research progresses in the study. Time and funding are huge constraints for researchers, which makes selecting candidates from a larger population an ideal process. Adding criteria to the selection process will limit the number of candidates, which saves time. To select the most

appropriate sampling method, a researcher should also take into consideration the nature of the population (Sarfo et al., 2022).

Saturation sampling occurs when the data collection reaches a satisfactory point (Mthuli et al., 202). The concept of saturation was developed in 1967 as part of a grounded theory approach to qualitative research. Nowadays, the concept of saturation is used in many qualitative research designs, specifically in case study design (Hennink & Kaiser, 2022). Despite the data saturation fuzziness, it is still a standard research practice (Chtiac, 2022).

Selection bias is a distortion that may occur when the researchers fail to achieve proper randomization in the sampling process. In a non-random selection, such as sampling saturation, researchers must select the participants based on criteria to avoid any selection bias. I selected and interviewed every participant that matched the following characteristics to achieve sample saturation: (a) must have at least 5 years of experience in leading IoT implementation projects in a manufacturing environment, (b) must have at least 3 years of experience in cybersecurity, (c) were at least 18 years and older, and (d) willing to share experience and security strategies. In total, I interviewed four IT leaders working for manufacturing organizations who have recent experience implementing IoT security strategies.

On the other hand, data saturation can be achieved when no new information emerges with additional interviews (Fofana et al., 2020). I interviewed participants to the point where no new information was discovered. Furthermore, with the approval of the organizations, I collected data from documents relating to IoT and security

implementation projects to achieve data saturation. Finally, the collected data is organized and analyzed. Organizing data includes classification and labeling which helps the research with the analysis process by effectively determining the cause of the problems and possible solutions.

Ethical Research

The researcher's duties and responsibilities are adhering to ethical principles such as honesty, objectivity, integrity, confidentiality, and ethical treatment of research participants. Plagiarism and data falsification will result in a serious failure of the integrity of the study (Jutten, 2022). It is crucial that the researcher report results honestly without any manipulation, avoid bias, respect intellectual property standards, protect the privacy and safety of the participants, and, most important, treat research participants according to the standards and regulations. Researchers must ensure legal compliance and ethical responses toward participants to ensure their safety and confidentiality (Mathews, 2022).

Walden University IRB is responsible for ensuring compliance with the university's ethical standards and U.S. federal regulations. It is required for all Walden studies before participant recruitment and data collection. Once I obtained the IRB approval, I obtained each participant's consent by having them complete the consent form. All participants were informed about the interview process, purpose, risks, benefits, and nature of the study in a one-on-one video call. Participants were informed that their participation was voluntary, and no incentive was offered. All participants were informed

that they could withdraw from the study at any time without any reason. However, no participants chose to withdraw from the study.

All collected data, including but not limited to interview recordings and company documents, are treated as private and confidential information. Preserving research data enables researchers to verify the validity of previous findings, build on it, and generate new insights. Also, many research studies are subject to regulations that require the preservation of data for a certain period of time. Preserving the privacy and confidentiality of collected data is an important ethical requirement by Walden University IRB.

Researchers must ensure that the confidentiality adopted protects the privacy and effectively disseminates sensitive results (Turcotte-Tremblay & Sween-Cadieux, 2018). Respecting confidentiality agreements can create trust between the researchers and participants (Van De Heuvel et al., 2021). As such, to protect the privacy of participants, I removed any identifying information from the data and replaced it with codes. I stored the data in an encrypted device. After 5 years, I will shred the storage device and delete all emails related to the study.

Data Collection

Instruments

Data collection instruments are tools used to gather information for a research study. These instruments aim to obtain accurate data that will contribute to the validity and reliability of the study's results. The choice of data collection instrument will depend on the type of research and data being collected. For this study, I was the primary

instrument. I used over-the-phone semistructured interviews to collect qualitative data. Semistructured interviews provide a degree of freedom and adaptability in gathering information (Schnitzler et al., 2023). Interviews allowed me to ask follow-up questions and provided me an opportunity to gain more in-depth information from the participants. Also, semistructured interviews helped me establish a better rapport with the participant, which led to more honest responses and improved the reliability of the data collected. I followed the interview protocol (See Appendix A) to address the research question and better understand their experiences implementing IoT security strategies.

I captured the interview call using two audio recordings to reduce the risk of data lost due to any electronic or battery malfunction. The audio recording devices are tested prior to every interview. After recording the interviews, I used multiple software, such as Watson by IBM, to convert audio to text. Then I used NVivo software to find patterns and connections in documents and audio. NVivo allows the researcher to digitalize the data management analysis process, which gives more flexibility to organize data, reduce time and effort, and improve the quality of the results (Alam, 2021).

I enhanced the data collection by adding member checking, which has become widely recommended as a validity and trustworthiness check for rigorous qualitative research. Member checking involves revisiting the interview data with the participant to confirm they understand and make any necessary corrections (Motulsky, 2021). Also, I used public company documents to verify and validate my findings from the interviews.

Furthermore, I used methodological triangulation to collect data from multiple data sources. Methodological triangulation increases the validity and reliability of results

and provides a more comprehensive understanding of the issues. It helps the researcher to overcome the limitations associated with any single-method (Nwanna-Nzewunwa et al., 2019). By triangulating data from multiple sources, I was able to cross-check findings and ensure that the results were robust and provided additional evidence to support existing theories.

Data Collection Technique

Data collection techniques are the methods used to gather data for a research study. Some of the commonly used data collection techniques include surveys, interviews, observations, focus groups, and archival research. One of the main elements for selecting the proper data collection method is finding the method that agrees with the purpose of the research (Palacios Martinez, 2020). For this study, I used semistructured interviews and documentation collection. The interviews were conducted online via video call software, such as Microsoft Teams and Zoom. Video calls allow for face-to-face communication from a comfortable place, saving time and resources (Mandy et al., 2019). However, like any technology, video calls come with a set of disadvantages. The most common ones are poor video and audio quality, technical issues, lack of privacy, and distraction (Domingo et al., 2022). Video calls can be disrupted by a poor internet connection or outdated software, leading to difficulties in seeing and hearing the other participants, which can detract from the overall experience.

I anticipated a 30- to 45-minute call; however, I scheduled 60 minutes for each meeting to allow the participants to ask additional questions. It is hard to estimate how long the interview is going to take, primarily since I used open-ended questions during

my interviews. Open-ended questions have encouraged a more in-depth and thoughtful response. And it allowed the participants to provide more detailed and nuanced answers. And it uncovered hidden information that I would not have gathered by using closed-ended questions (Scholz et al., 2022). Additionally, it helped me build rapport with each of the participants, which led to increased participant engagement and better-quality data. When participants feel at ease, they are more likely to provide detailed and accurate information (Dando et al., 2023).

I started the interviews by reminding the participants about their right to stop the interview and share their concerns at any given time. Also, I reminded them about the recording and asked them if they had any objections. I followed the interview protocol (see Appendix) during the whole process. After finishing the interview questions, I explained the concept of member checking and its importance to the research.

Member checking typically involves the researcher going back to the participants and asking them to review and provide feedback on the research findings to help identify any misunderstandings or miscommunications and make necessary revisions to the research report. This helps increase the validity of the study by ensuring that the researcher has a good understanding of the research perspective (Motulsky, 2021). I scheduled separate interviews for member checking to revise and correct the collected data. During the member-checking interviews, I provided the participants with the report of the findings and asked them to provide me with their feedback. After that, I made the necessary changes to the finding reports.

Lastly, I gathered public company documents from an online search to supplement the data I collected from the interviews. Access to accurate and reliable company documents is a valuable source of information for researchers. The collected company document can be a time-saving process and a cost-effective method of research, as it eliminates the need for long and expensive field research. By collecting accurate and reliable documents, I was able to eliminate the potential for bias that may arise from just personal interactions with the participants.

Data Organization Techniques

Data organization techniques are methods used to organize and store data collected from a research study. It is essential to properly organize data to ensure ease of access and interpretation, which helps to draw meaningful conclusions from the study. Some of the most common data organization techniques are tabulation, databases, spreadsheets, and file management. Using the tabulation technique, researchers can organize the data into a table format to summarize and display large amounts of data in an easily readable form.

I utilize Microsoft OneNote and OneDrive to organize and securely store the data collected for this study. OneNote is a digital notetaking and organizing application allowing me to capture and store notes, ideas, and information digitally. I created multiple notebooks, sections, and pages to organize the data and easily search notes and tags. I chose OneNote due to its ability to integrate with other Microsoft Office applications, making it a useful tool for managing interview meetings and tasks. Additionally, OneNote offers a strong algorithm encryption feature using 128-bit AES

encryption to protect the data collected. OneDrive is a cloud-based storage that offers several layers of encryption to protect data at rest and in transit. It is more cost-effective today to use cloud-based services for storing data (Horsman, 2020). OneDrive uses BitLocker technology to encrypt data at rest and Secure Sockets Layer (SSL) encryption to encrypt data in transit over the internet. SSL is a transmission security protocol that ensures data confidentiality and integrity (Liu et al., 2021). Furthermore, OneDrive allowed me to set up two-factor authentication, which added an extra layer of security to prevent unauthorized access to the data collected. Li et al. (2022) discussed how having two factor-authentication will reduce the chance of being impersonated.

Organizing data anonymously is an important step in protecting the privacy of research participants. Achieving anonymity can be difficult sometimes. Whenever possible, I collected and organized data in a way that avoids personally identifying information. I achieved anonymity by conducting a single session per participant, and I used a unique identifier. Sandnes (2021) suggested using the "CANDIDATE" tool for generating anonymous participant IDs. However, due to the small sample size, I manually assigned tags to replace names, addresses, and other identifying information. For example, participant 1 was identified as "P1", participant 2 was identified as "P2", etc. I stored the participants' personal information with their associated tags in an encrypted USB thumb drive and securely stored it with the rest of the physical documents in a locked safe. After 5 years, all the documents will be destroyed, and the data will be permanently deleted.

Data Analysis Technique

Data analysis allows researchers to make sense of the information collected to draw meaningful conclusions from their findings. Data analysis is a long process that requires a rigorous review of the narrative and data (Ehrmin & Pierce, 2021). Analyzing data using a proper data analysis technique can help researchers to uncover patterns in the data that may not be immediately visible, test the hypotheses, make predictions about outcomes, and identify errors that maybe missed in the data collection process. There are multiple methods that can be used to examine and interpret the data collected from a research study.

For this study, data were analyzed using methodological triangulation to identify codes and themes. Methodological triangulation involves the use of multiple research methods and data sources to strengthen the validity and reliability of the findings (Craig et al., 2021). The methodological triangulation can reduce the bias and limitations that are associated with any single data analyzing method. By cross-checking the results from each method against one another, researchers can get a more accurate picture of the research problem. Coding is the process of categorizing data into themes, patterns, or other groups and assigning them numerical code (Beresford et al., 2022). ML techniques can be used to code textual data (Nelson et al., 2021).

After organizing the data in a format that can be easily analyzed, I cleaned the data by checking for missing data, outliers, and other anomalies that may affect the analysis. Then, I systematically analyzed and categorized recurring patterns and ideas that emerged from the data during the coding process into themes. Themes helped me to

develop a deeper understanding of the major concepts. Coding and themes are important in qualitative research because they provide a structured approach to analyzing and interpreting data (Linneberg & Korsgaard, 2019). Nargesian et al. (2023) proposed using a metadata enrichment technique whenever the data is sparse to help annotate attributes with tags.

I used the qualitative data analysis software NVivo for organizing, coding, and analyzing unstructured data from interview transcripts and other collected documents. NVivo is a powerful and flexible tool that serves as a robust digital research workflow (Paulus, 2023). It allowed me to import data from various sources, including Microsoft Suite, PDFs, and audio and video files. And then identify themes and categorize them into groups. Also, I used NVivo for searching and retrieving specific data, exploring data relationships, and creating summaries of the findings. The three major themes that emerged are (a) organizational security measurements and controls, (b) Internal resources, and (c) awareness and education.

Furthermore, I analyzed the emerging themes using DOI theory and its four key concepts: Innovation, adopters, diffusion, and innovation attributes. I used a coding system that identifies instances of these key concepts within the data. For example, the code “diffusion” identifies cases where participants discuss how innovation spreads through the manufacturing sector and the social system. I kept repeating the analysis process until no new themes or codes were identified, and saturation was achieved. This happens when all categories have been identified (Daher, 2023).

