2021

Military Breaking Boundaries Implementing Third-Party Cloud Computing Practices for Data Storage

Marc Anthony Rangel
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Marc Rangel

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. Bob Duhainy, Committee Chairperson, Information Technology Faculty
Dr. Jon McKeeby, Committee Member, Information Technology Faculty
Dr. Jodine Burchell, University Reviewer, Information Technology Faculty

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

Walden University
2021

Abstract

Military Breaking Boundaries Implementing Third-Party Cloud Computing Practices for Data Storage

by

Marc Anthony Rangel

MS, Walden University, 2015

MS, University of Phoenix, 2004

BS, Wayland Baptist University, 2001

AA, Community College of the Air Force, 2000

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

September 2021

Abstract

Senior Information Technology (IT) military leadership cannot currently implement, maintain, and administer cloud data storage without the direct support of third-party vendors. This study explicitly impacts cloud practitioners, engineers, and architects requiring a most sophisticated and streamlined ability to safehouse invaluable data using third-party data storage. Grounded in the theory of planned behavior, the purpose of this qualitative single case study was to investigate strategies military leadership uses to implement third-party cloud computing for data storage. The participants (n = 22) consisted of cloud administrators, engineers, and architects within a sizeable midwestern city with a minimum of 3 years of cloud computing knowledge and 5 years of total IT experience. Data collection included semistructured interviews using Skype, face-to-face, and telephone interviews, and internal and external organizational documents (n = 17). Four themes were identified through thematic analysis: work relationships amongst AWS vendors and military technicians, the strength of newly created security practices, all training/learning curves are considered, and continuous safety and improvement. It is recommended that both AWS and military technicians continue to work together, promoting safety and security. The implications for positive social change include the potential for job creation and enhancing the community economically.

Military Breaking Boundaries Implementing Third-Party Cloud Computing Practices for Data Storage

by

Marc Anthony Rangel

MS, Walden University, 2015

MS, University of Phoenix, 2004

BS, Wayland Baptist University, 2001

AA, Community College of the Air Force, 2000

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

September 2021

Dedication

I would like to dedicate the completion of this Doctorate to my family, friends, and fellow veterans I served with all over the world. Throughout the toughest of times, you were there to support me and drive me forward. During my two-year hiatus, you continued to remind me that I must return to complete this historic academic achievement. Thanks to my father Gaston Rangel who has been a leader, a role model, and my best friend all of my life. Your success in life with the District Attorney's office is impressive. Also, to my Mom, Eva, thank you for raising me while teaching determination, strength, and focus to identify goals and achieve them without hesitation.

I do not want to forget the elite soldiers that I admired and eventually wound up being part of. To all Air Force Special Tactics, Army Special Forces, and Navy DevGru (SEALs), which I have deployed with all over the world, it was a pleasure working with such silent professionals in Iraq, Afghanistan, Somalia, and so many other undisclosed locations around the globe. Thank you for your selfless love and attitude for this great country of ours. Lastly, for all the soldiers which have paid the ultimate sacrifice, you will never be forgotten. May your families continue to grow stronger with the blessing of our good Lord.

Acknowledgments

I would like to start by thanking my Chair, Dr. Bob Duhainy, for your fantastic guidance and leadership. Your candid and sometimes stern feedback helped motivate me to continue forward. I'd also like to recognize Dr. Jon McKeeby for being so patient and understanding through the trials and tribulations I experienced while enrolled at Walden. Last, I'd like to thank my university research reviewer (URR), Dr. Jodine Burchell, for your continued hard-nose reviews and transparent reviews. I now have a great understanding of what it is to be a scholar-practitioner.

I cannot complete this program without acknowledging Dr. Gail Miles for her introduction speech at my first residency which struck a chord for the positive. Dr. Miles made it clear as IT professionals we can gather as many certifications as necessary although they all have expiration dates. She followed up by saying, "no matter what you do, your Doctorate will never be taken away from you." Although minimal to some, this statement has been a motivation for the past five years and I sincerely thank you!

I started my program in November of 2014 and met a great friend, brother, fellow veteran, and mentor which I was unaware of at the time. Thank you for all of your help as a fellow student/cohort. Due to life experiences, I had to leave the program for two years while he completed his doctorate in 2018. Since then, Dr. Lamonte Bryant Tyler has been an exceptional help with any questions, concerns, and simple complaints I had when needing someone to lean on. God bless you and your patience while I concluded my final study. We made it!

Table of Contents

List of Tables

Section 1: Foundation of the Study

In its simplest form, cloud computing is considered a pool of available resources ready to meet and exceed each user's ever-changing demands, thereby revolutionizing IT. Since its inception, military branches have expressed interest in cloud computing, but cloud security and safety have been insufficient for military use. The Department of Defense (DoD) proposes a more secure private cloud-based infrastructure, estimated to save approximately 75% in existing maintenance and security (Deale, 2016). With the onslaught of GovCloud and other third-party cloud vendors, soldiers can now incorporate a popular point-and-click technology providing backup information, performance metrics, and log monitoring. Cloud computing varieties make cloud storage capacity a commodity and expand items like extensive data indexes and simple analytics even the military can employ and administer. Cloud storage provides the opportunity to conduct business, minimizing downtime and overall loss of productivity (Attaran & Woods, 2018). In this section, I describe the background of the problem, in addition to the purpose of the study.

Background of the Problem

Senior IT military leadership must acclimate to the use of third-party cloud computing technology because it is now mandated from the Pentagon downward. Military branches are excited within their collective joint-force capabilities, knowing that the cloud is assisting in the overall success using near-peer adversaries; these adversaries are capable of competing against the United States in every aspect of each domain, including air, land, sea, space, and now cyberspace (Brading, 2020). Third-party vendors

must now initiate their due diligence because each GovCloud customer and their systems operate various identity and access management infrastructure considering the difference in authentication, authorization, and access control (Koo et al., 2020). As the cloud matures, it will continue to develop documentation to assist with the administration of storage like the DoD Cloud Computing Security Requirements Guide (SRG). Documentation and support, like the SRG provide military guidance to DoD agencies.

Adopting the cloud resulted in Amazon creating a private capability, which maintains stringent Defense Information Security Agency (DISA) security levels supporting DoD guidelines. Senior IT military leadership understands, at a minimum, where datum are processed and the organizations and administrative control where authorities have access to specific data (Zaerens, 2011). Dulik & Dulik, (2015) found that leadership will boost operational IT efficiency, increase interoperability using mission partners, and posture its military to adopt innovative cloud technology quicker and at lower costs. Future cloud usage can provide strong DoD security guidelines, which can offer logical responses to secure data storage and encryption. Additionally, cloud engineers can work on a need-to-know basis for security purposes, thereby enforcing mitigation practices if required.

Problem Statement

Adopting cloud computing in the military is an instrumental and critical strategy necessary to support the military's technological advancements sustaining the nation's warfighters with secure solutions and a tactical advantage, whether on land, sea, or air (Roche, 2019). One branch showed initiative with a cloud computing investment budget

of 700 million dollars supporting data sensors, artificial intelligence, smart goggles, and precision guidance satellite navigation data (McLeary, 2019). The general (IT) problem is that military units have never outsourced their data, until recently, to third party vendors and are still extremely reluctant to change. The specific IT problem is that some senior IT military leadership lack strategies to implement third-party cloud computing for data storage.

Purpose Statement

The purpose of this qualitative single case study was to investigate strategies military leadership used to implement third-party cloud computing for data storage. This study's target population were subject matter experts (SME) such as cloud architects and virtualization engineers with prior DoD experience from a random selection of men and women within the IT industry. Implications for positive social change included increased cloud computing security practices for military units to improve their current knowledge base, trust, and data storage evolution with third-party vendors. These practices may improve military personnel's safety and security, their families, and preserve national security.

Nature of the Study

I applied in-depth qualitative methodology to this study. As Aspers and Corte (2019) discussed, qualitative research is an iterative process that improves understanding within the scientific community by making innovative and significant distinctions resulting from getting closer to the phenomenon studied. For instance, a researcher can employ iterative tactics using specific searches seeking thorough explanations of models

and data; thereby, the results are not always used to draw causal inferences but lead to invaluable information (Yom, 2014). This qualitative approach was appropriate because the iterative concepts found within the actual data lead to additional interviews seeking exact concepts or simple clarification from those concepts (Lasch et al., 2010). In quantitative methodology, the study measures many variables at a specific moment in time, thereby preventing the researcher from delving too deeply due to many variables presented (Rahman, 2016). A quantitative approach would not have been practical because I sought in-depth experiences instead of numerical data gathering and generalization across personnel groups. Similarly, mixed methods research can provide the researcher with a greater scope of range to investigate educational issues. Still, both words and numbers must be involved to benefit the study and society (Almalki, 2016). The mixed-methods review could have been an effective approach, but I did not introduce statistical measurements.

A single case study design was chosen for this qualitative study. According to Lazar et al. (2017), single case studies apply existing theories assessing their explanatory control or generating newer theoretical ideas from intriguing properties, specifically the case's dynamics. Meaning, single case studies can produce complicated theories than multiple cases because a researcher's theory can be an exact fit for specific cases. In contrast, multiple-case studies only retain relationships that replicate most of their cases (Mariotto et al., 2014). At its core, phenomenology bases its investigation of daily human experiences to acquire common sense understanding the meaning they experience and others' experience (Bliss, 2016). Phenomenology was considered, but would have been

difficult to obtain specific answers due to the sensitive nature of unclassified proprietary practices the military uses to administer their cloud computing events. Likewise, an ethnographer's practice is to understand individual settings and social worlds, which can cause cultural indifferences where views or actions undertaken to come to odds against the researchers (Coffey, 2018).

Research Question

What strategies are senior IT military leadership using to implement third-party cloud computing for data storage?

Conceptual Framework

Ajzen proposed the theory of planned behavior (TPB) in 1985, providing the conceptual framework used in this study. Kan and Fabrigar (2017) stated that TPB is used to understand behavioral intentions determined by a 3-factor combination: subjective norms, attitudes toward the behavior, and perceived behavioral control. Normative influence, which plays a paramount role in people's lives, seems to be identified by the subjective norms and behavioral intentions included in the TPB (Vesely& Klöckner, 2018).

TPB will contributed to this study with the support of its volunteers' attitudes and behavioral intentions. This means that many engineers and architects working within the cloud computing domain on a military installation have favorable outcomes of their attitudes by successfully installing and administering this technical project. Members did not have to be active duty or veterans, but any prior DoD experience meeting the requirements extended if a must. Additionally, due to the desire and positive intentions to

successfully implementing a first-time infrastructure, the stronger the intention and desire to thrive, the more likely the behavior is to follow (Ajzen, 2020). TPB's practice allows for reliability and greater accuracy in understanding one's attitude predicting their planned, deliberate, and actual resulting behavior. Thus, engineers' and architects' attitudes predicted by privacy and security perceptions can identify their behavioral intentions relative to the use of cloud computing (Arpaci et al., 2015).

Definition of Terms

Cloud security: In cloud security, consumers, brokers, carriers, and everyone else must take the utmost precautions against vulnerabilities to secure cloud-computing platforms or be exposed to potential and sometimes business-critical risks (Ramachandra et al., 2017).

Department of Defense (DoD): The enduring mission of the DoD provides elite combat-credible military forces necessary to deter war and protect the nation (DoD, 2019).

GovCloud: Amazon Web Service (AWS) GovCloud (US) delivers government customers and their partners opportunities through flexibility and secure architectural cloud solutions that comply with DoD Cloud Computing Security Requirements Guide (SRG) for unclassified and classified data (AWS, 2020).

Military branches: The military comprises 5 active branches whose culture and daily values are unique due to their loyal support and beliefs, traditions, and their own unifying communication enabling each branch to communicate (Sanghera, 2020).

Senior IT military leadership: Senior military leaders perceive what is described as crisis-disaster leadership, which differs from normal leadership in daily operations and seeks to identify their experiences, education, and training; this exemplary leadership explains their self-development activities and what is believed to assist them in their effective and critical judgment in complex scenarios making them such a diverse group of leaders (Denny, 2019).

Third-party vendors: Third-party vendors are the process where professional companies monitor and manage their interactions with all external parties they have relationships with (Houshian, 2017).

Assumptions, Limitations, and Delimitations

Events occur daily, that can influence research and its hypothesized outcomes or expectations. The ability to collect data providing an outcome contributes to the expectations of a researcher formed by integrity and discipline. Three scenarios in-particular which assist in research are assumptions, limitations, and delimitations. I explain all assumptions, limitations, and delimitations in this qualitative single case study will be explained within the study.

Assumptions

An assumption explains the motives to believe a particular interpretation is correct and how that interpretation is justified (Lee, 2017). I assumed that all voluntary participants chosen for this research would speak of their personal experiences within their military organization(s) covering cloud computing. I expected that each participant would be forward and honest about each question presented to them.

Limitations

As described, a research limitation is an imposed restriction or statistical model constraint, essentially outside of the researcher's control (Theofanidis & Fountouki, 2018). One potential limitation in senior military IT leadership is the hesitation to answer all questions unabashed. These responses may not align with other senior leadership's opinions resulting in a political debate or public disagreement due to military cloud computing. Another limitation was that each professional interviewed may have seen a friend or co-worker and may have asked their opinion of the GovCloud project, thereby jeopardizing their responses. Additionally, all interview questions were unclassified to those volunteers already completing the interview remained within the cloud computing storage realm preventing volunteers from straying outside the interview's bounds.

Delimitations

In essence, delimitations are identified by the definitions that researchers decide to set as specific boundaries or limits of their work, so the study's aim and its objectives do not become impossible to achieve (Theofanidis & Fountouki, 2018). One delimitation in this study was speaking with soldiers and asking their opinion, which could be a drastic outlook from their supervisor's approach. Another delimitation is that each volunteer chosen was asked to have 5 years of system administration experience and a minimum of 3 years cloud computing knowledge, which significantly reduced the number of personnel available. The last delimitation within this study was the addition of the purposive sampling method used to identify voluntary participants in the study.

Significance of the Study

An in-depth analysis and lack of extensive research on military cloud computing articles provided this research's motivation. This study offers value to IT practitioners as researchers observe the transition through hands-on military experience working with third-party cloud vendors. Consequently, this cloud computing study's overall findings add extensive additions of cloud computing approaches and data storage practices providing endless opportunities for future scholars to utilize in future research. With the knowledge and capacity to accept data from anywhere globally, the military is seeking potential improvements to the DoD and those men and women in need of data they are requesting. This contribution to effective IT practice can enable soldiers to receive storage data within seconds, dependent on their internet or satellite connection, thereby allowing them to complete the mission at hand. This specific study proves invaluable to the DoD and military branches across the globe seeking information their specific unit or squadron requires for peace or wartime contingencies.

Positive social change results in improved social and human conditions and society's betterment (Morris, 2017). Additional implications for positive social change include refurbished cloud computing practices that military personnel, government employees, and contractors alike implement for greater security improvements. Similarly, within the range of social change, newly substituted processes can lead to higher quality products. Humans form relationships, along with virtual communities requiring group interaction and online behaviors, which allows insight into creating usable community-

centric virtual environments capable of introducing the most positive social changes (Cline, 2017).

Review of the Professional and Academic Literature

In this literature review, I identify the background of third-party government cloud computing and its supporting elements like cloud security, avoiding data spillage, and circumventing cyber-attacks. The implementation of third-party GovCloud usage can impact multiple areas of cloud technology. With the introduction of third-party cloud computing, a small company or a large corporation has chosen an external entity outside of their organization to maintain its infrastructure and data. The advantages of third-party cloud computing are security benefits, cost advantages, guaranteed 24/7 maintenance and support, and SME managing their resources. Within this literature review, 10 main themes are identified, which include, (a) the history of cloud computing, (b) public cloud, (c) private cloud, (d) hybrid cloud, (e) cloud platforms, (f) cloud security, (g) security privacy and risk, (h) GovCloud history, (i) GovCloud customers and (j) conceptual framework. These specific topics were chosen to illuminate and identify the exact themes used to support and secure third-party cloud computing with AWS GovCloud.

Effective search practice involves keeping a specific document or diary containing all search activities so that the researcher can keep immediate track of their search terms so that no one else will use the exact steps and retrieve the same results (McNally, 2020). During the research, it is imperative to use very specific keywords and subject headings. The study focuses on phrases while using the correct and/or combinations within the university database. The keywords used for this literature review

included *public cloud, private cloud, hybrid cloud, government cloud, military cloud, GovCloud, cloud security, and cloud privacy risk*.

This literature review encompasses articles from ProQuest Central, Research Gate, SpringerLink, Google Scholar, ScienceDirect, ACM Digital Library, Education Resource Information Center (ERIC), and SAGE Knowledge. Reciteworks.com, APA7 citation generator, and MyBib.com were used to substantiate each reference included in this qualitative study and its peer-reviewed sources. Grammarly.com provided me the ability to review, correct, and articulate myself after finding critical issues identified by Grammarly's site. To date, 236 articles were used in this study**.** Of the 239, 208 (89.02%) of the articles were peer-reviewed, and 199 (94.9%) were within the 5 years the CAO approval board requires. In a review of the conceptual frameworks, TPB is introduced within the literature along with self-efficacy, change theory, and transactional/management theory, and their current roles within this single case study.

The History of Cloud Computing

The phrase *cloud computing* began in the 1960s by McCarthy introducing the true history of the cloud within a telecommunications world where the telecom companies started offering a virtual private network; these services, along with the comparable quality of service, were offered at a much lower cost (Bairagi & Bang, 2015). Many people believe the cloud is relatively new. However, its roots were conceived as an idea of an intergalactic computer network in which a machine could be accessed from any location in the world (Alzahrani, 2016). The official use of cloud computing started in the mid-1990s when Compaq used the concept in an internal document. Since 1996, the

cloud has evolved from a quick buzzword to an accepted ubiquitous concept with definitive computing power; in addition, computer databases, storage, and applications interfacing over the internet have become the de facto mode of computing today. As an idea in the 1960s, the cloud has transformed into a real-world technology used by many today.

In the past 20 years, the cloud has undergone incredible changes. With the invention of the cloud, data information has traveled rapidly in every direction across various computing systems with attributes like virtualization; it also scales up and down to manage larger workloads or automated security patching encompassing thousands of machines, making it more flexible (Hardy, 2018). The cloud has grown to the point that its adoption is reaching a virtual tipping point; it is expected that increased workloads will transfer from traditional local storage capabilities to the cloud from more than an average user to many external commercial entities (Ramachandra et al., 2017). Users are now acclimating to the idea of saving their invaluable data online instead of one large storage server or external backups. Similarly, cloud computing technologies have virtually evolved and have made it possible for end-users to employ servers, data centers, and additional facilities previously required to use on-site systems (Krogh, 2013).

Deploying a cloud computing concept varies monetarily depending on the platforms, services, etc., the customer identifies as the most appealing to their business. Simply put, pricing is not easy given different abstractions like resource types, various networks, and specific vendor costs associated with migrating large volumes of proprietary data (Varghese & Buyya, 2018). Considering the cloud's constant advantages

and domains, such as cost, confidentiality, and security, the cloud can be easily customizable to meet different cost needs and complete these transactions with minimal effort (Ahmadi & Aslani, 2018). The cloud boasts cost savings bringing substantial benefits, including flexible deployments; however, many questions regarding how customers can realize benefits and specific contextual factors that can impact the overall benefits remain unanswered (Chen et al., 2016). The cloud now offers capabilities that can improve small businesses and corporations alike. In all, the cloud provides flexibility to IT organizations.

Public Cloud

The public cloud is one of several options an organization can choose to complement its infrastructure. The public cloud provides computing services supplied by multiple third-party vendors atop the public internet delivering services available for users who want to use them and simply pay for the services they consume (Srivastava & Khan, 2018). Public clouds' services are for organizations and individuals seeking elasticity and accountability without fully absorbing total in-house infrastructures. Due to its initial popularity, the public cloud has played a critical role in the new hybrid architecture due to its efficiency, scalability, and accessibility to high-value services for even the most complex workloads (Schweitzer, 2019). From a user's perspective, the public cloud offers affordable services, but they also wrestle with the overall lack of security compared to other cloud models (Aryotejo et al., 2018).

Public cloud computing benefits can positively impact an organization's efforts within its (IT) infrastructure. Implementing public cloud technology generates numerous

advantages for customers like capital investment savings, scalability, simplified operations, and improved information visibility and viable sustainability (Attaran & Woods, 2018). Due to its stronghold, the cloud is considered disruptive because it enables innovative new services supporting business models that decrease time to market, create innovative operational efficiencies, and engage customers in many new ways (Müller et al., 2015). To date, corporations like AWS, Microsoft, and Google have their own cloud infrastructure and offer services at competitive prices.

Viewing the public cloud from the big picture of cloud technology provides public cloud opportunities for customers to apply cyber-physical systems and cloud technologies to play a vital role for key maintenance purposes (Jantunen et al., 2018). Public cloud computing is versatile enough to provide applications, sets of tools, and web services providing access to vast amounts of computing resources in easy, user-friendly, and user-centric ways (Kim et al., 2016). As an evolving service, the public cloud has matured and has morphed into a user-friendly and customer service-oriented technology for all to use. The cloud is used by large corporate suppliers and by universities. However, stable institutions and managing data in a central location are safe. Integrating into various infrastructural elements provides students a unified experience (Jones & Laat, 2016). The cloud offers several options to strengthen the data storage through secure means and multiple tools to complete the task at hand.