Reliability and Validity

Reliability ensures that the results of a study can be trusted and replicated by other researchers. In other words, if a research study was repeated multiple times, it should have similar results every time (Spiers et al., 2018). Ensuring that the results of a study are reliable will help to increase the credibility and trustworthiness of the research findings. On the other hand, validity refers to the accuracy and truthfulness of the research findings (FitzPatrick, 2019). Validity is essential in research because it ensures that the results of a study accurately reflect the underlying phenomena being studied (Hayashi et al., 2021). Several factors can affect the reliability and validity of research findings, such as incorrect data recording, sampling size, and human error and bias. The researcher's beliefs, opinions, and expectations can have a huge influence on the study's results. Also, the sampling size can affect the reliability and validity of the results.

To increase the reliability and validity of my research findings, I use several strategies, including standardized measurement tools, triangulation, and appropriate sampling techniques. Therefore, I used the NVivo tool, which has been validated and tested to ensure reliability (David et al., 2022). NVivo is a qualitative data analysis tool researchers in various disciplines widely use. Also, I used NVivo to maintain an audit trail to provide transparency and traceability to the research process, which can help improve the validity and reliability of the study. An audit trail can help to establish the credibility of the research by providing evidence of the data collection process and any decisions made during the study (Carcary, 2020). Also, ensure that the study can be

replicated by providing a clear and detailed description of the data collection and analysis process.

I used sampling saturation by selecting participants based on criteria to ensure that the sample used was representative of the population being studied. And I confirmed that the research findings accurately represented the experiences and perspectives of the participants by using techniques such as member checking. I allowed the participants to verify the accuracy of the findings. I followed the interview protocol (See Appendix A) to ensure consistency and repeatability across all interviews. Interview protocols ensure that all participants are asked the same questions in the same way, to eliminate bias and ensure that the results are reliable and valid. A reliable interview protocol is essential for gathering good information (Yeong et al., 2018). By following a standardized protocol, the interviewer can remain neutral and not influence the participants' responses.

Methodologic triangulation is another method I used to help me enhance reliability and validity. It encompasses credibility, dependability, confirmability, and transferability of research findings (Moon, 2019). Reviewing company documents helped me confirm the findings from interviews. When different data sources converge on the same findings, it provides strong evidence to support the conclusions drawn from the research (Coleman, 2021). Also, this suggests that the findings are robust and not simply the results of a single methodological approach or measurement error. Lastly, I ensured that my actions and decisions were consistent with the goals of the research and were perceived as honest and ethical by using techniques such as reflexivity, where I critically

examined my own bias and assumptions. Peddle (2022) highlighted the benefits of reflexivity and its importance to the trustworthiness of the study.

Transition and Summary

Section 2 of this study expands on the purpose statement and the research method and design. This section also highlights the role of the researcher and participants and discusses ethical research. My duties and responsibilities as a researcher are adhering to ethical principles and Walden university IRB requirements. It is important to report honest results while protecting the privacy and safety of the participants. Therefore, I gathered, organized, and analyzed data using valid and reliable instruments. Section 3 will present the findings of the data analysis. Also, discuss any social implications and provide recommendations for further study.

Section 3: Overview of Study

The purpose of this qualitative multiple-case study was to determine strategies that IT leaders use to implement security for IoT devices in the manufacturing sector. The target population consisted of IT leaders of aerospace and defense manufacturing facilities in Southeast Los Angeles who have strategies to secure IoT devices from cyberattacks. The process included the use of semistructured interviews with an IT leader from each of the three chosen organizations. Data triangulation was used to verify and validate the findings and address any contradictions. Three main themes emerged during the analysis process: (a) authentication and access control, (b) data privacy and confidentiality, (c) device and network security. The following section will present the findings of the data analysis.

Presentation of the Findings

The main research question that guided this study was: What strategies are used by IT leaders to implement security for IoT devices in the manufacturing sector? Three main themes emerged during the analysis process: (a) authentication and access control, (b) data privacy and confidentiality, (c) device and network security. Research themes provide a useful way to organize and structure research and contribute to a broader understanding of the issue. I followed five main steps during the data analysis phase:

1. I familiarized myself with the data by thoroughly reading through the gathered information to get sense of the concepts that emerge.
2. I coded the data by tagging text that relates to specific concepts.
3. I grouped related codes together into categories.

4. I reviewed and refined the categories to create a more focused theme.
5. I checked for consistency by reviewing the themes against the original data to ensure they accurately capture the meaning of the data.

Table 1 demonstrates the frequency of responses for each theme.

Table 1

Frequency of the Major Themes

Major theme	Frequency
1. Authentication and access control	41
2. Data privacy and confidentiality	33
3. Device and network security	56

Theme 1: Authentication and Access Control

The first theme that surfaced from the data gathered was authentication and access control. One of the main challenges in securing IoT devices is ensuring that only authorized users can access the devices. Authentication mechanisms can be used to verify the identity of users and devices, and access control mechanisms can be used to limit access to system functions and sensitive data. The attacks exploit IoT devices inadequate authentication methods to gain access (Hussain et al., 2020). All three participants indicated that implementing strong authentication is one of the first and most important strategies that need to be implemented to improve the security posture of the organization.

Password-based authentication can be vulnerable to password cracking or brute-force attacks if not implemented securely. A side-channel attack defeats traditional cryptography during application execution by revealing passwords from memory (Salehi

et al., 2022). The participants suggested enforcing strong password policies that contain password complexity requirements, password length and expiration, account lockout, and password rotation policy. Participants 1, 2, and 3 stated that they developed strong password policies that require users to create passwords with a combination of eight or more uppercase and lowercase letters, numbers, and special characters. Additionally, passwords are required to be changed periodically to prevent the prolonged use of compromised passwords. When it comes to password rotation for IoT devices, the options are more limited compared to traditional user accounts, because IoT devices often have limited capabilities to support direct password rotation. Participants 2 and 3 suggested using device management platforms, such as AWS IoT device management and Microsoft Azure IoT Hub, to provide capabilities to manage and update IoT device configurations remotely. While they may not offer built-in password rotation features, their capabilities can be leveraged to push firmware or configuration updates to IoT devices, including password updates.

All participants stressed the need for multi-factor authentication (MFA) to increase the security of the authentication process. Deploying identity and access manage (IAM) alongside encryption, and MFA solutions is essential for safeguarding the confidentiality of IoT systems and data (Wang & Mu, 2021). MFA adds an extra layer of protection against unauthorized access by combining multiple authentication factors, such as passwords, biometrics, or hardware tokens. This helps ensure that the user accessing the IoT device is indeed the legitimate user, as it is highly unlikely that an attacker would possess all the necessary factors to authenticate. Participants 1 and 2 indicated that

hardware authentication offers several advantages over traditional password-based authentication by reducing the risk of password theft and providing more resistance to various forms of attacks, such as phishing and keylogging. However, hardware-based authentication comes with additional cost and complexity. All participants noted that many industries and jurisdictions have implemented regulations and standards that require organizations to implement MFA.

Participant 3 revealed that digital certificates are another great method to verify identities and ensure that communication occurs only between trusted parties. Digital certificates enable strong authentication and help ensure that communication occurs only between trusted parties. It also ensures the integrity of data by using encryption and digital signatures. Participant 3 suggested using public-key infrastructure (PKI), which refers to tools used to create and manage public keys for encryption. On a generic level, PKI helps the IoT network to establish the legitimacy of a device in a network. PKI provides non-repudiation, which aims to prevent an entity from denying the authenticity of their actions. It also supports secure protocols like transport layer security to establish a secure connection between clients and servers and mitigate the risk of impersonation or MITM attacks.

All participants concurred that it is crucial for organizations to manage access by ascertaining the permissions granted to a user or device in an IoT network. Effective measures for controlling access confirm that only approved individuals or devices have the ability to engage with specific IoT devices or data. Access control diminishes the likelihood of potential threats breaching secure systems or gaining access to valuable

data. It improves auditing and accountability, as access control systems often include features for logging and auditing, enabling organizations to monitor access activities. This creates an audit trail for investigating security incidents and holding individuals accountable for their actions. Furthermore, access control helps with regulatory compliance, as many industry regulations and data protection laws require the implementation of access control measures to protect sensitive data. By adhering to these standards, organizations not only exhibit their commitment to data security, but also substantially mitigate the risk of potential legal and regulatory ramifications.

There are multiple access control components that organizations can implement, such as role-based access control (RBAC), Attribute-based access control (ABAC), and Access control lists (ACL). Ouaddah et al. (2017) highlighted the advantages and challenges of existing access control solutions and their usability in the IoT domain. Participant 1 asserted that device provisioning is essential for implementing access control. The process of secure devices provisioning encompasses the safe introduction and setup of IoT devices within a network. This guarantees solely devices that are verified and authenticated can connect and interact with the IoT framework.

Participant 2 recommended implementing the principle of lease privilege, which ensures that individuals receive the bare minimum level of access necessary to carry out their designated roles. Shah et al. (2021) presented a novel lightweight continuous authentication protocol for IoT based on zero trust architecture (ZTA) approach from NIST Special Publication 800-207. ZTA is a manifestation of the key access control principle of the least privileged, where zero trust is the norm. Participant 3 stressed the

need for segregation of duties, which allows for the division of responsibilities. Signifying that crucial actions or transactions necessitate participation from several users. This guarantees that no lone user possesses full access, thereby minimizing the possibility of fraudulent activities, mistakes, or deliberate abuse of permissions. These restrictions minimize the possible harm that could be induced by a malicious internal actor or staff member who inadvertently jeopardizes security.

Theme 2: Data Privacy and Confidentiality

IoT devices continuously collect, process, and transmit data, often of a highly private and confidential nature. The level of IoT devices security indicates that malicious acts by hackers are not successful and privacy is the key to increasing the adoption of an innovation (Padyab et al., 2019). This makes data privacy and confidentiality a crucial concern in the IoT landscape. IoT devices often share data with third parties, including advertisers. While this can provide valuable insights for businesses, it also introduces potential privacy risks. Furthermore, regulations like CCPA in California (United States) and GDPR in the European Union highlighted the need for strict control over personal data. Non-compliance can lead to significant penalties for organizations.

The main objective of IoT security is to protect the privacy of the customers and their data integrity, confidentiality, and availability (Litoussi et al., 2020). According to all participants, data encryption, both in transit and at rest, is the most effective security measure that IT leaders can implement to protect the privacy and confidentiality of the data. However, a lot of the IoT devices used in the manufacturing sector do not use strong encryption algorithms due to several constraints that can make the implementation of

strong encryption more challenging. Some of these constraints are resource limitations, cost considerations, lack of standards, and short development cycles. Many of the IoT devices have limited processing power, memory, and energy capacity. Strong encryption algorithms can be computationally intensive and require significant resources. Also, IoT devices often have quick turnaround times from conception to market, which leaves little time for implementing robust security measures like strong encryption.

Participant 3 indicated that data loss prevention (DLP) strategies can safeguard sensitive information against unauthorized access, transmission, or disclosure of critical data. DLP solutions can protect the confidentiality of the IoT systems and data (Wang & Mu, 2021). DLP strategies encompass a range of techniques, including encryption, access controls, and activity monitoring, which collectively serve to mitigate the risk of data breaches and compliance violations. As data continue to spread across diverse platforms and devices, having robust DLP strategies becomes crucial in preserving the confidentiality, integrity, and availability of sensitive information.

This brings us to the second security measure that can help reduce the loss of private and confidential data. Participants 2 and 3 revealed that data minimization is a great measurement IT leaders can implement when their IoT devices use weak encryptions. It is important to collect and store only the necessary data to fulfill the intended purpose. Any personally identifiable information or sensitive data that is not relevant to the user experience, should not be collected. By implementing data minimization, organizations reduce the risk of data leaks and limit their exposure to potential privacy violations. In the event of a data leak, the potential damage is

significantly lower when organizations practice data minimization. The less data stored, the less information is exposed in case of a leak. Also, many data protection regulations, such as the GDPR, require organizations to implement data minimization principles. Adhering to these regulations helps organizations avoid legal and financial penalties.

Some of the application layer challenges are privacy and security of user data, compliance with regulations, and data management (Iqbal et al., 2020). Participant 1 indicated that implementing data minimization and data lifecycle management (DLM) policies is a must, even if the IoT devices use strong encryptions. DLM policy highlights the steps that need to be taken to manage the flow of data throughout its lifecycle properly. Effective DLM can minimize risk by ensuring data are appropriately protected, stored, shared, archived, and deleted. When private data are no longer required to be retained, they must be permanently deleted using secure methods to ensure that data cannot be recovered to prevent unauthorized access or potential misuse.

All participants noted that it is crucial to have a well-defined incident response plan in place before a breach occurs. A data breach involving IoT devices in the manufacturing sector can be particularly challenging, given the potential for operational disruptions. While there have been many academic studies concerning IoT security, there is still a lack of consistent approaches to security risks inherent in deployment of IoT solutions (Boyes et al., 2018). Participant 1 stated that no matter what security measures are implemented, there is always a risk of a data breach. Organizations should take a proactive approach to potential security incidents, rather than reacting haphazardly when a breach occurs.

According to Participant 2, a rehearsed incident plan can help reduce the downtime associated with the breach, which can help minimize the financial and reputational damage. Participant 3 revealed that a good incident response plan includes a post-incident review process, enabling the organization to learn from each incident and improve its security posture. Also, the incident response plan outlines the roles and responsibilities of different team members, leading to enhanced incident coordination. I discovered that it is crucial for organizations to follow privacy frameworks as they often reflect legal requirements and help prevent data breaches and the potential financial and reputational harm they can cause.

Theme 3: Device and Network Security

Device and network security is the third theme that surfaces from the data gathered. This security domain involves implementing protective measures to safeguard both IoT devices as well as the broader networks they operate within. As threats continue to evolve, the importance of device and network security has become paramount for businesses, necessitating constant adaptation to new challenges. The implementation of security by design in IoT devices has become essential; however, it can be complex and challenging due to cost consideration, limited resources, and lack of regulations.

Lack of standardization and the limited control over the built-in security features of IoT devices can be problematic to IT leaders. Lack of standardization increases the operational costs because it requires the involvement of different experts and tools in order to manage, monitor, and secure heterogeneous devices (Roe et al., 2022). According to Participant 1, efforts to educate manufacturers and create clear regulatory

guidelines could help encourage more widespread adoption of security by design in the IoT industry.

Tampering attacks are continuously increasing against IoT devices. Attackers violate the integrity of IoT by tampering with its hardware features and gaining access to it (Mastorakis et a., 2021). Participants 1 and 2 stress the need for physical security measures to protect IoT devices from physical tampering or theft by securing IoT devices in locked cabinets or restricted areas, implementing surveillance systems, and applying tamper-evident seals to detect any unauthorized access. An insider attacker can clone or swap a legitimate device with modified devices with overwritten parameters or firmware that perform different attacks (Iqbal et al., 2020). Participants 1 and 2 also mentioned that network segmentation is the most effective security measure that can be used to minimize the potential impact of a compromised device. Network segmentation not only reduces network congestion and improves performance, but it also enhances security. Segregating IoT devices into separate network segments can minimize the potential impact of a compromised device. If an incident occurs, it will be isolated to a particular segment and won't impact the entire network. For manufacturers that deal with sensitive data, network segmentation can help comply with regulations, such as PCC-DSS, that require separation of certain types of data.

On top of network segmentation, Participant 3 recommended implementing an extra layer of security by deploying intrusion detection and prevention systems to monitor IoT networks for suspicious activities or anomalies. Intrusion detection and prevention systems provide proactive defense capabilities by stopping potential attacks

before they reach their target. By detecting and responding to threats quickly, IT leaders can minimize the impact of security incidents. Pu and Choo (2021) investigated Sybil attacks in IoT and proposed lightweight detection as a countermeasure.

All participants have implemented robust monitoring and logging mechanisms to capture and analyze device and network activities. They have implemented security information and event management (SIEM) solutions, such as Splunk, to aggregate and analyze logs from different IoT devices for early threat detection. Participant 1 indicated that modern SEIM solutions can be tailored to monitor specialized systems like Industrial Control System (ICS) and SCADA, which are common in manufacturing environments. Participant 2 noted that SEIMs can integrate with other security solutions like Intrusion Prevention Systems (IPS), and endpoint security solutions. This integration boosts the overall security posture by sharing threat intelligence and response mechanisms.

According to Participant 3, secure device lifecycle management is an essential practice throughout the lifecycle of IoT devices. This involves secure device onboarding, secure firmware updates, and proper disposal of devices to prevent unauthorized access or data leakage. Secure Device Onboarding (SDO) protocols can help streamline and secure the devices and prevent unauthorized devices from joining. Before disposal, all sensitive stored on the devices should be securely erased and network and cloud access need to be removed to prevent potential data leakage and network exploitation.

From the analysis of the transcripts and the follow-up conversations, I discovered that having regular vulnerability scanning, penetration testing, and firmware patching can help organizations identify, address, and mitigate potential security threats, ensuring the

integrity, availability, and confidentiality of their systems and data. IoT systems working across multiple layers makes them complex and harder to secure because vulnerability across these layers can lead to system breach or failure (Fang et al., 2021). Vulnerability scanning helps in detecting known vulnerabilities in IoT devices, whereas penetration testing can uncover unknown or zero-day vulnerabilities. Penetration testing can also validate the effectiveness of an organization's security controls, procedures, and processes. Regular firmware updates often contain patches for known vulnerabilities. By applying these patches, organizations can prevent malicious actors from exploiting these vulnerabilities. Furthermore, I discovered that minimizing the attack surface of your IoT devices isn't just a good security practice; it's essential for ensuring the privacy, safety, and trust of users, as well as the stability and reliability of the internet at large.

The participants' findings align with the results of my research, emphasizing the critical importance of implementing robust authentication measures, device security, and data protection strategies. Robust authentication methods strengthen defenses against unauthorized access attempts, while comprehensive device security measures, such as regular updates and endpoint security solutions, safeguard against malware and vulnerabilities. Prioritizing data security through encryption, access controls, and data loss prevention mechanisms ensures the integrity and confidentiality of sensitive information, enhancing compliance and trust. Combining these efforts, fortifies organizational defenses, mitigates cyber risks, and preserves the integrity of assets' evolving threats.

The DOI significantly supported my exploration of IoT security strategies by enabling a structure analysis of adoption patterns. This framework sheds light on the diverse attitudes and approaches toward IoT security across different organizations. Innovators and early adopters may be at the forefront of deploying data encryption protocols, secure access controls, and advanced intrusion detection systems to protect sensitive information transmitted and stored by IoT devices. Understanding the factors driving their adoption decisions can help promote widespread adoption of IoT security practices among other adopters, thereby enhancing the overall cybersecurity resilience within IoT ecosystems. Furthermore, the framework not only aided in identifying the factors influencing adoption but also highlighted the importance of tailored strategies to accommodate varying levels of readiness among adopters.

Applications to Professional Practice

This study aimed to explore security strategies used by IT leaders to secure IoT devices in the aerospace and defense manufacturing sector. Participants in this study provided a real-world interaction with IoT security, leading to more authentic and comprehensive security practices that could help organizations and IT leaders in securing their IoT devices. Having different expertise can lead to insights into how different leaders perceive and manage security. Also, the participants tested the effectiveness of the proposed security strategies, and provided feedback on what works and what doesn’t in real-world scenarios.

Findings from such studies can inform security policies and educational programs tailored to IT leaders, improving overall security awareness and practices related to IoT

devices. Effective cybersecurity measures help ensure business continuity and minimize disruption. Also, cybersecurity practices maintain customer trust by safeguarding their data. Customers expect their personal information to be secure at all times. Promoting security at work helps educate employees about potential risks, reducing the likelihood of human error in security breaches.

IT leaders engaged in this study shared insights into the significant challenges they faced when implementing security strategies. A primary obstacle often revolves around constraints in essential resources, encompassing budget limitations, manpower shortages, and time constraints. Allocation of adequate resources to comprehensive security measures becomes very difficult for IT leaders as they navigate competing organizational priorities. Furthermore, the diverse array of technologies introduces many compatibility challenges. The complex task of integrating various security solutions and ensuring their seamless collaboration poses a complex undertaking for IT leaders.

Most of the participants stated that they follow cybersecurity frameworks for safeguarding their organizations against the evolving landscape of cyber threats. The frameworks provide structured guidelines and best practices that help establish a robust defense mechanism, ensuring the confidentiality, integrity, and availability of their IoT devices. By adopting a cybersecurity framework, organizations can systematically identify and mitigate potential vulnerabilities, fortify network defenses, and implement incident response strategies.

Implications for Social Change

Implementing the strategies outlined in this study has the potential to bring positive social change by improving the organization's quality of goods, and employee safety. The integration of secure IoT devices allows for real-time monitoring of various machinery, enabling the maintenance of stringent quality control standards. Predictive maintenance ensures the optimal performance of machinery, minimizes downtime and prevents defects, which becomes instrumental in delivering high-quality products that meet customer expectations.

Enhanced IoT security measures in manufacturing prevent potential cyberattacks on machinery. These safeguards protect not only the machinery within manufacturing facilities but also the workforce that uses it. Ensuring the integrity of manufacturing processes contributes to overall safety and prevents incidents that could have far-reaching consequences. Also, secure IoT applications contribute to the early detection of anomalies and malfunctions, enabling swift responses to mitigate risks and maintain a secure working environment.

Recommendations for Action

This study's findings show the need for implementing multi-layer strategies in order to secure IoT devices in the manufacturing sector. This approach recognizes that no single security measure is foolproof, and by layering different defenses, organizations can increase their overall resilience. By employing multiple layers of defense, manufacturing organizations can mitigate the impact of a single security failure. Even if one layer is breached, other layers can still provide protection, reducing the overall risk of a

successful cyberattack. This approach requires a combination of technical controls, policies, procedures, and user awareness to create a comprehensive security framework. The technical controls include Identity and Access Management (IAM), network, application, data, and endpoint security.

Standardization of IT in manufacturing plays a crucial role in enhancing cybersecurity within the industry. By using consistent protocols for IoT devices and systems, IT leaders can ensure interoperability in security measures across their infrastructure. This standardized approach enables the implementation of strong security controls, including encryption, authentication, and access management, which are essential for safeguarding sensitive access and critical operations from cyber threats. Furthermore, standardized IoT frameworks facilitate improved visibility and management of connected devices, enabling IT leaders to detect and respond to security incidents promptly. Without visibility, it becomes challenging to monitor the IoT devices' activities and assess their security posture.

Recommendations for Further Study

The edge IoT trend refers to the growing adoption of edge computing technologies in IoT implementations. This approach entails the processing and analysis of data in proximity to its origin, typically at the edge of the network where IoT devices and sensors are situated. Edge IoT drives innovation and enables new use cases across industries, inducing manufacturing. Applications range from predictive maintenance and asset tracking to real-time monitoring, leveraging the capabilities of edge computing to deliver value and insights for time-sensitive applications. However, edge IoT now

introduces a new attack surface. Attackers may target vulnerable edge devices to gain unauthorized access to sensitive data, launch attacks against other devices or network infrastructure, or compromise the integrity of data streams.

The aim of this study was to investigate the security strategies employed to safeguard IoT devices within the manufacturing sector. As the landscape of IoT undergoes continuous evolution, emerging trends like edge IoT necessitate deeper examination due to their potential to introduce new attack surface and security challenges. Therefore, there is an urgent need to explore and understand the implications of these evolving cases to develop effective security measures and mitigate associated risks.

Reflections

The past 2 years have been marked by many challenges. Nevertheless, the benefits made it all worthwhile. The most challenging aspect of conducting research often lies in sourcing peer-reviewed articles. This process entails thorough selection from a vast array of scholarly publications to ensure the reliability and credibility of the information gathered. Despite these challenges, the pursuit of peer-reviewed articles is essential for maintaining the integrity and validity of research findings, ultimately contributing to the advancement of knowledge in the IoT security field.

The findings from this study were enlightening. Delving into the research opened up new perspectives and shed light on important security strategies. Through rigorous analysis and investigation, this study uncovered significant findings. Armed with these

insights, IT leaders can enhance their IoT security posture against threats and ensure the integrity and resilience of their IoT devices in the manufacturing sector.

Summary and Study Conclusions

The adoption of IoT in manufacturing offers numerous advantages that revolutionize traditional processes but introduces security risks. The purpose of this qualitative multiple-case study was to determine strategies that IT leaders use to implement security for IoT devices in the manufacturing sector. I employed the five characteristics of the DOI theory to emphasize to IT leaders the security concerns and the potential complexities and reliability issues that could hinder the implementation of the IoT security strategy.