Private Cloud

Along with public cloud resources, private clouds are also growing in popularity due to their security practices and organizational contributions. A private cloud is often

used by government agencies, select financial institutions, and other mid to large-sized corporations requiring business-critical operations demanding total environment control (Microsoft, 2019). The flexibility of the private cloud is mostly necessitated by the desire to take full control of corporate data, system performance, and security guidelines; an organization can also fully deploy its own cloud capabilities through a third-party organization that can control the data for the customer (Senyo et al., 2018). In its multiuse, the private cloud has expanded into universities allowing faculty and students to create and engage in experimental cloud environments specifically for learning and design, configuration, and management (Hwang et al., 2016). The multiple uses of the private cloud offer potential for any organization.

A private cloud's benefits can assist in the security and hardening of an organization's infrastructure or data center. Due to its growth and efficient management, virtual resources are of great importance resulting in a direct impact on scalability and the cloud service's actual operational costs (Maenhaut et al., 2019). Similarly, some learning institutions are employing a private cloud because it will not involve much cost or more expense than owning an entire data center (Hakak et al., 2018). As Hemdan and Manjaiah (2018) pointed out, one of the significant deployment models is the private cloud used by large organizations for creating a corporate cloud internally, providing computing services at reduced cost and saving time. The private cloud has many prospective uses capable of delivering cloud storage to many.

Viewing the private cloud from the big picture of cloud technologies is a prime effort for large corporations and businesses to secure and solidify their cloud

infrastructures. Nissim et al. (2019) noted that the trend of private cloud adoption throughout organizations has significantly increased from 63% to 77% from 2017 to 2018; with this growth, virtual servers are now considered attractive targets for malicious cyber-attackers trying to inject their malware into this virtual environment. Regardless of its security practices, the cloud's success and extreme growth will likely continue to entice malicious users to embed their destructive code at any cost. Utilization of hashing is a privacy option for data as companies upload their proprietary information to the cloud with encryption practices; additionally, these entities want to compute the data to perform operations like pattern matching, private searches, and other computations where their private equality testing is vital and mandatory (Saha & Koshiba, 2018).

Hybrid Cloud

A hybrid cloud is a computing environment that uses a combination of on-premise, third-party, and private cloud services with controlled orchestration amongst each platform. The use of platforms interfacing with each other provides workloads for businesses' computing to allow greater flexibility and diverse data deployment choices. Perrons (2015) identified hybrid cloud usage as an emerging necessity for customers to administer and manage security-related vulnerabilities or risks while allowing the cloud experts to maintain the enhanced scalability that the public cloud delivers. Due to the sensitivity of the hybrid cloud managing both private and public sectors of the cloud, most solutions must be given the necessary privacy required, thus enforcing cryptographic and access control techniques directing fine-grained access control in each solution (Kanwal et al., 2019). A hybrid cloud option offers an enterprise the broader mix

of technical services like a business running a mission-critical tasking with the security of a private cloud but the database or the archival service of a public cloud.

A hybrid cloud's benefits, and the adoption of this resource can easily be calculated by simple comparison versus traditional IT investments, resulting in a cheaper overall cost (Koo & Kim, 2015). A hybrid cloud also incorporates environmental workload portability. Hybrid cloud options provide organizations access to desktop virtualization, a key advantage for any company with a distributed, ever-increasing global, and remote workforce. This model provides customers a more efficient means of retaining data and its applications through an elevated level of security of sensitive data and instances protecting companies particularly impacted by industries and their financial regulations (Srinivasan et al., 2015).

As the hybrid cloud is viewed from the big picture of cloud computing technology, it is apparent that the mixed computing capability offers invaluable storage capacity, data cost savings, and on-premises resource abilities for local users. Another facet of hybrid cloud computing is existing systems currently running on legacy architecture processing business-critical applications that can easily migrate to a more up-to-date virtual infrastructure with no downtown, which is a seamless transition for the end-users. Due to the growth of hybrid cloud usage, administrators can use cloud bursting, a private cloud bursting into a public cloud, if additional resources are required. Corporations are sometimes hesitant to use the hybrid technology because several private cloud platforms interfacing with public clouds have caused communication errors or

issues; however, hybrid cloud computing allows for translation requests to pacify consumers requiring these current resources (Hanney et al., 2019).

Cloud Platforms

The cloud offers multiple platforms for small and large users globally. The platforms I focus on for this literature review are platform as a service (PaaS), software as a service (SaaS), infrastructure as a service (IaaS), and functions as a service (FaaS). The onslaught of multiple platforms brings many viable options for customers. A social network recently developed for higher education and institutions focused on management, sharing academic content, and cloud-based platforms relevant to assist and manage online classrooms (Nleya, 2016). Showing its expanse and integration into society, cloud platforms are now used for intermediate platforms for scheduling services, assisting multi-robot connections, and interoperability and understanding (Zhou et al., 2020).

Since its inception, cloud platforms facilitating exchange between either side of the market called cloud service providers (CSPs), can create indirect externalities in that its value of the CSP on one side of the market rises, thereby expecting the other side to do the same (Arce, 2020). Cloud platforms offer customers many options to choose from, impacting their daily tasks and administration for the better. Cloud-based platforms can include a database module where each user inputs collected data, an intelligent module for processing data optimizing feasible solutions for evaluation and comparison (Simeone et al., 2019). Cloud computing platforms are now expanding as their popularity and usability soar. For example, to improve the integration of resources like online learning,

additional information resources facilitate interaction between students and teachers using a newly designed learning system based on Google's cloud platform (Zhao et al., 2017).

Platform as a Service

PaaS offers a provider and user greater control of its cloud infrastructure and applications, thus improving security and resiliency, resulting in user access and restricted networks with stern security designations (Ali et al,. 2018). PaaS cloud computing has many benefits to global organizations by increasing business effectiveness within IT processes, reducing costs while procuring, and maintaining IT infrastructures (Ali et al., 2020). Data storage and archiving component cover offer all other business phases within PaaS (Lnenicka & Komarkova, 2019). In all, PaaS offers clients a delivered platform enabling them to develop, run, and ultimately manage their own business applications without the software infrastructure.

PaaS brings the advantages of cloud computing platforms to effectively broaden and simplify the advent of sharing information resources while improving those shared resources (Li, 2017). PaaS also offers an excellent alternative for selective academic institutes which are specified under budget shortages to build, host, and operate their own collegiate e-learning systems effectively, thereby alleviating the purchases for computers, software, and storage; additionally, network devices, licensing, software, and cooling costs assist the maintenance teams without having to administer the entire infrastructure of old (Nasr & Ouf, 2012). PaaS has been a successful platform service because it enables applications to consume a specific cloud to be transferred to an alternate provider

without refactoring the applications entirely (Munisso & Chis, 2017). Since the inception of PaaS cloud computing, its popularity has grown due to minimal development, rapid time-to-market development, reduced pressure on internal resources, and opportunity for scalability, to name just a few of the options implemented.

Storage as a Service

SaaS is recognized as a capable technology providing operational and in-depth financial benefits to firms, and it is dominating IT service delivery models (Oliveira et al., 2019). With SaaS, offers of scalability, collaboration, and efficiency enhance cloud providers with global data centers the ability to provide high levels of fault tolerance through replicating their data amongst vast geographical distances (Astri, 2015). The simplicity of SaaS is providing hundreds of local governments along with thousands of vendors across 20 states a seamless ability to connect, ensuring compliance, which generates new revenues while managing more competitive price-reducing costs. SaaS offers customers a software distribution model where they host customer's applications, making them available to their customers.

SaaS cloud computing offers many benefits for small and large businesses and corporations alike. Cost comparative analysis is common for companies to equate before any data migrations. With that, Scientific Computing World (2019) said not only did their analyses of SaaS vs. on-premises show they were the most efficient decision, and they would also have seen benefits including individual client installations, regulated software upgrades, and user application performance. Another benefit of SaaS computing is its flexibility compared to other options offered by third-party vendors. According to

International Data Corporation (2018), part of the beauty is SaaS cloud-enabled software that can maintain relatively heavy configurations, and alterations can be made through extensions (custom apps) without the core service product being impacted. With the ever-expanding SaaS model, its capabilities seem endless for small and large businesses alike.

Infrastructure as a Service

IaaS is growing in popularity and could be the simplest of all platforms for customer consumption. In IaaS, it is considered the quintessence of all models whereby its users have the ability to manage and provision their own environments into remote physical servers like CPU and storage servers on the Internet. (Chawki et al., 2018). Professional business organizations believe IaaS can match various users' needs in a profitable margin, thereby offering multiple classes delivering various service levels on its elasticity and capacity performance spectrum (Carvalho et al., 2017). An E-Gov cloud's flexibility provides reliable third-party vendors a platform or government administration and many public services to share data resources on cost savings of operations and development, improving load capacities (Liang et al., 2019). IaaS can deliver fundamental computing, storage resources, and network to consumer's on-demand and over the Internet on a pay-as-you-go basis.

IaaS cloud models have many benefits that public and private organizations worldwide can implement and improve their mission and overall infrastructure. IaaS benefits are expanding and offer scalability, availability and access, self-service approach, business agility, and security. By contrast, legacy single-tenant systems can serve clients requiring strict separation from others but can prove costly. In contrast,

updated IaaS technology offers greater scalability, a wider variety of technology options, and stronger security because this platform was specifically created to support hundreds or even thousands of private customers (Violino, 2019). Due to the flexibility of IaaS, the idea of reusability is deployed in a large-scale system allowing the scalability and its multi-tenancy to provide advantages of the cloud model, which is transparent to the users (Bui et al., 2016). The IaaS model has grown so quickly in the computing market by leaps and bounds that vendors have quickly realized they have to create datacenter space worldwide to meet the customer demands (Butler, 2016). Of the four cloud models described, it seems IaaS is playing a large role in the majority of small companies and large corporations alike.

Functions as a Service

The growth of cloud computing has led to another platform referred to as functions as a service. In the simplest of terms, it is a server-less approach to implement modular pieces of code. FaaS allows developers to make extraneous changes to code, which can process/execute immediately to an event, such as end-users being able to access web applications immediately due to the recent update. Server-less computing is exactly what it sounds like; it allows application development without concerns for tweaking, implementing, or scaling a server from the user's perspective. FaaS frees the user's responsibilities from maintaining a server managing virtual machines and configuration management while resource management provides the platform automation in a scalable way (Malawski et al., 2017). FaaS can be more cost-efficient than basic containerized deployments due to its fine-grained micro-services and facilitates

additional creations of those functions (Kratzke & Siegfried, 2020). According to Rajan (2020), a more thorough explanation of FaaS is software architecture as an application is composed into actions (functions) and triggers (events), providing a seamless execution and hosting environment for the developer.