This research can significantly contribute to positive social change by promoting the importance of securing IoT in the manufacturing sector. This study identifies three key themes: (a) authentication and access control, (b) data privacy and confidentiality, (c) device and network security. And advocates for multi-layer security strategies due to recognizing the limitations of individual measures.

References

Abidoye, A. P., & Obagbuwa, I. C. (2018). DDoS attacks in WSNs: Detection and countermeasures. *IET Wireless Sensor Systems (Wiley-Blackwell)*, *8*(2), 52–59. https://doi.org/10.1049/iet-wss.2017.0029

Agyemang, J. O., Kponyo, J. J., Klogo, G. S., & Boateng, J. O. (2020). Lightweight rogue access point detection algorithm for WiFi-enabled Internet of Things (IoT) devices. *Internet of Things*, *11*, Article 100200. https://doi.org/10.1016/j.iot.2020.100200

Akpakwu, G. A., Silva, B. J., Hancke, G. P., & Abu-Mahfouz, A. M. (2017). A survey on 5G networks for the Internet of Things: Communication technologies and challenges. *IEEE Access*, *6*, 3619–2647. https://doi.org/10.1109/ACCESS.2017.2779844

Al Reshan, M. S. (2021). IoT-based application of information security Triad. *International Journal of Interactive Mobile Technologies*, *15*(24), 61–76. https://doi.org/10.3991/ijim.v15i24.27333

Alam, M. K. (2021). A systematic qualitative case study: Questions, data collection, NVivo analysis and saturation. *Qualitative Research in Organizations and Management: An International Journal*, *16*(1), 1–31. https://doi.org/10.1108/QROM-09-2019-1825

Alazab, M., Gadekallu, T. R., & Su, C. (2022). Guest editorial: Security and privacy issues in industry 4.0 applications. *IEEE Transactions on Industrial Informatics*, *18*(9), 6326–6329. https://doi.org/10.1109/TII.2022.3164741

Al-Boghdady, A., Wassif, K., & El-Ramly, M. (2021). The presence, trends, and causes of security vulnerabilities in operating systems of IoT's low-end devices. *Sensors*, *21*(2329), 2329. https://doi.org/10.3390/s21072329

Al-Jabri, I. M., & Sohail, M. S. (2012). Mobile banking adoption: Application of diffusion of innovation theory. *Journal of Electronic Commerce Research, 13*(4), 379–391.

Alkhabbas, F., Spalazzese, R., & Davidsson, P. (2019). Characterizing Internet of Things systems through taxonomies: A systematic mapping study. *Internet of Things*, *7*, Article 100084. https://doi.org/10.1016/j.iot.2019.100084

Alles, M. (2020). Using the 2019 JBE conference and 2017 JIS themed issue as natural experiments to examine the role of editors as gatekeepers of the research literature in AIS and ethics. *International Journal of Accounting Information Systems*, *39*, Article 100489. https://doi.org/10.1016/j.accinf.2020.100489

Al-Rahmi, W. M., Yahaya, N., Alamri, M. M., Alyoussef, I. Y., Al-Rahmi, A. M., & Kamin, Y. B. (2021). Integrating innovation diffusion theory with technology acceptance model: supporting students' attitude towards using a massive open online courses (MOOCs) systems. *Interactive Learning Environments*, *29*(8), 1380–1392. https://doi.org/10.1080/10494820.2019.1629599

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*, 26797–26809.

https://doi.org/10.1109/ACCESS.2019.2899368

Alsheikh, M., Konieczny, L., Prater, M., Smith, G., & Uludag, S. (2022). The state of IoT security: Unequivocal appeal to cybercriminals, onerous to defenders. *IEEE Consumer Electronics Magazine, 11*(3), 59–68. https://doi.org/10.1109/MCE.2021.3079635

Aly, M., Khomh, F., & Yacout, S. (2021). What do practitioners discuss about IoT and industry 4.0 related technologies? Characterization and identification of IoT and industry 4.0 Categories in stack overflow discussions. *Internet of Things, 14*. Article 100364. https://doi.org/10.1016/j.iot.2021.100364

Anajemba, J. H., Iwendi, C., Razzak, I., Ansere, J. A., & Okpalaoguchi, I. M. (2022). A counter-eavesdropping technique for optimized privacy of wireless industrial IoT communications. *IEEE Transactions on Industrial Informatics, 18*(9), 6445–6454. https://doi.org/10.1109/TII.2021.3140109

Angela M. Lonzetta, Peter Cope, Joseph Campbell, Bassam J. Mohd, & Thaier Hayajneh. (2018). Security vulnerabilities in Bluetooth technology as used in IoT. *Journal of Sensor and Actuator Networks*, *7*(3), 28. https://doi.org/10.3390/jsan7030028

Archibald, M., Ambagtsheer, R., Casey, M., & Lawless, M. (2019). Using Zoom videoconferencing for qualitative data collection: Perceptions and experiences of researchers and participants. *International Journal of Qualitative Methods*, *18*. https://doi.org/10.1177/1609406919874596

Arshad, A., Hanapi, Z., Subramaniam, S., & Latip, R. (2021). A survey of Sybil attack countermeasures in IoT-based wireless sensor networks. *PeerJ Computer Science*,

7, Article e673. https://doi.org/10.7717/peerj-cs.673

Arvidsson, N. (2014). Consumer attitudes on mobile payment services – results from a proof of concept test. *International Journal of Bank Marketing*, *32*(2), 150–170. https://doi.org/10.1108/IJBM-05-2013-0048

Aslam, F., Aimin, W., Li, M., & Ur Rehman, K. (2020). Innovation in the era of IoT and industry 5.0: Absolute innovation management (AIM) framework. *Information (2078-2489)*, *11*(2), 124. https://doi.org/10.3390/info11020124

Attié, E., & Meyer-Waarden, L. (2022). The acceptance and usage of smart connected objects according to adoption stages: An enhanced technology acceptance model integrating the diffusion of innovation, uses and gratification and privacy calculus theories. *Technological Forecasting & Social Change*, *176*. Article 121485. https://doi.org/10.1016/j.techfore.2022.121485

Bala, K., & Kaur, P. D. (2022). Changing trends of blockchain in IoT: Benefits and challenges. *2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 324–329. https://doi.org/10.1109/Confluence52989.2022.9734206

Barbareschi, M., Casola, V., De Benedictis, A., Montagna, E. L., & Mazzocca, N. (2021). On the adoption of physically unclonable functions to secure IIoT devices. *IEEE Transactions on Industrial Informatics*, *17*(11), 7781–7790. https://doi.org/10.1109/TII.2021.3059656

Bartlett, T. (2020). Emerging challenges with Internet of Things. *Issues in Information Systems*, *21*(3), 142–152. https://doi.org/10.48009/3_iis_2020_142-152

Bataineh, M. R., Mardini, W., Khamayseh, Y. M., & Yassein, M. M. B. (2022). Novel and secure blockchain framework for health applications in IoT. *IEEE Access*, *10*, 14914–14926. https://doi.org/10.1109/ACCESS.2022.3147795

Bedeković, N., Havaš, L., Horvat, T., & Crčić, D. (2022). The Importance of developing preventive techniques for SQL injection attacks. *Technical Journal / Tehnicki Glasnik*, *16*(4), 523–529. https://doi.org/10.31803/tg-20211203090618

Belviso, N., Zhang, Y., Aronow, H. D., Wyss, R., Barbour, M., Kogut, S., Lawal, O. D., Zhan, S. Y., Don, P. K., & Wen, X. (2022). Addressing posttreatment selection bias in comparative effectiveness research, using real-world data and simulation. *American Journal of Epidemiology*, *191*(2), 331–340. https://doi.org/10.1093/aje/kwab242

Beresford, M., Wutich, A., Du Bray, M. V., Ruth, A., Stotts, R., SturtzSreetharan, C., & Brewis. A. (2022). Coding qualitative data at scale: Guidance for large coder teams based on 18 studies. *International Journal of Qualitative Methods*, *21*. https://doi.org/10.1177/16094069221075860

Bigini, G., Freschi, V., & Lattanzi, E. (2020). A review on blockchain for the Internet of Medical Things: Definitions, challenges, applications, and vision. *Future Internet*, *12*(12), Article 208. https://doi.org/10.3390/fi12120208

Blut, M., Yee Loong Chong, A., Tsigna, Z., & Venkatesh, V. (2022). Meta-analysis of the unified theory of acceptance and use of technology (UTAUT): Challenging its validity and charting a research agenda in the red ocean. *Journal of the Association for Information Systems*, *23*(1), 13–95.

https://doi.org/10.17705/1jais.00719

Bout, E., Loscri, V., & Gallais, A. (2022). Evolution of IoT Security: The era of smart attacks. *IEEE Internet of Things Magazine*, *5*(1), 108–113. https://doi.org/10.1109/IOTM.001.2100183

Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. *Computers in Industry*, *101*, 1–12. https://doi.org/10.1016/j.compind.2018.04.015

Candal-Ventureira, D., Gonzalez-Castano, F. J., Gil-Castineira, F., & Fondo-Ferreiro, P. (2021). Coordinated allocation of radio resources to Wi-Fi and cellular technologies in shared unlicensed frequencies. *IEEE Access*, *9*, 134435–134456. https://doi.org/10.1109/ACCESS.2021.3115695

Cangea, O. (2019). A comparative analysis of Internet of Things security strategies. *Petroleum - Gas University of Ploiesti Bulletin, Technical Series*, *71*(1), 1–10.

Carcary, M. (2020). The research audit trail: Methodological guidance for application in practice. *Electronic Journal of Business Research Methods*, *18*(2), 166–177. https://doi.org/10.34190/JBRM.18.2.008

Carpenter, D., Barrett, P., Young, D. K., & McLeod, A. J. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems*, *44*, 380–407. https://doi.org/10.17705/1CAIS.04422

Catalano, C., Chezzi, A., Angelelli, M., & Tommasi, F. (2022). Deceiving AI-based malware detection through polymorphic attacks. *Computers in Industry*, *143*. https://doi.org/10.1016/j.compind.2022.103751

Cavalieri, S., Cantali, G., & Susinna, A. (2022). Integration of IoT technologies into the smart grid. *Sensors (14248220)*, *22*(7), 2475. https://doi.org/10.3390/s22072475

Chen, D. Q., & Liang, H. (2019). Wishful thinking and IT threat avoidance: An extension to the technology threat avoidance theory. *IEEE Transactions on Engineering Management*, *66*(4), 552–567. https://doi.org/10.1109/TEM.2018.2835461

Chen, J., Touati, C., & Zhu, Q. (2020). Optimal secure two-layer IoT network design. *IEEE Transactions on Control of Network Systems*, *7*(1), 398–409. https://doi.org/10.1109/TCNS.2019.2906893

Cirne, A., Sousa, P. R., Resende, J. S., & Antunes, L. (2022). IoT security certifications: Challenges and potential approaches. *Computers & Security*, *116*. https://doi.org/10.1016/j.cose.2022.102669

Coleman, P. (2021). Validity and reliability within qualitative research in the caring sciences. *International Journal of Caring Sciences*, *14*(3), 2041–2045.

Compare, M., Baraldi, P., & Zio, E. (2020). Challenges to IoT-enabled predictive maintenance for industry 4.0. *IEEE Internet of Things Journal*, *7*(5), 4585–4597. https://doi.org/10.1109/JIOT.2019.2957029

Correia Simões, A., Lucas Soares, A., & Barros, A. C. (2020). Factors influencing the intention of managers to adopt collaborative robots (cobots) in manufacturing organizations. *Journal of Engineering and Technology Management*, *57*. https://doi.org/10.1016/j.jengtecman.2020.101574

Craig, S. L., McInroy, L. B., Goulden, A. & Eaton, A. D. (2021). Engaging the senses in qualitative research via multimodal coding: Triangulating transcript, audio, and

video data in a study with sexual and gender minority youth. *International Journal of Qualitative Methods*, *20*. https://doi.org/10.1177/16094069211013659

Cubellis, L., Schmid, C., & von Peter, S. (2021). Ethnography in health services research: Oscillation between theory and practice. *Qualitative Health Research*, *31*(11), 2029–2040. https://doi.org/10.1177/10497323211022312

Cui, Y., Liu, W., Rani, P., & Alrasheedi, M. (2021). Internet of Things (IoT) adoption barriers for the circular economy using Pythagorean fuzzy SWARA-CoCoSo decision-making approach in the manufacturing sector. *Technological Forecasting & Social Change*, *171*. https://doi.org/10.1016/j.techfore.2021.120951

Czosnek, L., Zopf, E., Cormie, P., Rosenbaum, S., Richards, J., & Rankin, N. (2022). Developing an implementation research logic model: Using a multiple case study design to establish a worked exemplar. *Implementation Science Communications*, *3*(1), 1–12. https://doi.org/10.1186/s43058-022-00337-8

Daher, W. (2023). Saturation in qualitative educational technology research. *Education Sciences*, *13*(98), 98. https://doi.org/10.3390/educsci13020098

Damanpour, F., Sanchez, H. F., & Chiu, H. H. (2018). Internal and external sources and the adoption of innovations in organizations. *British Journal of Management*, *29*(4), 712–730. https://doi.org/10.1111/1467-8551.12296

Dando, C., Taylor, D. A., Caso, A., Nahouli, Z., & Adam, C. (2023). Interviewing in virtual environments: Towards understanding the impact of rapport-building behaviours and retrieval context on eyewitness memory. *Memory & Cognition*,

51(2), 404–421. https://doi.org/10.3758/s13421-022-01362-7

Davahli, A., Shamsi, M., & Abaei, G. (2020). A Lightweight anomaly detection model using SVM for WSNs in IoT through a hybrid feature selection algorithm based on GA and GWO. *Journal of Computing & Security*, *7*(1), 63–79. https://doi.org/10.22108/jcs.2020.119468.1033

David B. Allsop, Joe M. Chelladurai, Elisabeth R. Kimball, Loren D. Marks, & Justin J. Hendricks. (2022). Qualitative methods with Nvivo software: A practical guide for analyzing qualitative data. *Psych*, *4*(13), 142–159. https://doi.org/10.3390/psych4020013

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* [Doctoral thesis, Massachusetts Institute of Technology]. DSpace@MIT. https://dspace.mit.edu/handle/1721.1/15192

Dearing, J. W., & Cox, J. G. (2018). Diffusion of innovations theory, principles, and practice. *Health Affairs*, *37*(2), 183-190. https://doi.org/10.1377/hlthaff.2017.1104

Dibaei, M., Zheng, X., Jiang, K., Abbas, R., Liu, S., Zhang, Y., Xiang, Y., & Yu, S. (2020). Attacks and defences on intelligent connected vehicles: a survey. *Digital Communications and Networks*, *6*(4), 399–421. https://doi.org/10.1016/j.dcan.2020.04.007

Domingo, A., Rdesinski, R. E., Stenson, A., Aylor, M., Sullenbarger, J., Hatfield, J., Walker, S., Hervey, S., Singer, J., Cois, A., & Cheng, A. (2022). Virtual residency interviews: Applicant perceptions regarding virtual interview effectiveness, advantages, and barriers. *Journal of Graduate Medical Education*, *14*(2), 224–

228. https://doi.org/10.4300/JGME-D-21-00675.1

Dowdy, A., Hantula, D. A., Travers, J. C., & Tincani, M. (2022). Meta-analytic methods to detect publication bias in behavior science research. *Perspectives on Behavior Science*, *45*(1), 37–52. https://doi.org/10.1007/s40614-021-00303-0

Drame-Maigne, S., Laurent, M., Castillo, L., & Ganem, H. (2021). Centralized, distributed, and everything in between: Reviewing access control solutions for the IoT. *ACM Computing Surveys*, *54*(7), 1–34. https://doi.org/10.1145/3465170

Ehrmin, J. T., & Pierce, L. L. (2021). Innovative qualitative research data collection and analysis activities that engage nursing students. *Journal of Professional Nursing*, *37*(1), 38–42. https://doi.org/10.1016/j.profnurs.2020.11.009

El Hadj Youssef, W., Abdelli, A., Dridi, F., Brahim, R., & Machhout, M. (2022). An efficient lightweight cryptographic instructions set extension for IoT device security. *Security & Communication Networks*, 1–17. https://doi.org/10.1155/2022/9709601

Ellsworth, P. C. (2021). Truth and advocacy: Reducing bias in policy-related research. *Perspectives on Psychological Science*, *16*(6), 1226–1241. https://doi.org/10.1177/1745691620959832

Esmalifalak, M., Liu, L., Nguyen, N., Zheng, R., & Han, Z. (2017). Detecting stealthy false data injection using machine learning in smart grid. *IEEE Systems Journal*, *11*(3), 1644–1652. https://doi.org/10.1109/JSYST.2014.2341597

Fahad Azam, Rashid Munir, Mehboob Ahmed, M. Ayub, Ahthasham Sajid, & Zaheer Abbasi. (2019). Internet of Things (IoT), security issues and its solutions. *Science*

Heritage Journal, *3*(2), 18–21. https://doi.org/10.26480/gws.02.2019.18.21

Fang, H., Qi, A., & Wang, X. (2020). Fast authentication and progressive authorization in large-scale IoT: How to leverage AI for security enhancement. *IEEE Network*, *34*(3), 24–29. https://doi.org/10.1109/MNET.011.1900276

Fang, Z., Fu, H., Gu, T., Qian, Z., Jaeger, T., Hu, P., & Mohapatra, P. (2021). A model checking-based security analysis framework for IoT systems. *High-Confidence Computing*, *1*(1). https://doi.org/10.1016/j.hcc.2021.100004

Filho, G. P. R., Villas, L. A., Freitas, H., Valejo, A., Guidoni, D. L., & Ueyama, J. (2018). ResiDI: Towards a smarter smart home system for decision-making using wireless sensors and actuators. *Computer Networks*, *135*, 54–69. https://doi.org/10.1016/j.comnet.2018.02.009

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in Pharmacy Teaching and Learning*, *11*(2), 211–217. https://doi.org/10.1016/j.cptl.2018.11.014

Fofana, F., Bazeley, P., & Regnault, A. (2020). Applying a mixed methods design to test saturation for qualitative data in health outcomes research. *PLoS ONE*, *15*(6), 1–12. https://doi.org/10.1371/journal.pone.0234898

Gallagher, R., Kennedy, H. W., & Atkinson, S. (2019). “ASMR” autobiographies and the (life-)writing of digital subjectivity. *Convergence: The Journal of Research into New Media Technologies*, *25*(2), 260–277. https://doi.org/10.1177/1354856518818072

George, G., & Thampi, S. M. (2022). Combinatorial analysis for securing IoT-assisted

industry 4.0 applications from vulnerability-based attacks. *IEEE Transactions on Industrial Informatics*, *18*(1), 3–15. https://doi.org/10.1109/TII.2020.3045393

Gnoni, M. G., Bragatto, P. A., Milazzo, M. F., & Setola, R. (2020). Integrating IoT technologies for an "intelligent" safety management in the process industry. *Procedia Manufacturing*, *42*, 511–515. https://doi.org/10.1016/j.promfg.2020.02.040

Halabi, T., & Bellaiche, M. (2018). A broker-based framework for standardization and management of Cloud Security-SLAs. *Computers & Security*, *75*, 59–71. https://doi.org/10.1016/j.cose.2018.01.019

Hamza, A., Ranathunga, D., Gharakheili, H. H., Benson, T. A., Roughan, M., & Sivaraman, V. (2022). Verifying and monitoring IoTs network behavior using MUD profiles. *IEEE Transactions on Dependable and Secure Computing*, *19*(1), 1–18. https://doi.org/10.1109/TDSC.2020.2997898

Hardgrave, B. C., Davis, F. D., & Riemenschneider, C. K. (2003). Investigating determinants of software developers' intentions to follow methodologies. *Journal of Management Information Systems*, *20*(1), 123–151. https://doi.org/10.1080/07421222.2003.11045751

Harvey, A. K. (2021). *Strategies for integrating the Internet of Things in educational institutions* [Doctoral study, Walden University]. Walden Dissertations and Doctoral Studies.

Hayashi, P., Abib, G., Hoppen, N., & Gonçalves Wolff, L. G. (2021). Processual validity in qualitative research in healthcare. *Inquiry: The Journal of Health Care*

Organization, Provision, and Financing, *58*. https://doi.org/10.1177/00469580211060750

Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine*, *292*. https://doi.org/10.1016/j.socscimed.2021.114523

Heritage, I. (2019). Protecting industry 4.0: Challenges and solutions as IT, OT and IP converge. *Network Security*, *2019*(10), 6–9. https://doi.org/10.1016/S1353-4858(19)30120-5

Ho, J. C. (2022). Disruptive innovation from the perspective of innovation diffusion theory. *Technology Analysis & Strategic Management*, *34*(4), 363–376. https://doi.org/10.1080/09537325.2021.1901873

Hogewoning, M. (2018). IoT and regulation – striking the right balance. *Network Security*, *2018*(10), 8–10. https://doi.org/10.1016/S1353-4858(18)30099-0

Hopkins, D., & Schwanen, T. (2022). Recruiting research participants for transport research: Reflections from studies on autonomous vehicles in the UK. *Journal of Transport Geography*, *102*. https://doi.org/10.1016/j.jtrangeo.2022.103377

Horsman, G. (2020). What's in the cloud? An examination of the impact of cloud storage usage on the browser cache. *Journal of Digital Forensics, Security & Law*, *15*(1), 1–16. https://doi.org/10.15394/jdfsl.2020.1592

House, J. (2018). Authentic vs elicited data and qualitative vs quantitative research methods in pragmatics: Overcoming two non-fruitful dichotomies. *System*, *75*, 4–12. https://doi.org/10.1016/j.system.2018.03.014

Hu, S., Hu, B., & Cao, Y. (2018). The wider, the better? The interaction between the IoT diffusion and online retailers' decisions. *Physica A: Statistical Mechanics and Its Applications*, *509*, 196–209. https://doi.org/10.1016/j.physa.2018.06.008

Huang, S., Guo, Y., Liu, D., Zha, S., & Fang, W. (2019). A two-stage transfer learning-based deep learning approach for production progress prediction in IoT-enabled manufacturing. *IEEE Internet of Things Journal*, *6*(6), 10627–10638. https://doi.org/10.1109/JIOT.2019.2940131

Huh-Yoo, J., Kadri, R., Buis, L. R., & Marcu, G. (2021). Pervasive healthcare IRBs and ethics reviews in research: Going beyond the paperwork. *IEEE Pervasive Computing*, *20*(1), 40–44. https://doi.org/10.1109/MPRV.2020.3044099

Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2020). Machine learning in IoT security: Current solutions and future challenges. *IEEE Communications Surveys & Tutorials*, *22*(3), 1686–1721. https://doi.org/10.1109/COMST.2020.2986444

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet of Things Journal*, *7*(10), 10250–10276. https://doi.org/10.1109/JIOT.2020.2997651

Iuliana M. CHITAC. (2022). The rationale for saturation in qualitative research: When practice informs theory. *Cross-Cultural Management Journal*, *XXIV*(1), 29–35.