FaaS has many cloud benefits, like providing a means of achieving a server-less vision by empowering developers to execute their own code in response to work events without creating or maintaining a diverse, complex infrastructure. Benefits in FaaS cloud computing allows a developer to quickly load modular chunks of functionality inside the cloud that is executed independently. Developers can now run their backend code without maintaining servers or provisioning itself. Additional benefits of FaaS is the management of horizontal scaling, only pay for what you use, and the cloud administrators control server management. Ideally, developers using FaaS benefit from easy deployments, reducing operational efforts, and the user-friendly, pay-as-you-go pricing (Leitner et al., 2018).

Cloud Security

With the invention of cloud computing and secure data storage, third-party vendors have had to secure their operational datacenters from external vulnerabilities and attacks. The advent of cloud security offers specific requirements involving security information functionality, identity authentication, security management, and access control bypassing attacks (Song, 2020). Cloud security offers ways to distinguish any long-lasting attacks like persistent threats and repeated Denial of Service of Attacks attempting to exploit slow systems deploying password spraying (Jakóbik, 2020).

Employing security utilizing government standards and policies may prevent on-going external attacks if used properly. Due to the increase of cloud security, IT workloads that migrate to the cloud are offered the benefits of provisioning needing to be weighed or balanced against duties and security risks (Kemp, 2018). Cloud security can offer protection of data and applications and infrastructures involving security environments.

As the cloud evolves, given its offerings' unique nature, security threats can take various forms. These unique threats require making individual and unique security measures necessary for successful security management (Alani, 2017). Since the government has integrated into cloud computing use, FedRAMP certifications require stringent security frameworks; they support identified weaknesses improving the certification build process highlighting various improvements through previous flaws (Di Giulio et al., 2017). Cloud security must continue to utilize up-to-date practices to keep the client's data and proprietary information protected. Due to the cloud's popularity, data transfers can equate to enormous data pulls within software capabilities.

The benefits of cloud security vary dependent on the utilization and physical infrastructure the organization is administering. Cloud security can be incorporated into any organization; hence it is highly recommended that cloud customers add to the current cloud security lockdowns ensuring the appropriate provisions are made during the design, development, and deployment, ensuring safe and secure practices are in place (Bhatia & Malhotra, 2018). It is clear that cloud practices are growing at an unbelievable rate, but it is also understood that the larger the cloud becomes, the more security presence it will have to foster. According to Anand (2017), multiple security threats posing

vulnerabilities include data leakage risks, the insecurity of an interface, countless risks in sharing data resources, and internal and external attacks. In all, cloud administrators and organizations of the cloud will continue to benefit by providing additional services: risk management in the cloud, preventing attacks with encryption implementations, and remaining up-to-date on new security risks. Cloud security will continue to evolve and further solidify its security efforts in response to the ever-growing vulnerabilities and threats posed daily.

Cloud Privacy Risk

Cloud security supports the effort of privacy risks with counteractive tools capable of combating external attacks and vulnerabilities. Even today's cloud use, privacy notices supplied by third-party vendors and their data practices/options can protect their privacy through lengthy and free-flowing contextual formats often too difficult for users to comprehend (Karunagaran, et al., 2017). The practice of cloud privacy risk addresses the main challenge of allowing cloud vendors performance rankings computation may unsafely reveal privacy or sensitive data information (Ji et al., 2018). Data controllers have a duty to report any security breaches, while both the processor and controller may be jointly liable for damages from the breach. Both parties must understand and adhere to the standards and rigorous policies held in-place if either expects to maintain their security posture against vulnerabilities and attacks. Each cloud service provider supports a privacy risk of their legal liability, and overall credibility concerns should include sensitive data leak; similarly, this data subject is potentially at risk of having personal and proprietary data exposed since all administrators and

engineers are carrying the burden which needs to be addressed should privacy issues arise (Coss & Dhillon, 2019).

The benefits of cloud privacy and risk practices can lead to a solidified infrastructure and hardened virtual environment capable of battling malicious exploits. Masood and Aslam (2016) stated the main idea of adding a honey pot to the DMZ outside of the cloud network environment would allow data to be encrypted internally, thereby avoiding the insecurity of data leakage and potentially limiting hacker's attempts. Cloud privacy and risk comes with a heavy reliance of trust on the part of the customer, which is especially relevant now due to a growing number of service providers offering diverse cloud services, virtual storage, and enabling complex services and overall workflows (Trapero et al., 2016). Through stern security practices and privacy employments, the cloud and its virtual platform can perform undeterred from internal and external attacks if properly hardened according to organizational guidelines (Abdullah & Abu Bakar, 2018).

GovCloud History

The AWS GovCloud will provide customers with the ability to host and store sensitive data information in addition to regulated workloads. The GovCloud will provide customers with additional workload redundancy, resiliency and durability, and additional disaster recovery options (Preimesberger, 2017). The GovCloud is widespread, and the Philippines have developed a government core objective of developing and creating infrastructure; these services consolidate IT resources, streamline overall organizational costs in implementation and improve operational efficiency (Gupta et al., 2013). The public sector, particularly federal agencies, uses GovCloud to secure cloud infrastructures

despite maintaining compliance with numerous mandates surrounding sensitive workloads and datasets. Although newer than cloud platform services, GovCloud assists federal agencies around the United States and global theater.

The GovCloud is now making data storage possible for sensitive and unclassified information stored via a third-party vendor. GovCloud supports customer compliance through every tier of their cloud journey, supporting certifications, attestations, regulations, laws, security, and additional security frameworks covered by the compliance regimes (AWS, 2018). Due to government requirements deploying GovCloud to military installations, the cloud follows what is considered a high-level security policy employing the most stringent regulations including, HIPAA, FedRAMP, and various other entities (Perry, 2018). The GovCloud is still considered in its infancy, only having been out a decade, but its accomplishments continue to aid government organizations.

In today's cloud society, the benefits of the GovCloud continue to grow at a fast pace to meet the stringent requirements of government storage and security of their sensitive data. Due to their adamant pursual of cloud computing contracts within the DoD, the GovCloud has heralded the conception of the US Federal Government's first cloud policy, which turns out to be the premier global trend of cloud adoption services by governments around the world (Jackson, 2015). Due to stringent government's data storage expectations, the bridging of various government options or services between the government clouds and cloud vendor marketplaces demands more network visibility and security capabilities (Jackson, 2016). Following the Defense Information Systems

Agency (DISA) guidelines, both the cloud and DISA's stringent security requirements will continue to grow and become more practical for military units around the world to deploy.

GovCloud Customers

GovCloud customers can be just as secretive and sensitive as the data storage they seek from their cloud provider. The GovCloud supports world-renowned organizations like the FBI, Department of Veterans Affairs, the Justice Department, and Lockheed Martin, to name a few (Wootton, 2018). These mega-giants understand that GovCloud enforces standards like FedRAMP, U.S. International Traffic in Arms Regulations (ITAR), Department of Defense Security Requirements Guide (SRG), and Defense Federal Acquisition Regulation Supplement (DFARS) for security (Wootton, 2018). GovCloud customers like Cohesity provide comprehensive solutions for customer's broad data capabilities for secured clouds, including backup and recovery, analytics, long-term retention, and protection of Amazon compute infrastructure (Cohesity, 2019). With the cloud's growth, it is assumed that the GovCloud will continue to grow in popularity for government businesses.

GovCloud offers many benefits to grow with its product, like the value of GovCloud costs, security compliance, highly scalable performance, guaranteed uptime, disaster recovery, and no hardware or unpredictable maintenance costs (Histed, 2019). GovCloud customers seek the ability to augment IT infrastructure capacity, enhancing disaster recovery and quicker application development and testing, bypassing the complete re-architecture or retraining of new technologies. The GovCloud has been able

to advance into several government environments by following compliant and scalable cloud practices. With GovCloud, by being 100% cloud-native, it removes the need for infrastructure and the continual maintenance required (such as patches and upgrades), providing global scalability and access (Duff, 2019).

The continuous growth of GovCloud immersing its services into the military and other federal entities simply strengthens its popularity, cloud knowledge base, and ability to abide by government regulations. The Defense Health Agency (DHA) will now be a host of DHA's Armed Forces Billing and Collection Utilization within the GovCloud's U.S. West focal region consisting of data center clusters built specifically hosting the government's most sensitive data. AWS GovCloud is pushing military organizations outside of their comfort zone to explore comprehensive, broad, end-to-end application visibility needed to quickly identify and troubleshoot disruptions while tracking performance before, during, and after new migrations occur to new data center technologies within the cloud; that said, map service dependencies, the cloud, and its trend user-experiences delivering from each of their global sites to data centers and cloud services ensure uniformity and security through quality service delivery.

Conceptual Framework

A strong conceptual framework allows researchers to define the importance of previous research studies that proffer why the topic requires to be extended in accordance outlined by the researcher. Research covering the formation of entrepreneurial intention has truly attracted substantial scholarly attention and interest from entrepreneurship scholars; since its inception, Professor Ajzen has tested TPB by advancing and

challenging many social fields, and as a result, TPB has generated substantial interest amongst many researchers (Tornikoski & Maalaoui, 2019). TPB proposes that behavior is uniquely predicted by behavioral intention, which, in turn, predicted 3 base components: attitudes toward the behavior, perceived control over the behavior, and the subjective norms regarding the behavior itself (Sussman & Gifford, 2018). TPB consists of 3 types of beliefs, and each belief is accompanied by one construct. Attitudes toward the behavior (ATT) and behavioral beliefs, subjective norms regarding the behavior (SN) and normative beliefs, and perceived control over the behavior (PBC) and control beliefs. Additionally, the Theory of Reasoned Action (TRA) prefaces the TPB theory and contributes to its research approach. A scholar/practitioner must understand, select, and integrate the proper conceptual framework into their study to create a firm blueprint. The theories bypassed were self-efficacy theory, transactional/management theories, and change theory since they were not the most representative of this doctoral study. However, they held strong viewpoints that were considered as closely as possible.

The History of Theory of Planned Behavior

Looking back, an extension of TPB was the Theory of Reasoned Action (TRA) developed in 1975 by Fishbein and Ajzen, asserting the most important research determinant of behavior was the behavioral intention (Yang et al., 2017). In past research, TPB was used for illustrative content as an individual cognitively combines subjective norm, attitude, and a perceived behavioral control referencing target IT to achieve an intention to use IT; additionally, each individual cognitively combines their intention and perceived behavioral control to define the use of IT (Ferratt et al., 2018). TPB is a

fundamental approach to research seeking an individual's primary intentions to engage in a specific behavior at a particular place and time, thus resulting in full intention to explain these behaviors over why people do have the ability to practice and exert self-control. Similar to online cloud research, scholars draw on TPB to identify critical factors that may motivate these online customers, including their own beliefs involving trust in the product, the trust of the given information, in addition to attitude and overall intention (Chou & Hsu, 2015).

In its simplest form, TPB is used to understand and predict human behavior, which posits these behaviors immediately determined by each human's intentions under certain circumstances leading to perceived behavioral control (Kan & Fabrigar, 2017). TPB contributes to attitude, in-depth perceived behavioral control, and an assumed self-identity pathway coefficient significant to predictors of intentions. TPB states that behavioral achievement mostly depends on motivation (intention) and ability (behavioral control), distinguishing amongst 3 types of hardened beliefs, behavioral, control, and normative. Typically, TPB is used to predict new and exciting behaviors without including any repetitive behaviors or habits in a stable context (Zhang, 2018). TPB has come a long way since its initial inception researching attitudes, combining perceived controls and norms to predict our overall intentions. In totality, the past few sections are TPB encapsulated, and it is used to predict planned behavior.

Theory of Reasoned Action (TRA)

The TRA prefaces TPB, and it intends to perform specific tasks as a function of 2 individual constructs called attitude and subjective norms (Redda, 2019). TRA

contributes to TRB's success since it introduced the initial constructs of attitude and subjective norms before adding the final identifier as perceived behavioral control. While researching, Ajzen discovered an additional key factor within control beliefs in the human behavior process of decision making, which intrigued him to introduce perceived behavior as the final element. The intention is the immediate antecedent of personal behavior, which indicates an individual's readiness to engage in a relative behavior. Similarly, behavioral intention is considered a core concept of TRA, which posits the individual behavior is directly driven by behavior intention formed by attitudes towards subjective and behavioral norms (Wu, 2020). From a researcher's perspective, TRA has been described as a parsimonious, intuitive, and insightful model used to explain human behaviors widely applied in predicting behavioral intentions. That said, the TRA approach posits greater awareness of most social issues generating positive attitudes amongst them in which that said attitude will, in true fashion, engender a likelihood of younger adults making social commitments (Zarzuela & Antón, 2015).

In research, TRA shows a well-rounded approach allowing flexibility and conceptualization. TRA previously demonstrated its effectiveness in predicting the variability of people's behaviors across multiple contexts, populations, and behaviors themselves (Hagger, 2019). The TRA is quite arguably the most common and widely used theory of its kind. TRA has been used in business management, social psychology, health care, and marketing. Due to its friendly use in research, TRA explains customer's behavioral intentions by assuming each intention is the single most reliable and essential predictor; thus, all humans should be rational while making systematic choices (Paul et

al., 2016). TRA has served as the foundation for extended theories encompassing constructs towards developing more comprehensible explanations of behavior that test salient processes determining relationships between behavior and true intentions. TRA's behavioral intention is viewed as the precursor immediately building to the actual behavior itself; meaning, an individual will react or decide dependent on the behavioral intention easily formed or developed. In all, TRA effectively predicts behavioral intention identifying a compromise, therefore, stopping at one's attitude predictions in addition to predicting behavior.

Theory of Planned Behavior

Initially, the theory of planned behavior (TPB) was proposed by Icek Ajzen in 1985, providing the conceptual framework used in this study. A researcher's choice of the ideal framework is not entirely arbitrary but does reflect their important personal beliefs and understandings concerning the nature of knowledge. Similarly, the ideal framework exists within the metaphysical sense compared to the observer's relation and potential roles. They can adapt the tools to be consequently employed is his/her work (Grant & Osanloo, 2014). With TPB, as a general rule in research, the more favorable the volunteer's attitude and subjective norms are, the stronger their perceived control, the stronger the individual's intention to perform a behavior should be (Suh & Hsieh, 2016). TPB has been applied to an assortment of research issues, such as physical activities, blood donations, drinking problems, quitting cigarette smoking, and fundamental issues like leisurely behavior. Over the past few decades, Information Systems (IS) adopted TPB studies as basic theoretical models for computer resource centers, spreadsheets,

mobile commerce, and electronic commerce services (Yang et al., 2017). TPB is not the most favorable of researchers' research methods, but it gravitates towards human behavior, so there is interest in researching this theory. Within the TPB research, intentions derive 3 factors suggesting whether the individual plays a favorable or unfavorable role in attitude towards that behavior (Proctor et al. 2019).

TPB practice merely explains specific intentions to perform a given behavior, and that intention is correlated to how hard people are willing to perform for that behavior; this explains that people are influenced by attitude, and their subjective norms are a perceived control of behavior (Teo et al., 2016). In turn, 2 variables can determine subjective norms, specifically behavioral beliefs and evaluations of an outcome. The attitude construct plays an immediate antecedent predicting an individual's intention to participate in particular behaviors (Redda, 2019). TPB is such a vast research area that Ajzen realized the more positive a person's attitude and subjective norm were, the stronger their perceptual behavior became, identifying that individual's necessity to choose and implement exact behaviors (Yang et al., 2019). TPB has emerged in the scholastic community as a major framework for predicting and changing the fabric of human social behavior from its roots. The following descriptions will delve into all 3 types of TPB beliefs and their constructs in detail to paint the overall picture of TPB.

Theory of Planned Behavior: Attitudes Toward Behavior (ATT)

TPB research is broken down into 3 distinguishable identities: attitude towards the behavior, subjective norms, and perceived control over the behavior. This section will specifically speak to the attitude of TPB within research development. Weber and

Gillespie (2001) posed, about attitude within TPB, data sets show the significant differences existing between action and belief, intention and belief, intention and action, and the true rationale used to support a belief, its intentions, and how each action differs from one another (Weber & Gillespie, 2001). Additionally, prior studies on the growth and acceptance of technology adoption consider the relative concept of attitude. Whether reflecting favorable or unfavorable feelings concerning particular behavior, it is just as important a determinant influencing their intention to use (Yang et al, 2017). Historically, TPB attitudes were assumed to be predictive of behavior, although this assumption has often been viewed and held as compelling evidence under the contrary. If researching perceptions of feasibility and desirability in entrepreneurial event models, it would have similar overall effects on intentions, caused by attitudes and behavioral controls as referenced in TPB (Alam et al., 2019).

The attitude in behavior plays a composite role in TPB research, and overall attitudes impacting the results. Due to TPB's growth and its components such as attitude, corporations, and organizations alike attempt to utilize psychological behavior changes to attract business. For instance, the travel industry practitioners and researchers began to turn their undivided attention to extraneous psychological constructs like beliefs, attitudes, and values they seek to meet for various responsibilities and customer expectations (Li, 2017). As Lai (2017) described, attitude is also defined as an individual's evaluation of said object and a defined belief creating a link between some attribute and that object leading to behavior due to intention. To understand and respond to TPB's attitude component in an individual's behavior, higher education institutions are

exploring the importance of both models and theories of unethical IT use; apparently, it is more obvious at the social level given technological changes can penetrate societies faster than these new attitudes towards implemented legal codes and ethical adopted standards (Ghiatâu et al., 2019). The component attitude impacts researchers and professional organizations globally, considering the true influence behavior has in an ordinary environment.

Theory of Planned Behavior: Behavioral Beliefs

The construct of ATT is identified as behavioral beliefs. In the simplest of terms, BB refers to its motivational factors that influence a given behavior suggesting the strongest intention to perform this behavior, the more probable the behavior is to be performed. Like the military cloud computing environment, administrators and engineers utilize every possibility to stand apart from their peers. Thus, the successful implementation and administration of third-party cloud storage is a positive start. This optimistic and expectant behavior acts as a motivational tool to succeed and deliver a product for the organization. Behavioral beliefs can produce favorable or unfavorable attitudes regarding their behavior and guides true considerations of both positive and negative outcomes. Gkargkavouzi et al. (2019) stated their behavioral beliefs mainly guide an individual's behavior regarding possible outcomes of that behavior and the final evaluations corresponding outcomes producing a favorable or unfavorable action toward that attitude. Behavioral beliefs can dramatically influence an action's overall result if that belief overrides every other sense leading to an expected outcome. Similar to taking a math exam, various theories posit that if attitudes and self-beliefs should truly predict

students' final achievements in mathematics, a great deal of independent research has proven this is indeed the case (Niepel et al., 2018).

Behavioral beliefs are sometimes referred to as behavioral intention, along with a person's pre-existing attitudes. It is these intentions predicting or even ultimately guessing his/her behaviors or responses. This designation truly epitomizes the motivation of those responsible for deploying this new cloud computing third-party storage practice. Cloud computing is a new practice to military installations worldwide, and it is these new practices that may trigger positive emotions previously experienced by current engineers. Therefore, replicating a project's completion with success could activate the desire to prosper by reliving that behavioral stimulus. Like an individual's perspective, behavioral beliefs point or refer to the once perceived advantages and disadvantages of actually performing a certain behavior (Yuriev et al., 2020). The behavioral belief's intention, for true results, must be specific enough to predict a specific behavior.

Theory of Planned Behavior: Subjective Norms (SN)

TPB's second component is subjective norms, also known as social pressure arising through other people's expectations, also seen as the individual's perspective. Subjective norms are comprised of 2 components described as the individual's normative beliefs. In all, what he/she perceives to be what researchers want or expect; second, is the individual's motivation or driving need to comply with what others want or expect. Lee (2017) states subjective norms that each individual is exposed to or privy will have a true impact on their intentions in recognition of the man being, by his nature, a social creature, so they will no doubt care about the opinions of what others think, or in fact, believe.

TPB subjective norms in true form refer to the belief about whether most people approve or disapprove of their behavior related to an individual's beliefs about whether those peers and others of importance think they should engage in further behavior. As researchers apply this TPB component, the question format is the most used formula measuring subjective norms; this leads respondents to, at best, a well-defined, or to a well-defined range of specified people (Passafaro et al., 2019).

The benefits of utilizing subjective norms as a TPB component favored the researcher utilizing the practice since many factors weighed into their efforts. The subjective norms determined by an individual's normative beliefs determine whether important people like friends, teachers, or parents disapprove of their particular behavior and the important people's specific appraisals of that behavior (Guerin & Toland, 2020). Subjective norms are also important to a researcher because positive support from persons, individuals, or particular organizations with meaning becomes greater; thereby, their attitude also improves (Peng et al., 2014). Human nature can yield positive results when highlighting a subject that the individual identifies as positive or preferable concerning a subjective norm. Moreover, researchers found that people's subjective norms commonly turn towards specific groups for their judgments or standards towards a particular behavior (Sun et al., 2020). Lastly, the effective composition of injunctive norms that most people are meant to follow to perform any given behavior describes the perception of what/how people are doing (Fishbein & Ajzen, 2011). In review, subjective norms can be determined by perceived social pressure or others to behave or act reasonably, which is motivated to comply with other views.