Ivica Dodig, Davor Cafuta, Tin Kramberger, & Ivan Cesar. (2021). A novel software architecture solution with a focus on long-term IoT device security support. *Applied Sciences*, *11*(4955), 4955. https://doi.org/10.3390/app11114955

Jalali, M., Kaiser, J., Siegel, M., & Madnick, S. (2019). The Internet of Things promises new benefits and risks: A systematic analysis of adoption dynamics of IoT products. *IEEE Security & Privacy*, *17*(2), 39–48. https://doi.org/10.1109/MSEC.2018.2888780

Jin, P., Mangla, S. K., & Song, M. (2022). The power of innovation diffusion: How patent transfer affects urban innovation quality. *Journal of Business Research*, *145*, 414–425. https://doi.org/10.1016/j.jbusres.2022.03.025

Jing, Q., Vasilakos, A., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks (10220038)*, *20*(8), 2481–2501. https://doi.org/10.1007/s11276-014-0761-7

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. https://doi.org/10.1016/j.chb.2017.10.035

Jutten, C. (2022). Scientific integrity: A Duty for researchers [From the Editor]. *IEEE Signal Processing Magazine*, *39*(6), 3–84. https://doi.org/10.1109/MSP.2022.3198298

Kaedi, S., Doostari, M. A., & Ghaznavi-Ghoushchi, M. B. (2018). Low-complexity and differential power analysis (DPA)-resistant two-folded power-aware Rivest-Shamir-Adleman (RSA) security schema implementation for IoT-connected devices. *IET Computers and Digital Techniques*, *12*(6), 279–288. https://doi.org/10.1049/iet-cdt.2018.5098

Kaliyar, P., Jaballah, W. B., Conti, M., & Lal, C. (2020). LiDL: Localization with early detection of sybil and wormhole attacks in IoT Networks. *Computers & Security*, *94*. https://doi.org/10.1016/j.cose.2020.101849

Karahoca, A., Karahoca, D., & Aksoz, M. (2018). Examining intention to adopt to internet of things in healthcare technology products. *Kybernetes*, *47*(4), 742–770. https://doi.org/10.1108/K-02-2017-0045

Kasim, Ö. (2021). An ensemble classification-based approach to detect attack level of SQL injections. *Journal of Information Security and Applications*, *59*. https://doi.org/10.1016/j.jisa.2021.102852

Kelly, L. M. (2022). Focused Ethnography for Research on Community Development Non-Profit Organisations. *Forum: Qualitative Social Research*, *23*(2), 114–135. https://doi.org/10.17169/fqs-22.2.3811

Khan, F., Al-Atawi, A. A., Alomari, A., Alsirhani, A., Alshahrani, M. M., Khan, J., & Lee, Y. (2022). Development of a model for spoofing attacks in Internet of Things. *Mathematics (2227-7390)*, *10*(19), 3686. https://doi.org/10.3390/math10193686

Kim, J., Ko, M., & Chung, J. (2022). Physical identification based trust path routing against sybil attacks on RPL in IoT networks. *IEEE Wireless Communications Letters*, *11*(5), 1102–1106. https://doi.org/10.1109/LWC.2022.3157831

Kosmanos, D., Karagiannis, D., Argyriou, A., Lalis, S., & Maglaras, L. (2021). RF jamming classification using relative speed estimation in vehicular wireless networks. *Security and Communication Networks*, *2021*.

https://doi.org/10.1155/2021/9959310

Kumar, S., Eugster, P., & Santini, S. (2022). Software-based remote network attestation. *IEEE Transactions on Dependable and Secure Computing*, *19*(5), 2920–2933. https://doi.org/10.1109/TDSC.2021.3077993

Kumar, V., Jha, R. K., & Jain, S. (2020). NB-IoT security: A survey. *Wireless Personal Communications*, *113*(4), 2661–2708. https://doi.org/10.1007/s11277-020-07346-7

Latif, S. A., Wen, F. B. X., Iwendi, C., Wang, L. F., Mohsin, S. M., Han, Z., & Band, S. S. (2022). AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Computer Communications*, *181*, 274–283. https://doi.org/10.1016/j.comcom.2021.09.029

Lee, S., Choi, H., Kim, T., Park, H., & Choi, J. K. (2022). A novel energy-conscious access point (eAP) System with cross-layer design in Wi-Fi networks for reliable IoT services. *IEEE Access*, *10*, 61228–61248. https://doi.org/10.1109/ACCESS.2022.3181304

Lee, Y., Chae, H., & Lee, K. (2021). Countermeasures against large-scale reflection DDoS attacks using exploit IoT devices. *Automatika: Journal for Control, Measurement, Electronics, Computing & Communications*, *62*(1), 127–136. https://doi.org/10.1080/00051144.2021.1885587

Lee, Y.-H., Hsieh, Y.-C., & Hsu, C.-N. (2011). Adding innovation diffusion theory to the technology acceptance model: Supporting employees' intentions to use e-learning systems. *Journal of Educational Technology & Society*, *14*(4), 124–137.

Li, J., Zhang, D., Zhou, M., & Cao, Z. (2022). A motion blur QR code identification algorithm based on feature extracting and improved adaptive thresholding. *Neurocomputing*, *493*, 351–361.

Li, M., Yang, X., Khan, F., Jan, M. A., Chen, W., & Han, Z. (2022). Improving physical layer security in vehicles and pedestrians networks with ambient backscatter communication. *IEEE Transactions on Intelligent Transportation Systems*, *23*(7), 9380–9390. https://doi.org/10.1109/TITS.2021.3117887

Liang Zhang, Xuesheng Qian, Ping Lv, & Xue Zhou. (2019). A novel recommendation algorithm based on diffusion of innovation theory. *Journal of Engineering Science & Technology Review*, *12*(6), 87–95. https://doi.org/10.25103/jestr.126.11

Liang, H., & Xue, Y. (2009, March). Avoidance of Information technology threats: A theoretical perspective. *MIS Quarterly*, *33*(1), 71-90.

Lindstrom, J., Viklund, P., Tideman, F., Hällgren, B., & Elvelin, J. (2019). Oh, no – not another policy! Oh, yes - an OT-policy! *Procedia CIRP*, *81*, 582–587. https://doi.org/10.1016/j.procir.2019.03.159

Linneberg, M. S., & Korsgaard, S. (2019). Coding qualitative data: A synthesis guiding the novice. *Qualitative Research Journal*, *19*(3), 259–270. https://doi.org/10.1108/QRJ-12-2018-0012

Litoussi, M., Kannouf, N., El Makkaoui, K., Ezzati, A., & Fartitchou, M. (2020). IoT security: challenges and countermeasures. *Procedia Computer Science*, *177*, 503–508. https://doi.org/10.1016/j.procs.2020.10.069

Liu, A., Alqazzaz, A., Ming, H., & Dharmalingam, B. (2021). Iotverif: Automatic

verification of SSL/TLS certificate for IoT applications. *IEEE Access*, *9*, 27038–27050. https://doi.org/10.1109/ACCESS.2019.2961918

Liu, C., Zhu, H., Tang, D., Nie, Q., Zhou, T., Wang, L., & Song, Y. (2022a). Probing an intelligent predictive maintenance approach with deep learning and augmented reality for machine tools in IoT-enabled manufacturing. *Robotics and Computer-Integrated Manufacturing*, *77*. https://doi.org/10.1016/j.rcim.2022.102357

Liu, G., Han, J., Zhou, Y., Liu, T., & Chen, J. (2022b). QSLT: A quantum-based lightweight transmission mechanism against eavesdropping for IoT networks. *Wireless Communications & Mobile Computing*, 1–13. https://doi.org/10.1155/2022/4809210

Liu, Y., Yu, W., Dillon, T., Rahayu, W., & Li, M. (2022c). Empowering IoT predictive maintenance solutions with AI: A distributed system for manufacturing plant-wide monitoring. *IEEE Transactions on Industrial Informatics*, *18*(2), 1345–1354. https://doi.org/10.1109/TII.2021.3091774

Lopez-Pena, M. A., Diaz, J., Perez, J. E., & Humanes, H. (2020). DevOps for IoT systems: Fast and continuous monitoring feedback of system availability. *IEEE Internet of Things Journal*, *7*(10), 10695–10707. https://doi.org/10.1109/JIOT.2020.3012763

Lu, Y. (2021). Examining User Acceptance and Adoption of the Internet of Things. *International Journal of Business Science & Applied Management*, *16*(3), 1–17.

Lu, Y., Papagiannidis, S., & Alamanos, E. (2018). Internet of Things: A systematic review of the business literature from the user and organisational perspectives.

Technological Forecasting & Social Change, *136*, 285–297. https://doi.org/10.1016/j.techfore.2018.01.022

Mahjabin, T., Xiao, Y., Li, T., & Guizani, M. (2022). Hotlist and stale content update mitigation in local databases for DNS flooding attacks. *Telecommunication Systems*, *81*(3), 417–430. https://doi.org/10.1007/s11235-022-00950-x

Makarem, N., Bou Diab, W., Mougharbel, I., & Malouch, N. (2022). On the design of efficient congestion control for the Constrained Application Protocol in IoT. *Computer Networks*, *207*. https://doi.org/10.1016/j.comnet.2022.108824

Maniriho, P., Mahmood, A. N., & Chowdhury, M. J. M. (2022). A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends and challenges. *Future Generation Computer Systems*, *130*, 1–18. https://doi.org/10.1016/j.future.2021.11.030

Martins, R., Oliveira, T., & Thomas, M. A. (2016). An empirical analysis to assess the determinants of SaaS diffusion in firms. *Computers in Human Behavior*, *62*, 19–33. https://doi.org/10.1016/j.chb.2016.03.049

Masabo, E., Kaawaase, K., Sansa-Otim, J., Ngubiri, J., & Hanyurwimfura, D. (2018). A state-of-the-art survey on polymorphic malware analysis and detection techniques. *ICTACT Journal on Soft Computing*, *8*(4), 1762–1774.

Mastorakis, S., Zhong, X., Huang, P.-C., & Tourani, R. (2021). DLWIoT: Deep learning-based watermarking for authorized IoT onboarding. *IEEE Consumer Communications and Networking Conference, 2021*. https://doi.org/10.1109/ccnc49032.2021.9369515

Mathews, B. (2022). Legal duties of researchers to protect participants in child maltreatment surveys: Advancing legal epidemiology. *University of New South Wales Law Journal*, *45*(2), 722–763. https://doi.org/10.53637/oakc2052

Mazhar, N., Salleh, R., Zeeshan, M., & Hameed, M. M. (2021). Role of device identification and manufacturer usage description in IoT security: A survey. *IEEE Access*, *9*, 41757–41786. https://doi.org/10.1109/ACCESS.2021.3065123

Mazur, D. C., Entzminger, R. A., Kay, J. A., & Peterson, C. A. (2022). Analysis and overview of message queueing telemetry transport (MQTT) as applied to forest products applications. *IEEE Transactions on Industry Applications*, *PP*(99), 1–7. https://doi.org/10.1109/TIA.2022.3192424

Mehra, A., Paul, J., & Kaurav, R. P. S. (2021). Determinants of mobile apps adoption among young adults: theoretical extension and analysis. *Journal of Marketing Communications*, *27*(5), 481–509. https://doi.org/10.1080/13527266.2020.1725780

Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BaIoT— network-based detection of IoT botnet attacks using deep autoencoders. *IEEE Pervasive Computing*, *17*(3), 12–22. https://doi.org/10.1109/MPRV.2018.03367731

Menzli, L. J., Smirani, L. K., Boulahia, J. A., & Hadjouni, M. (2022). Investigation of open educational resources adoption in higher education using Rogers' diffusion of innovation theory. *Heliyon*, *8*(7). https://doi.org/10.1016/j.heliyon.2022.e09885

Mezhuyev, V., Al-Emran, M., Ismail, M. A., Benedicenti, L., & Chandran, D. A. P.

(2019). The acceptance of search-based software engineering techniques: An empirical evaluation using the technology acceptance model. *IEEE Access*, *7*, 101073–101085. https://doi.org/10.1109/ACCESS.2019.2917913

Min, S., So, K. K. F., & Jeong, M. (2019). Consumer adoption of the Uber mobile application: Insights from diffusion of innovation theory and technology acceptance model. *Journal of Travel & Tourism Marketing*, *36*(7), 770–783. https://doi.org/10.1080/10548408.2018.1507866

Mohamad Noor, M. binti, & Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks*, *148*, 283–294. https://doi.org/10.1016/j.comnzet.2018.11.025

Mokbal, F. M. M., Dan, W., Xiaoxi, W., Wenbin, Z., & Lihua, F. (2021). XGBXSS: An extreme gradient boosting detection framework for cross-site scripting attacks based on hybrid feature selection approach and parameters optimization. *Journal of Information Security and Applications*, *58*. https://doi.org/10.1016/j.jisa.2021.102813

Monica Peddle. (2022). Maintaining reflexivity in qualitative nursing research. *Nursing Open*, *9*(6), 2908–2914. https://doi.org/10.1002/nop2.999

Moon, M. D. (2019). Triangulation: A method to increase validity, reliability, and legitimation in clinical research. *Journal of Emergency Nursing*, *45*(1), 103-105. https://doi.org/10.1016/j.jen.2018.11.004

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information*

Systems Research, *2*(3), 192–222. https://doi.org/10.1287/isre.2.3.192

Moosa, I. A. (2019). The fragility of results and bias in empirical research: An exploratory exposition. *Journal of Economic Methodology*, *26*(4), 347–360. https://doi.org/10.1080/1350178X.2018.1556798

Motulsky, S. L. (2021). Is member checking the gold standard of quality in qualitative research? *Qualitative Psychology*, *8*(3), 389–406. https://doi.org/10.1037/qup0000215

Mrabet, H., Belguith, S., Alhomoud, A., & Jemai, A. (2020). A survey of IoT security based on a layered architecture of sensing and data analysis. *Sensors*, *20*(3625), 3625. https://doi.org/10.3390/s20133625

Mthuli, S. A., Ruffin, F., & Singh, N. (2022). 'Define, explain, justify, apply' (DEJA): An analytic tool for guiding qualitative research sample size. *International Journal of Social Research Methodology: Theory & Practice*, *25*(6), 809–821. https://doi.org/10.1080/13645579.2021.1941646

Murray, C. R. (2020). *A secure and strategic approach to keep IoT devices safe from malware attack* [Doctoral study, Walden University]. Walden Dissertations and Doctoral Studies.