Theory of Planned Behavior: Normative Beliefs

Subjective, also referred to as social norms, refers to the customary codes or behaviors in a group of larger cultural context. These norms are identified as normative in groups of people. Normative beliefs are beliefs that an individual is accepted by particular groups of people and dictate whether that behavior in a specific fashion is appropriate. According to Fang et al. (2017), while the social norm is meant to refer to broad ranges of permissible, although not necessarily required behaviors, these beliefs call a specific behavioral act by the performance of what is expected or even desired under given circumstances. Normative beliefs practice 2 general uses; it aids in the prediction of more variables like subjective norms and intention and wishes to perform interventions measuring normative beliefs providing data where intervention efforts are truly focused. TPB's normative beliefs are estimated by the cumulative data of all normative beliefs, referent's opinion performing a specific behavior in addition to the motivation to comply with each referent (Salleh, 2016).

Theory of Planned Behavior: Perceived Behavior Control (PBC)

The third and final component of TPB is behavioral control. PBC is assumed to reflect many past experiences with the behavior's actual performance and its anticipated obstacles, which could inhibit the behavior itself. This clarification of these dimensions of PBC could help a consumer's behavior research since it is expected to enhance the validity and reliability of the PBC definition; accordingly, this will enhance the predictive accuracy of the 2 variables PBS and TPB (Kiriakidis, 2016). In research, Ajzen (2006) perceived behavioral control, commonly assessed, is 2 components: self-efficacy (largely

dealing with the ease or difficulty performing a behavior) and controllability (the extent to which the performance is entirely up to the actor). A continuous review of the PBC component seems that it directly predicts behavior as well. Conversely, understanding perceived behavior control can have a direct effect on and had zero impact on intention. PBC identifies individual attitudes toward a behavior to emanate from certain underlying salient beliefs referencing outcomes of that behavior; additionally, those social pressures are quickly influenced by salient beliefs factoring whether others important to this individual can believe they should perform that behavior (Chipidza et al., 2019). Intentions performing behaviors of various types can be predicted with exceptionally high accuracy from different attitudes towards that behavior, true subjective norms, or perceived behavioral control; these intentions are tied together with behavioral control perceptions, accounting for variance in actual behavior (Ajzen, 1991).

With PBC in research today, there are benefits for potential researchers to utilize this theory and its components. Prior research states an individual's intention is ultimately affected, mostly in part, by their perceived behavioral control, which also found that PBC had a tremendous effect on behavioral intention to learning. Understanding PBC is important for behaviors identified as not under volitional control extending the PBC as it really reflects all external factors which can impede or facilitate the performance (Cheung & Chan, 2000). PBC offers flexibility, which suggests individuals are rational and are truly affected by motivation within their own decision-making processes, making it a reasoned choice amongst various alternatives (Sarmah et al., 2018). In the simplest of terms, PBC is used in research since it refers to people's

ideal perceptions of whether or not he/she can perform the identified behavior and how easy the application is to perform. PBC directly influences people's behavioral change and can moderate or even mediate relationships between behaviors and intentions (Kauer et al., 2016).

Theory of Planned Behavior: Control Beliefs

The theory of planned behavior control beliefs supports the perception of likely factors to inhibit or facilitate these behaviors (Ryan & Carr, 2010). These factors include control beliefs, internal control factors (personal deficiencies, information, skills, emotions, and abilities) in addition to external controls (opportunities and dependence on others). Control beliefs reflect information individuals have with the performance of any behavior, although this take is sometimes inaccurate or incomplete; the reason is it may rest on irrational premises or faulty information biased by motives like anger, fear, or other unknown emotions. According to Anand (2017), control beliefs can dictate your overall perceived behavioral control as each factor is viewed individually. One's perception of the power of that control may differ from the power additional control factors maintain. Control beliefs are beliefs which reflect information people maintain concerning performances of any given behavior, but his data can also be inaccurate or misleading and incomplete; in all, it rests on irrational or otherwise faulty premises, by fear, anger, bias by self-serving intentions, or otherwise reflect failed reality (Ajzen, 2011).

Human action is identified by 3 variations of considerations like behavioral beliefs, normative beliefs, and control beliefs, which believe that factors impede or

facilitate the behavior's actual performance. In addition to additional opportunities and more resources, individuals tend to believe they possess, and the fewer impediments or obstacles they anticipate, the greater the control beliefs over the behavior (Ajzen, 1991).

Analysis of Contrasting Theories

Theories are explanations where a system of constructs (concepts) and its propositions (the relationships between the constructs) collectively presents a systematic, logical, coherent explanation describing a phenomenon of interest within boundary conditions and assumptions (Bacharach, 1989). Besides, contrast theories allow each researcher to predict specific differences amongst cases, thereby testing to see if those differences reflect the data (Allen, 2017).

Self-Efficacy Theory

In total, there is an abundance of choices to choose from to satisfy the requirements for this doctoral study, and the TPB seems to be the most identifiable and required theory supporting case studies. In contrast, multiple rival theories were reviewed, contenders but not chosen for this scholar/practitioner study. That said, Self-Efficacy Theory, otherwise known as SET, reflects confidence in one's ability to exert complete control over one's true motivation, social environment, and behavior. SET indicates that individuals with high self-efficacy are more likely to engage in realistically evident and challenging tasks than those with low self-efficacy. Regarding its stability, SET aligns with personality traits referring to the psychological structures making an individual's behavioral tendencies stable, consistent, and persistent (Li, 2017). Self-efficacy and self-esteem, although similar, are not parallel beliefs. Self-efficacy relates to

an individual's self-worth or the overall value of a human being. In contrast, self-esteem is focused on "being" or feeling accepted just as you are. In other words, people with high self-efficacy usually have high motivation levels and vice versa, although it is not what one would consider a foregone conclusion.

The benefits of using SET to support case studies promote the success of participants supporting research questions and other additional facets of research because of their motivation to succeed. SET backs beliefs in one's ability to confront various situations that play a role in how one feels about themselves and whether they can successfully achieve their life goals. SET is a positive TPB component but must be used carefully and consider when dealing with people like students. In higher learning, the less likely the positive relationship, the greater the chances students will frame a negative image completely underestimating their abilities; thus, the role of SET in motivating students a top priority for academics explaining performance is vital to success. SET is also impacted by IT's world and its many technical requirements to learn how to use PCs, the Internet, etc. SET significantly impacts a user's satisfaction and image, implying that more confident students feel navigating the web, using email, and learning online tools is perceived as success and meeting lofty expectations (Abdullah & Abu Bakar, 2018). Positive thinking leads to positive accomplishments when dealing with self-esteem and control. In self-efficacy, belief in one's own abilities to deal with unexpected scenarios can play a vital role in how someone feels about themselves and whether they choose to succeed in life by achieving goals. In its simplest terms, self-efficacy supports TPB by

believing in our own abilities, specifically our ability to confront challenges before successfully completing the task.

Transactional/Management Theory

Transactional leadership (TL) theory was another approach that could have been used to complete the study but quickly learned it was too direct and not creative enough. Meaning, TL theory is more apt to become a military commander or is comfortable running large corporations that require stringent rules and regulations to complete objectives on a timely basis satisfactorily. On the other hand, TL's will not be a solid fit for places where their creativity and innovative mindset will not allow ideas to flourish. Think tanks are assumed to utilize TL regularly since it creates an atmosphere more conducive to knowledge creation, exploitation, and sharing; in particular, while pushing and encouraging intellectual development, paying specific attention to workers allows TL's to motivate these exceptional workers through shared knowledge (Senyo et al., 2018). TL can be an effective approach if current TL styles simulate employees specifically based on intrinsic motivation enhancing productivity, which should be considered too. Successful TL practices center on the rewards and final consequences of not achieving goals, motivating an employee to be more innovative, thereby motivated by end-goal success.

The benefits of using TL are that people follow great leaders since they inspire them, and that leader exhibits an ideal vision and passion emphasizing supervision, performance, and organization. Positivity breeds positivity, and TL's are people choosing to be responsive to their subordinate's necessities who follow them to satisfy these

qualitative necessities. TL focuses on their supervisory role, ensuring enhanced performance and organization while also focusing on structure and subordinate success. TL's importance can lean on trust in an organization, which was discovered that in many cases that trust is lacking, TL leans towards the overall efficiency promoting positive learning performances.

Change Theory

Lastly, the Change Theory was also a credible choice but did not meet the needs sufficient for case studies leading to success. CT allows the implementation of change agents to draw from existing knowledge bases leading to better contributions to collective knowledge and meaningful change. CT, similar to TL, promotes success using solutions offered to enhance motivational strategies with existing behavior. CT forms an organizational pathway towards impact, thereby creating links between development and a research project and environmental outcomes delivering explicit and critical analysis through a series of change processes. CT can be developed during multiple stages like planning but is also useful for evaluation and monitoring, which can develop evaluation questions, identify indicators for monitoring, and identify gaps in data providing a structure encompassing reporting and data analysis.

Transition and Summary

In this section, the study's sole purpose is to explore strategies senior IT military leadership uses to implement third-party cloud computing for data storage. Within this section, the history of cloud computing was introduced, and with the new use of GovCloud computing, the military has decided to take advantage of their production

environment. The literature review was a candid explanation of cloud computing, including the history of cloud computing, public cloud, private cloud, hybrid cloud, cloud platforms, cloud security, security privacy and risk, GovCloud history, GovCloud customers, and finally, conceptual framework. Main cloud platforms were discussed, which were Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Functions as a Service (FaaS). In section 2, the study's purpose is identified in addition to the researcher's role, data collection, and data analysis techniques, to name a few. Finally, the methodology and justification for using that method are covered in detail.

Section 2: The Project

In Section 2, I discuss the project thoroughly, including the employment of a qualitative single case study. This section specifically details my role and the procedures for gaining complete anonymity for each participant. Next, full justification and descriptions are provided for my participation population. Additionally, the method and design are addressed with the data collection tools and research ethics. Finally, data analysis is presented in addition to the information gathered through the study's reliability as a whole before concluding with a transition into Section 3.

Purpose Statement

The purpose of this qualitative single case study was to investigate strategies military leadership uses to implement third-party cloud computing for data storage. The participants were SME, such as cloud architects and virtualization engineers with prior DoD experience from a random selection of men and women within the IT industry. Members did not have to be current active duty or veterans, but any prior DoD experience meeting the extended requirements was necessary. Implications for positive social change include increased cloud computing security practices for military units to improve their current knowledge base, trust, and data storage evolution with third-party vendors. These practices can improve the military personnel's safety and security, protect their families, and preserve national security.

Role of the Researcher

As the researcher, my role was to conduct a qualitative single case study by collecting data, analyzing the findings, and, most importantly, providing results with an

unbiased outcome. Through examining collected information through various methods, researchers they can corroborate their findings over data sets, reducing the impact of probable biases that may exist within a single study (Bowen, 2009). Similarly, Hammarberg et al. (2016) mentioned the validity and reliability of the terms are contentious amongst qualitative researchers, some of them preferring verification; in turn, research robustness and integrity are just as highly valued in qualitative studies as they can be in other forms of research. I was fortunate enough to work as a cloud engineer within this topic and interfaced with many professionals through hands-on training and networking. This is a familiar process since the researcher was able to assist many units and organizations alike migrating from local storage to AWS GovCloud Impact Level (IL2) to IL4 housing sensitive and unclassified data containers. For a researcher, the pre-understanding and true openness, distance and closeness, and construction and the situating of knowledge; plus trustworthiness and integrity, sheer power relations, and overall ethical dilemmas are certain primacy in qualitative methodology (Råheim, et al., 2016).

The Belmont Report summarized 3 ethical principles that they determined guide human research: respect for persons, beneficence, and justice, which exemplifies the primary ethical framework for all researchers to follow to this day (Kirsh, 2019). It is known that practices applied to research involving individual human subjects, the overall benefits, and burdens of those participating in a research study should be fairly distributed (Mueller & Hook, 2006). The plan was to honor and adhere to these basic guidelines without question or issue because the men and women involved were civilians,

contractors, or government schedule (GS) personnel who have been in and around the military and its practices for many years. For that reason, nothing but the utmost respect was provided to each participant, and I continued to treat them as the professionals they were after completing the study.

The Belmont Report was created in response to a study in Tuskegee, resulting in Congress passing the National Research Act, which protects Human Subjects of Behavioral and Biomedical Research (Kirsh, 2019). Remaining focused and determined mitigated any bias from the study while reviewing data and making conclusions. Scholars have asserted that if the interviewer purposefully maintains a specific bias and leads to effects in the tone with which they ask questions, there is zero doubt the resulting information will result in a skewed study (Adhabi & Anozie, 2017). Lastly, data bias can be controlled when research is combined using complete observations or completely unstructured observations, expanding the true sample size of the total number of people contacted by the researcher; and providing cross-checks testing for bias within the actual field data (Gaber & Gaber, 2018).

In this research, I implemented a rationale for an interview protocol while using a semistructured interview (data triangulation) and data analysis. I had data from the multiple interviews, organizational documents such as infrastructure builds and server farm layouts, encompassing the specific criteria required for that portion of the study to achieve triangulation for data analysis. Methodological triangulation has its strengths and weaknesses and uses multiple methods to combine various opinions into a singular topic, allowing comprehensive cross-checking elements for validation. Online interviews were

incorporated, ensuring proper data collection. Additionally, with the implementation of member checking and methodological triangulation, I used both practices to increase the validity of all future findings resulting from the volunteer's information. Combining different approaches into one method is a useful tool many researchers can employ to meet the basic foundations of success for that specific research point. The use of methodological triangulation is employed to converge several methods upon a singular conclusion better supporting a conclusion than one of the multiple methods arriving at a conclusion (Heesen et al., 2016). Member checking in a qualitative research study is implemented when researchers use multiple sources of specific evidence increasing their validity of any given study (Candela, 2019).

Throughout the span of the research, the use of cross-checking data or triangulation, was incorporated using multiple data resources for theme verification. For simplification purposes, my member checking practice focused on semistructured research question interviews for validity, accuracy, and credibility. In research, the purpose of data triangulation is not always to cross-validate data. Instead, it may be to capture various dimensions of the exact phenomenon itself. Data triangulation is considered less of a strategy for validating results and procedures than a true alternative to the validation, increasing scope, consistency, and depth in methodological proceedings (Wilson, 2014). Additionally, data triangulation uses variances in events, times, settings, and so forth may illuminate, revealing atypical data and recurrent patterns, improving all the findings (Turner & Turner, 2009).

During the interview protocol, when practicing triangulation, trustworthiness through triangulation increases confirmability, credibility, and dependability in overall qualitative studies (Johnson et al., 2017). Semistructured interviews can effectively use standardizing questions, moderating levels of involvement, and data saturation to solicit as much information as possible. While employing these online interviews, persistence requires a consistent, skilled, and motivated facilitator to identify any underlying discussions potentially recognized, contributing to the data collection. Therefore, the researcher must supervise existing relationships with their participants and create a comfortable and relaxing environment for any unfamiliar participants new to this process (Nyumba et al., 2018). Employing interview protocols were enforced for member checking and methodological triangulation, ensuring data saturation and alleviating total bias. The results provided me the opportunity to return to randomly speak to interviewees and verify the accuracy reported, and I was able to conclude that each narrative was complete, thereby validating data saturation had occurred.

Participants

This study's target population included 22 SMEs such as cloud architects and virtualization engineers with prior DoD experience from a random selection of men and women within the IT industry. Members did not have to be current active duty or veterans, but any prior DoD experience meeting the extended requirements was necessary. In this study, to participate, each volunteer was a minimum of 18 years of age; additionally, they were an administrator, engineer, or architect overseeing cloud administration or will be a senior-level technician maintaining GovCloud infrastructure

for a minimum of 3 years. In terms of young researchers, learning to write in a scholarly fashion meeting peer-reviewed expectations was a stringent task; however, when invited to understand the intricacies of these rules, it taught the researcher in-depth research and professional participants enabled the discovery of difficulties, specificities, and the overall responsibilities involved (Rodríguez-Bravo et al., 2017). All participants had a minimum of 5 years of IT experience and at least 3 years of cloud knowledge in administration or engineering to meet study requirements.

Accessing the participants was not a simplistic task. Using semistructured interviews, a single case study was used implementing social media for previously employed active duty members who had separated and worked in a Communications Squadron or Cyber organization. Additionally, those men and women with military communications IT experience were recognized and offered an opportunity to complete a face-to-face, telephone, or Skype interview reviewing research questions for military cloud computing. After approval, I started with random sampling from military veterans with IT experience in cloud computing. Approximately 20 to 25 laid the baseline solidifying their experience, technical expertise, and future military cloud computing and data storage expectations using third-party vendors. According to McGrath et al. (2018), rapport is crucial throughout the interview, thus enabling the respondent time to provide a detailed and rich account of their own experiences at the center of the study.

Each participant in this study aligned with the focal point research question of what strategies senior IT military leadership are using to implement third-party cloud computing for data storage. I vetted each participant's credibility because I am a certified

AWS Cloud Engineer and assessed the interviewee's qualification. Importantly, the influence of credibility is something researchers strive for while designing their study, collecting or analyzing their data and thinking about ways to present those findings to the reader (Hoque et al., 2017). Building a rapport, requesting honesty, and validating credibility is just a small sample of what can be injected into a successful research collection of information. A strong rapport can assist in collecting quality information during an interview hinging on the researcher's ability to place them at ease as well as quickly earn trust; if not, the participant will remain nervous, hesitant, or even suspicious to share their opinions or stories which will prevent the study from obtaining good information (Margolis, 2017). The advantages of building a strong rapport and a professional relationship using a qualitative research approach allows the interviewer to ask open-ended questions while offering probing questions and allows participants an opportunity to respond in their own words (Mack & Woodsong, 2005).

First and foremost, all research questions were presented to all participants in a way that they understood, acknowledged, and responded to without multiple questions seeking clarification. I used professionalism to introduce each question with clarity and conciseness to make every effort to avoid misconceptions from the participants. An individual should retain the capacity for an individual's overall consent to relatively simple research but can have extreme difficulty with their participation decisions. The actual procedures and/or their risk-benefit considerations seem complex (Palmer, 2015). Some researchers may, at times, consciously decide to provide information regarding their own experience and background in an attempt to reduce the imaginary power

imbalance between them (Waller et al., 2015). Likewise, I ensured that the participants understood I was a combat veteran in Iraq, Afghanistan, and multiple other contingencies, which provided the men and women with the knowledge and that I was trustworthy for also having served honorably.

Research Method and Design

In this study, qualitative research was implemented. It was a single case study design that suited the focus and was the most appropriate for exploring the strategies SME such as cloud architects, and virtualization engineers tended to implement third-party cloud computing. Analyzing qualitative data swiftly and rigorously are important for an applied researcher aiming to relinquish solutions to practical problems and their social conditions directly impacting the world (Watkins, 2017). Accordingly, a single case study creates a convincing theory if the suggestions are intensely embedded in several empirical studies (Gustafsson & Gustaffson, 2017). Therefore, a single case study design was the most appealing choice of the selections because its efficient approach to identify and question multiple veterans with IT knowledge highlighted experienced professionals on the subject of cloud computing.

Research Method

A qualitative method was used because qualitative research is obtained through conversation and open-ended communication, identifying what people think and why they believe so. The qualitative method in this study was a collection of narrower data sets normally associated with quantitative studies. Benson & Filippaios (2016) noted that enforcing a qualitative approach helped capture and map statements, non-verbal cues,

feelings, contexts, and actions to include social relationships and sections of each participant within their social settings. This particular cloud computing topic is relatively less theory-driven solidifying, qualitative, and the quantitative approach. Qualitative research is not one-dimensional, meaning it is not statistical and can incorporate multiple realities (Rahman, 2016). Understanding that the qualitative research method can be somewhat dynamic provides the proper focus to ask the necessary research questions and keep an open mind. At the same time, the participants expanded on their experiences. Research like qualitative methods is specifically designed to assess each users' experience. Thus, how and what their participants feel is truly an intrinsic part of each experience and its emotions, which are the driving factors behind what these participants do.

The quantitative method was considered for this doctoral research, but it did not meet the basic requirements. The quantitative viewpoint can limit a researcher by solely focusing on numbers that can detract and lead researchers to overlook comprehensive themes, thereby risking big picture data benefitting research. Quantitative methods also assume their research is more credible because it is based on statistics instead of mere observational research. Any researcher's idea can pose biases or indirect opinions negating the proper approach to collective information gathering. Additionally, quantitative methods heavily rely on the ability to anticipate in their research what must be reviewed and measured in advance (Noyes et al., 2019). Non-experimental research method designs often fail to provide sufficient data, making a convincing argument supporting correlation, let alone causation (Lee, 2017). Quantitative researchers must

develop their hypothesis and use an effective model for analyzing collected data, especially considering that errors in the setup or bias on the researcher's part can lead to troubling mistakes, invalidating all of the results. A large percentage of quantitative research's respondents is required for a true representation of its target population, which is one reason this method is difficult, is expensive, and demands much time to perform analysis.

Mixed methods were also considered due to the combination of both qualitative and quantitative methodologies. Mixed methods can be difficult for a researcher since employing this method calls for expansive knowledge in qualitative and quantitative research. Similarly, a researcher must dedicate an infinite amount of time to their research since it is time-consuming, leading to greater expenses, which can be a large discouragement to researchers. For a clear and decisive study, the researcher must prioritize every component, ensuring established guidelines are set before commencing research, leading to contradictory results. Using mixed methods research, sufficient time is expected to collect and analyze trends from the first data set before commencing collections of subsequent data; thus, if sufficient time is not allowed for analysis, the secondary data set will not address the key issues from the initial data set (Halcomb, 2018). Mixed methods design combines exploratory and confirmatory components superior to traditional methods if applied to research beyond basic hypotheses, with generational testing towards insights into mechanisms responsible for variances in outcomes amongst groups.