Myers, M. (2004, February 24). Qualitative research in information systems. *MISQ*. Qualitative Research in Information Systems (misq.org)

Nargesian, F., Pu, K., Ghadiri-Bashardoost, B., Zhu, E., & Miller, R. J. (2023). Data lake organization. *IEEE Transactions on Knowledge and Data Engineering*, *35*(1), 237–250. https://doi.org/10.1109/TKDE.2021.3091101

Naserrudin, N. A., Culleton, R., Pau Lin, P. Y., Baumann, S. E., Hod, R., Jeffree, M. S., Ahmed, K., & Hassan, M. R. (2022). Generating trust in participatory research on plasmodium knowlesi Malaria: A study with rural community gatekeepers during the COVID-19 pandemic. *International Journal of Environmental Research and Public Health*, *19*(23). https://doi.org/10.3390/ijerph192315764

Nath N., R., & Nath, H. V. (2022). Critical analysis of the layered and systematic approaches for understanding IoT security threats and challenges. *Computers and Electrical Engineering*, *100*. https://doi.org/10.1016/j.compeleceng.2022.107997

Nelson, L. K., Burk, D., Knudsen, M., & McCall, L. (2021). The future of coding: A comparison of hand-coding and three types of computer-assisted text analysis methods. *Sociological Methods & Research*, *50*(1), 202–237. https://doi.org/10.1177/0049124118769114

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. https://doi.org/10.1109/COMST.2019.2910750

Nikou, S. (2019). Factors driving the adoption of smart home technology: An empirical assessment. *Telematics & Informatics*, *45*. https://doi.org/10.1016/j.tele.2019.101283

Ning, L., Ali, Y., Ke, H., Nazir, S., & Huanli, Z. (2020). A hybrid MCDM approach of selecting lightweight cryptographic cipher based on ISO and NIST lightweight

cryptography security requirements for Internet of Health Things. *IEEE Access*, *Access*, *8*, 220165–220187. https://doi.org/10.1109/ACCESS.2020.3041327

Noor, M., Abbas, H., & Shahid, W. B. (2018). Countering cyber threats for industrial applications: An automated approach for malware evasion detection and analysis. *Journal of Network and Computer Applications*, *103*, 249–261. https://doi.org/10.1016/j.jnca.2017.10.004

Nosouhi, M. R., Sood, K., Grobler, M., & Doss, R. (2022). Towards spoofing resistant next generation IoT networks. *IEEE Transactions on Information Forensics and Security*, *17*, 1669–1683. https://doi.org/10.1109/TIFS.2022.3170276

Nwanna-Nzewunwa, O. C., Ajiko, M. M., Motwani, G., Kabagenyi, F., Carvalho, M., Feldhaus, I., Kirya, F., Epodoi, J., Dicker, R., & Juillard, C. (2019). Identifying information gaps in a surgical capacity assessment tool for developing countries: A methodological triangulation approach. *World Journal of Surgery*, *43*(5), 1185–1192. https://doi.org/10.1007/s00268-019-04911-5

Oden, C. (n.d.). Tips on making assumptions in a research paper. *Project Topics*. Tips on Making Assumptions in a Research Paper - Project Topics

Okoli, T. T., & Tewari, D. D. (2021). Does the adoption process of financial technology in Africa follow an inverted U-shaped hypothesis? An evaluation of Rogers diffusion of innovation theory. *Asian Academy of Management Journal of Accounting & Finance*, *17*(1), 281–305. https://doi.org/10.21315/aamjaf2021.17.1.10

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., Alshoura,

W. H., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*. https://doi.org/10.1016/j.cose.2021.102494

Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ouahman, A. A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *COMPUTER NETWORKS*, *112*, 237–262. https://doi.org/10.1016/j.comnet.2016.11.007

Padyab, A., Habibipour, A., Rizk, A., & Ståhlbröst, A. (2019). Adoption barriers of IoT in large scale pilots. *Information*, *11*(1), 23. https://doi.org/10.3390/info11010023

Pajouh, H., Dehghantanha, A., Khayami, R., & Choo, K.-K. R. (2018). A deep recurrent neural network based approach for Internet of Things malware threat hunting. *Future Generation Computer Systems*, *85*, 88–96. https://doi.org/10.1016/j.future.2018.03.007

Pal, D., Zhang, X., & Siyal, S. (2021). Prohibitive factors to the acceptance of Internet of Things (IoT) technology in society: A smart-home context using a resistive modelling approach. *Technology in Society*, *66*. https://doi.org/10.1016/j.techsoc.2021.101683

Pal, S. K., Datta, B., & Karmakar, A. (2022). An artificial neural network technique of modern cryptography. *Journal of Scientific Research*, *14*(2), 471–481. https://doi.org/10.3329/jsr.v14i2.55669

Palacios Martínez, I. M. (2020). Methods of data collection in English empirical linguistics research: Results of a recent survey. *Language Sciences*, *78*.

https://doi.org/10.1016/j.langsci.2019.101263

Paulus, T. M. (2023). Using qualitative data analysis software to support digital research workflows. *Human Resource Development Review*, *22*(1), 139–148. https://doi.org/10.1177/15344843221138381

Peng, A., Tseng, Y., & Huang, S. (2021). An efficient leakage-resilient authenticated key exchange protocol suitable for IoT devices. *IEEE Systems Journal*, *15*(4), 5343–5354. https://doi.org/10.1109/JSYST.2020.3038216

Peranzo, P. (2020, Jun 13). Infographic: Benefits of IoT in manufacturing. *Imaginovation*. https://imaginovation.net/blog/iot-benefits-manufacturing/

Pu, C., & Choo, K.-K. R. (2022). Lightweight sybil attack detection in IoT based on bloom filter and physical unclonable function. *Computers & Security*, *113*. https://doi.org/10.1016/j.cose.2021.102541

Rana, M. M., & Dahotre, N. (2021). IoT-based cyber-physical additive manufacturing systems: A secure communication architecture, research challenges and directions. *2021 6th International Conference on Inventive Computation Technologies (ICICT)*, 216–219. https://doi.org/10.1109/ICICT50816.2021.9358643

Ritchie, K. (2021). Using IRB protocols to teach ethical principles for research and everyday life. *Journal of the Scholarship of Teaching and Learning*, *21*(1). https://doi.org/10.14434/josotl.v21i1.30554

Roberts, L. W., Dunn, L. B., Kim, J. P., & Rostami, M. (2018). Perspectives of psychiatric investigators and IRB chairs regarding benefits of psychiatric genetics

research. *Journal of Psychiatric Research*, *106*, 54–60. https://doi.org/10.1016/j.jpsychires.2018.08.027

Roe, M., Spanaki, K., Ioannou, A., Zamani, E. D., & Giannakis, M. (2022). Drivers and challenges of internet of things diffusion in smart stores: A field exploration. *Technological Forecasting & Social Change*, *178*. https://doi.org/10.1016/j.techfore.2022.121593

Rogers, E. (1962). *Diffusion of innovations.* (1st ed.). The Free Press.

Rogers, E. (1995). *Diffusion of innovations* (4th ed). The Free Press.

Rogers, E. (2003). *Diffusion of innovations.* (5th ed.). The Free Press.

Rondon, L. P., Babun, L., Aris, A., Akkaya, K., & Uluagac, A. S. (2022). Survey on Enterprise Internet-of-Things systems (E-IoT): A security perspective. *Ad Hoc Networks*, *125*. https://doi.org/10.1016/j.adhoc.2021.102728

Rungruengkultorn, P., & Boonsiri, S. (2022). Warehouse processes improvement using lean six sigma and RFID technology. *International Journal of Mathematics & Computer Science*, *17*(3), 1175–1186.

Saafi, S., Fodor, G., Hosek, J., & Andreev, S. (2021). Cellular connectivity and wearable technology enablers for industrial mid-end applications. *IEEE Communications Magazine*, *59*(7), 61–67. https://doi.org/10.1109/MCOM.001.2000988

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, *57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261

Said, O. (2022). LBSS: A Lightweight Blockchain-based security scheme for IoT-enabled healthcare environment. *Sensors (14248220), 22*(20). https://doi.org/10.3390/s22207948

Salehi, M., Borger, G. D., Hughes, D., & Crispo, B. (2022). NemesisGuard: Mitigating interrupt latency side channel attacks with static binary rewriting. *Computer Networks*, *205*. https://doi.org/10.1016/j.comnet.2021.108744

Samanta, A., & Nguyen, T. G. (2022). Quality-driven energy-efficient big data aggregation in WBANs. *IEEE Sensors Letters*, *6*(8), 1–4. https://doi.org/10.1109/LSENS.2022.3192620

Sandnes, F. E. (2021). CANDIDATE: A tool for generating anonymous participant-linking IDs in multi-session studies. *PLoS ONE*, *16*(12), 1–23. https://doi.org/10.1371/journal.pone.0260569

Šarac, M., Pavlović, N., Bacanin, N., Al-Turjman, F., & Adamović, S. (2021). Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture. *Energy Reports*, *7*, 8075–8082. https://doi.org/10.1016/j.egyr.2021.07.078

Sarfo, J. O., Debrah, T. P., Gbordzoe, N. I., & Obeng, P. (2022). Types of sampling methods in human research: Why, when and how? *European Researcher*, *13*(2), 55–63. https://doi.org/10.13187/er.2022.2.55

Savoury, R. D., & Burchell, J. M. (2021). Exploring the Influential Determinants of IoT Adoption in the U.S. Manufacturing Sector. *International Journal of Applied Management and Technology*.

Schnitzler, L., Paulus, A. T. G., Roberts, T. E., Evers, S. M. A. A., & Jackson, L. J. (2023). Exploring the wider societal impacts of sexual health issues and interventions to build a framework for research and policy: A qualitative study based on in-depth semi-structured interviews with experts in OECD member countries. *BMJ Open*, *13*(1), Article e066663. https://doi.org/10.1136/bmjopen-2022-066663

Scholz, E., Dorer, B., & Zuell, C. (2022). Coding issues of open-ended questions in a cross-cultural context. *International Journal of Sociology*, *52*(1), 78–96. https://doi.org/10.1080/00207659.2021.2015664

Shah, S. W., Syed, N. F., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2021). LCDA: Lightweight continuous device-to-device authentication for a zero trust architecture (ZTA). *Computers & Security*, *108*. https://doi.org/10.1016/j.cose.2021.102351

Shammar, E. A., Zahary, A. T., & Al-Shargabi, A. A. (2021). A survey of IoT and blockchain integration: Security perspective. *IEEE Access*, *9*, 156114–156150. https://doi.org/10.1109/ACCESS.2021.3129697

Shen, Y., Shen, S., Wu, Z., Zhou, H., & Yu, S. (2022). Signaling game-based availability assessment for edge computing-assisted IoT systems with malware dissemination. *Journal of Information Security and Applications*, *66*. https://doi.org/10.1016/j.jisa.2022.103140

Shin, D. (2019). A living lab as socio-technical ecosystem: Evaluating the Korean living lab of internet of things. *Government Information Quarterly*, *36*(2), 264–275.

https://doi.org/10.1016/j.giq.2018.08.001

Shin, J., Park, Y., & Lee, D. (2018). Who will be smart home users? An analysis of adoption and diffusion of smart homes. *Technological Forecasting & Social Change*, *134*, 246–253. https://doi.org/10.1016/j.techfore.2018.06.029

Shuqin Zhang, Guangyao Bai, Hong Li, Peipei Liu, Minzhi Zhang, & Shujun Li. (2021). Multi-source knowledge reasoning for data-driven IoT security. *Sensors*, *21*(7579), 7579. https://doi.org/10.3390/s21227579

Siegel, L. N., & Valtierra, K. M. (2022). Disrupting their frame of reference: teacher candidates in alternative education settings. *Teaching Education*, *33*(4), 387–403. https://doi.org/10.1080/10476210.2021.1948990

Sivathanu, B. (2019). Adoption of Industrial IoT (IIoT) in Auto-Component Manufacturing SMEs in India. *Information Resources Management Journal*, *32*(2), 52–75. https://doi.org/10.4018/IRMJ.2019040103

Soewito, B., & Marcellinus, Y. (2021). IoT security system with modified Zero Knowledge Proof algorithm for authentication. *Egyptian Informatics Journal*, *22*(3), 269–276. https://doi.org/10.1016/j.eij.2020.10.001

Sofie, S., Hanna, P., Henriëtte, S., Pseudonym, B., Patrick, S., & Elisabeth, D. S. (2022). A collective biography on working relationships in inclusive research teams. *Disability & Society*. https://doi.org/10.1080/09687599.2022.2071228

Song, F., Zhu, M., Zhou, Y., You, I., & Zhang, H. (2020). Smart collaborative tracking for ubiquitous power IoT in edge-cloud interplay domain. *IEEE Internet of Things Journal*, *7*(7), 6046–6055. https://doi.org/10.1109/JIOT.2019.2958097

Sorri, K., Mustafee, N., & Seppänen, M. (2022). Revisiting IoT definitions: A framework towards comprehensive use. *Technological Forecasting & Social Change*, *179*. https://doi.org/10.1016/j.techfore.2022.121623

Souri, A., & Hosseini, R. (2018). A state-of-the-art survey of malware detection approaches using data mining techniques. *Human-Centric Computing and Information Sciences 8*, 3. https://doi.org/10.1186/s13673-018-0125-x

Spiers, J., Morse, J. M., Olson, K., Mayan, M., & Barrett, M. (2018). Reflection/Commentary on a past article: "Verification strategies for establishing reliability and validity in qualitative research." *International Journal of Qualitative Methods*, *17*(1), 1–2. https://doi.org/10.1177/1609406918788237

Suman, S., Perumal, T., Mustapha, N., & Yaakob, R. (2019). Device verification and compatibility for heterogeneous semantic IoT Systems. *2019 4th International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE)*, 1–3. https://doi.org/10.1109/ICRAIE47735.2019.9037767

Sundstrom, B. (2016). Mothers "Google It Up:" Extending communication channel behavior in diffusion of innovations theory. *Health Communication*, *31*(1), 91–101. https://doi.org/10.1080/10410236.2014.936339

Tahsien, S. M., Karimipour, H., & Spachos, P. (2020). Machine learning based solutions for security of Internet of Things (IoT): A survey. *Journal of Network and Computer Applications*, *161*. https://doi.org/10.1016/j.jnca.2020.102630

Teixeira, F. A., Pereira, F. M. Q., Wong, H.-C., Nogueira, J. M. S., & Oliveira, L. B. (2019). SIoT: Securing Internet of Things through distributed systems analysis.

Future Generation Computer Systems, *92*, 1172–1186. https://doi.org/10.1016/j.future.2017.08.010

Tekinerdogan, B., Çelik, T., & Köksal, Ö. (2018). Generation of feasible deployment configuration alternatives for Data Distribution Service based systems. *Computer Standards & Interfaces*, *58*, 126–145. https://doi.org/10.1016/j.csi.2018.01.002

Theofanidis, D., & Fountouki, A. (2018). Limitations and delimitations in the research Process. *Perioperative Nursing*, *7*(3), 155–163. https://doi.org/10.5281/zenodo.2552022

Timans, R., Wouters, P., & Heilbron, J. (2019). Mixed methods research: What it is and what it could be. *Theory & Society*, *48*(2), 193–216. https://doi.org/10.1007/s11186-019-09345-5

Tortorella, G. L., Fogliatto, F. S., Cauchick-Miguel, P. A., Kurnia, S., & Jurburg, D. (2021). Integration of Industry 4.0 technologies into Total Productive Maintenance practices. *International Journal of Production Economics*, *240*. https://doi.org/10.1016/j.ijpe.2021.108224

Tournier, J., Lesueur, F., Mouël, F. L., Guyon, L., & Ben-Hassine, H. (2021). A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things*, *16*. https://doi.org/10.1016/j.iot.2020.100264

Trappey, A. J. C., Trappey, C. V., Govindarajan, U. H., & Sun, J. J. H. (2021). Patent value analysis using deep learning models—The case of IoT technology mining for the manufacturing industry. *IEEE Transactions on Engineering Management, Engineering Management*, *68*(5), 1334–1346.

https://doi.org/10.1109/TEM.2019.2957842

Trochim, W. (n.d.). *Qualitative approaches*. Conjointly. https://conjointly.com/kb/qualitative-approaches/

Tsai, Y.-T., & Tiwasing, P. (2021). Customers' intention to adopt smart lockers in last-mile delivery service: A multi-theory perspective. *Journal of Retailing and Consumer Services*, *61*. https://doi.org/10.1016/j.jretconser.2021.102514

Tu, Q. (2018). *Diffusion of Innovation Theory*. In *The SAGE Encyclopedia of Communication Research Methods* (pp. 433-434). SAGE Publications.

Turcotte-Tremblay, A. & Sween-Cadieux E. M. (2018). A reflection on the challenge of protecting confidentiality of participants while disseminating research results locally. *BMC Medical Ethics*, *19*(S1), 5–11. https://doi.org/10.1186/s12910-018-0279-0

University of Southern California. (n.d.). *Organizing your social sciences research paper*. https://libguides.usc.edu/writingguide/limitations

Urcia, I. A. (2021). Comparisons of Adaptations in Grounded Theory and Phenomenology: Selecting the Specific Qualitative Research Methodology. *International Journal of Qualitative Methods*, *20*. https://doi.org/10.1177/16094069211045474

Van De Heuvel, L. M., Maeckelberghe E., Ploem, M. C., & Christiaans, I. (2021). A genetic researcher's devil's dilemma: Warn relatives about their genetic risk or respect confidentiality agreements with research participants? *BMC Medical Ethics*, *22*(1), 1–7. https://doi.org/10.1186/s12910-021-00721-4

Velliangiri, S., Manoharn, R., Ramachandran, S., Venkatesan, K., Rajasekar, V., Karthikeyan, P., Kumar, P., Kumar, A., & Dhanabalan, S. S. (2022). An efficient lightweight privacy-preserving mechanism for industry 4.0 based on elliptic curve cryptography. *IEEE Transactions on Industrial Informatics*, *18*(9), 6494–6502. https://doi.org/10.1109/TII.2021.3139609

Vijayakumaran, C., Muthusenthil, B., & Manickavasagam, B. (2020). A reliable next generation cyber security architecture for industrial internet of things environment. *International Journal of Electrical & Computer Engineering (2088-8708)*, *10*(1), 387–395. https://doi.org/10.11591/ijece.v10i1.pp387-395

Walas Mateo, F., & Redchuk, A. (2021). IIoT/IoT and artificial intelligence/machine learning as a process optimization driver under industry 4.0 model. *Journal of Computer Science & Technology (JCS&T)*, *21*(2), 170–176. https://doi.org/10.24215/16666038.21.e15

Wamba, S. F., Anand, A., & Carter, L. (2013). RFID applications, issues, methods and theory: A review of the AIS basket of TOP journals. *Procedia Technology*, *9*, 421–430. https://doi.org/10.1016/j.protcy.2013.12.047

Wang, Q., & Mu, H. (2021). Privacy-preserving and lightweight selective aggregation with fault-tolerance for edge computing-enhanced IoT. *Sensors (Basel, Switzerland)*, *21*(16). https://doi.org/10.3390/s21165369

Wang, T., Li, C., & Zhang, P. (2021). A system dynamics model for the diffusion of cloud manufacturing mode with evolutionary game theory. *IEEE Access*, *9*, 1428–1438. https://doi.org/10.1109/ACCESS.2020.3043833

Wang, X., McGill, T. J., & Klobas, J. E. (2020). I want it anyway: Consumer perceptions of smart home devices. *Journal of Computer Information Systems*, *60*(5), 437–447.

Warner, L. A., Lamm, A. J., & Silvert, C. (2020). Diffusion of water-saving irrigation innovations in Florida's urban residential landscapes. *Urban Forestry & Urban Greening*, *47*. https://doi.org/10.1016/j.ufug.2019.126540

Washizaki, H., Ogata, S., Hazeyama, A., Okubo, T., Fernandez, E. B., & Yoshioka, N. (2020). Landscape of architecture and design patterns for IoT systems. *IEEE Internet of Things Journal*, *7*(10), 10091–10101. https://doi.org/10.1109/JIOT.2020.3003528

Whiffin, C. J., Smith, B. G., Selveindran, S. M., Bashford, T., Esene, I. N., Mee, H., Barki, M. T., Baticulon, R. E., Khu, K. J., Hutchinson, P. J., & Kolias, A. G. (2022). The value and potential of qualitative research methods in neurosurgery. *World Neurosurgery*, *161*, 441–449. https://doi.org/10.1016/j.wneu.2021.12.040

Woo, J., & Magee, C. L. (2022). Relationship between technological improvement and innovation diffusion: an empirical test. *Technology Analysis & Strategic Management*, *34*(4), 390–405. https://doi.org/10.1080/09537325.2021.1901875

Xu, B., Wang, W., Hao, Q., Zhang, Z., Du, P., Xia, T., Li, H., & Wang, X. (2018). A security design for the detecting of buffer overflow attacks in IoT device. *IEEE Access*, *6*, 72862–72869. https://doi.org/10.1109/ACCESS.2018.2881447

Yamao, E., & Lescano, N. L. (2020). Smart campus as a learning platform for Industry 4.0 and IoT ready students in higher education. 2*020 IEEE International*

Symposium on Accreditation of Engineering and Computing Education (ICACIT), 1–4. https://doi.org/10.1109/ICACIT50253.2020.9277679

Yan, Q., Huang, W., Luo, X., Gong, Q., & Yu, F. R. (2018). A multi-level DDoS mitigation framework for the industrial Internet of Things. *IEEE Communications Magazine*, *56*(2), 30–36. https://doi.org/10.1109/MCOM.2018.1700621

Yang Lu. (2021). Examining user acceptance and adoption of the Internet of Things. *International Journal of Business Science & Applied Management*, *16*(3), 1–17.

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*(11), 2700–2713. https://doi.org/10.46743/2160-3715/2018.3412

Yesmin, T., Carter, M. W., & Gladman, A. S. (2022). Internet of things in healthcare for patient safety: An empirical study. *BMC Health Services Research*, *22*(1), 1–14. https://doi.org/10.1186/s12913-022-07620-3

Yılmaz, N., & Olgan, R. (2020). Perceived attributes of instructional computer use in early childhood education: A scale adaptation and validation study. *Ilkogretim Online*, *19*(3), 1267–1283. https://doi.org/10.17051/ilkonline.2020.728040

Yin, C., Xi, J., Sun, R., & Wang, J. (2018a). Location privacy protection based on differential privacy strategy for big data in Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *14*(8), 3628–3636. https://doi.org/10.1109/TII.2017.2773646

Yin, D., Zhang, L., & Yang, K. (2018b). A DDoS attack detection and mitigation with

software-defined Internet of Things framework. *IEEE Access*, *6*, 24694–24705. https://doi.org/10.1109/ACCESS.2018.2831284

Yu, X., Qiu, J., Yang, X., Cong, Y., & Du, L. (2019). A graph-based adaptive method for fast detection of transformed data leakage in IOT Via WSN. *IEEE Access*, *7*, 137111–137121. https://doi.org/10.1109/ACCESS.2019.2942335

Yuen, K. F., Cai, L., Qi, G., & Wang, X. (2021). Factors influencing autonomous vehicle adoption: an application of the technology acceptance model and innovation diffusion theory. *Technology Analysis & Strategic Management*, *33*(5), 505–519. https://doi.org/10.1080/09537325.2020.1826423

Appendix: Interview Protocol

1. Introduce myself to the participants and thank them for participating in the study.
2. Go through their consent one more time before starting the audio recording.
3. Announce the date and time.
4. Reminding them of their right to withdraw from the interview at any time and for any reason.
5. Ask the following interview questions:
    a. How many years of experience do you have in implementing cybersecurity technical controls?
    b. What strategies have you used to secure IoT devices?
    c. What problems or road blocked did you encounter when implementing these strategies?
    d. Which of those strategies worked well, and why?
    e. How regulations affected your choice of strategies?
    f. What steps have you taken before implanting your controls?
    g. How do you measure IoT risks on the organization?
    h. How do you assess the effectiveness of the strategies used to secure IoT devices in your manufacturing environment?
    i. How do you ensure the continued security of IoT devices in your manufacturing environment?
    j. Do you have any other information you would like to share?
    k. Do you have any questions related to the study?
6. Thank the participants and turn off the audio recording.