Research Design

A single case study design was chosen as opposed to ethnography and phenomenology. Case studies can be conducted at various points within the research process, providing researcher's ways to develop exceptional ideas for additional projects in the future. One definitive aspect of a single case study is that it offers an incredibly flexible and efficient assessment and treatment development within the evaluation process. Single case studies also act as effective broad range conduits covering multiple research methods non-prejudicial against any specific research type. Moreover, one strategic implementation might be chosen vice another is solely the researcher's responsibility and his/her intentions to meet the study's requirements (Crowe et al., 2011). Approaching this research design as an exploratory role, the single case study design will contribute to the research providing clarity and new insight. Since a single case study approach was used, comparisons were drawn throughout the research. These chosen cases predicted similar outcomes and potentially contrasting results based on theory.

Ethnography was considered for this research design, but it did not fulfill the study's parameters. Ethnographic methods can assess an existing design. However, in its simplest terms, ethnography is holistic in nature, including a formal history of the culture being studied and their practices, routines, and discussions of that specific environment (Hurst & Taccone, 2013). In ethnographic research, ethnography requires well-trained researchers, is time-consuming and takes time for both researchers and participants to build trust and rapport for full discourse (Malinowski, 2016). Ethnographic data

collection can be challenging and time-consuming, so the framework approach is highly recommended. In contrast, the framework approach is rigorous, logical, and transparent, particularly suitable for managing large amounts of information that remained close to its data (Jones & Smith, 2017). Ethnography was a strong choice for this research method since it focused on understanding each participant's perspectives and observing their everyday life actions, which was too time-consuming. In all, ethnography was not chosen because research takes too much time. It can lead to bias. The success of the research truly depends on the honesty and cooperation of the volunteers within the study.

Phenomenology allows us to better understand the full meaning of people's lived experiences, so the study explores people's experiences in-depth of the actual phenomena. Phenomenology was not chosen because new researchers can gather interview transcripts, unstructured notes, and personal texts simply to emerge as unorganized until all information is reviewed and organized. Secondly, since phenomenology can accumulate large quantities of recordings and interview notes, a researcher can find it difficult to identify key themes right away, causing research. According to Pringle et al. (2011), the phenomenological approach can offer difficulties at times; however, it has also been documented that even the terminology and definitions can be unclear. Phenomenology, a qualitative research design, fits the inquiry of discovering participants' experience and perception within a phenomenon (Ataro, 2020). In a research environment, phenomenology can be a powerful strategy well suited to explore challenging problems and build a greater understanding of its nature to properly align between particular research questions encouraging scholars to utilize its research

more frequently. A research methodology, the phenomenology approach uniquely positions scholars to learn and grow from other's experiences. However, this is a powerful method for inquiry. The basic nature of phenomenological research is and can be, intimidating to researchers (Neubauer et al., 2019).

Data saturation must be implemented in an approach that is consistent with all research questions and analytic framework and theoretical positions adopted; similarly, there should be limits to its scope not to risk true saturation losing potency and coherency if its conceptualization and practices are too widely stretched (Saunders et al., 2017). It is widely apparent if data saturation is not reached within this research product; the outcome will most likely hamper content validity. While choosing the study design, it is imperative the focus on aiming for a design that explicitly details how maximizing data saturation is recognized. Data saturation is achieved in research when the complete range of research constructs that make up the theory is represented fully by the data leading to no more emerging themes (Saunders et al., 2017). The correct sample size must be chosen, which affords the greatest opportunity to reach data saturation. A large sample group cannot guarantee the data saturation sought, nor can a small group.

Population and Sampling

The population planned for use will be administrators, engineers, and architects overseeing cloud administration or a senior-level technician maintaining GovCloud familiarity. Employers tend to use their secretaries or individuals of their Human Resources department as gatekeepers, an initial first-line defense from any external employee or unplanned visitors. Fortunately, gatekeepers will not play a role in this study

since the population is comprised of men and women with previous military cloud computing experience found on social networking like LinkedIn, etc. If the DoD currently employs them, they will be identified by other volunteers who feel they are a positive fit concerning the minimal requirements the researcher has set forth. Plus, there is no given timeframe away from the DoD as long as he/she has the necessary systems engineering or architectural background for cloud computing. A qualitative research protocol practicing the semistructured research questions during interviewing occurred when the researcher's judgment chose selected elements for a specific sample.

Choosing a specific population knowledgeable to include that in-the-know about cloud infrastructure was more difficult than initially assumed. Although most IT offices and Communications Squadron personnel are very aware of the migration to third party cloud practices, pinpointing and specifically narrowing down senior administrators, engineers, and architects is a delicate balance between networking and politics. Therefore, the study starts with 22 participants. The most representative and forthcoming with this new technological practice is referred to as GovCloud computing.

It is important to know that populations chosen for qualitative samples are purposive, meaning, chosen by their capacity to produce richly textured information pertinent to the investigated phenomenon (Vasileiou et al., 2018). Besides, the mere idea of selecting a sample population is to gather with the smallest (least) number of volunteers or participants (Malterud et al., 2016). Amongst the administrators, engineers, and architects, the researcher believed it would benefit the study to start with the Linkedin social networking page to quickly identify and invite the first dozen participants

into the study. As previously mentioned, each participant must have acquired at least 3 years of cloud experience and 5 years of hands-on IT experience to be accepted to interview. If the need for additional engineers and architects is required, each participant will be asked to supply a solid reference they may know and want to volunteer. Regardless of the number of participants interviewed, data saturation was practiced and acquired to meet university requirements.

For this research project, a single case study using semistructured interviews was the most beneficial. In turn, after gaining full access to each preliminary sample, these participants can begin to introduce others they feel would be interested in the research; additionally, this random process continued until full data saturation was achieved. The researcher identified and announced the anonymity and confidentiality of all data received, guaranteed by the researcher. Simply put, non-probability sampling concentrates on techniques where units were investigated solely on the judgment of each researcher. The saturation point is a simple term used to represent any moment throughout data analysis where identical themes keep recurring. At the same time, no new material is introduced through additional data sources. In all, saturation is important since it provides indications of data validity, therefore included in criteria accessing the quality of the research (Hennink & Kaiser, 2019).

Ethical Research

It is the researcher's responsibility to explain and identify the study and its expectations in totality. Each participant's role was explained and how the researcher planned on protecting them from external parties. The Belmont report enforces ethical

principles each researcher must follow to ensure fairness and equality throughout their research. Technology offers new researcher's ways to carry out explorations in education and learning, although these opportunities can provide new ethical challenges (Haythornthwaite et al., 2016). The researcher planned to ensure that all of the research material was approved by the Institution Review Board (IRB) before proceeding any further with any participants. The informed consent process requires many consent elements, including study purpose, costs, benefits, risks, compensation, procedures, volunteerism, confidentiality, and withdrawal (Lindsley, 2019).

The overall privacy is a top priority for all the participants and their responses to research questions during their interview. A solid rapport must be built with each individual the researcher hopes will quickly form into a trusted relationship amongst us all. In this situation, participants' potential ethical hazards or risks must be taken extremely seriously by any researcher, especially when a specific duty of compassion and caring exists beyond the research project (Hoffmann et al., 2018). The consent form will ensure confidentiality and protection, detailed in the actual form when emailed to all participants. The consent form plan is to disperse it to senior administrators, engineers, and architects is displayed in Appendix A. Similarly, each participant will also have an option to accept or decline at any time in person, by telephone, or email. Similarly, the consent form for non-senior IT military leadership was listed in Appendix A1 with identical original options. By returning a signed consent form, each participant (volunteer) understood the study's nature and was still aware they could have opted out at any time during the interview should it be necessary.

Each participant was advised of their voluntary participation and how their responses to the questions was stored away after each interview. All participants were notified that their information will continue be kept on a disc and encrypted for security purposes inside the researcher's basement and a 500lb capacity steel vault. In research, secure storage is vitally important. This is simply one aspect from a larger group of habits and behaviors that are important during the handling of research data meant to be kept confidential. The data collected from each participant will be securely stored for 5 years to protect everyone's confidentiality. There has been controversy offering financial incentives to varieties of research participants, and this long history remains a contentious issue in current discussions about ethics research in addition to institutional reviews humans/bodies ethics committees; thus, they are given the responsibility of concluding whether these incentives should fall within these ethical guidelines. There was no type of monetary incentives offered to the participants for the study. The researcher performed a transcript follow-up to ensure they were honest and open about their experiences and did not want them to be financially motivated or swayed in any fashion or form.

As the study progressed, a creative environment of trust, honesty, and openness was established. Promising ethical protection in the form of allowing any participant to withdraw or decline is mandated. At no time were false expectations for the participants or any misleading guidance promised during any specific study results. The researcher reiterated that all personal information will be stored and encrypted safely in his home, thereby preventing leaked data. When goals of the research are designed to provide major contributions to specific fields or to improve the understanding or process determining

the overall efficacy of their intervention; many times, these investigators may perceive desired outcomes of their studies to be exaggerated or more important than protecting the individual participants volunteering in the research. Overall IRB approval was provided by Walden University's Center for Research Quality providing approval number 03-17-21-0471977 thereby allowing the researcher to legally participate in active interviews and data. Upon receipt of their acceptance, a document was scanned with a wet signature from the volunteer, and it was required they email or fax it back immediately. Upon acceptance, they were notified that all data will remain in a secure location for 5 years following University guidelines protecting their full confidentiality. Lastly, all organizations were listed in the study as organization one, organization two, etc. Additionally, the same organization description will protect each participant by identifying them as participant one, participant two, etc. This practice will provide anonymity from the Army, Navy, and Air Force. This nomenclature will keep everyone safe and free from any self-identification when identifying participants in key roles and their major responsibilities. I ensured each participant was briefed that their privacy and their identities were not disclosed.

Data Collection Instruments

This section discussed how to collect and meticulously apply information gathered from the face-to-face, telephone, or Skype interviews reviewing research questions for military cloud computing. It was necessary to apply direct research questions as a primary data collection approach during the ongoing semistructured interviews. When objectives and research questions of a specific study determine whether

the scope is to gather purely interactional information or data, it informs us about participants' interactional behavior under the study or alternate contexts (Canals, 2017). For this doctoral study, I served as the primary data collection instrument while conducting a semistructured interview with Linkedin volunteers. According to Ainsworth (2020), the primary data collection tools at a researcher's disposal are interviews, focus groups, observations, documents or records, oral histories, questionnaires, and surveys. The focus will concentrate on gathering information through individuals completing a face-to-face, telephone, or Skype interview for military cloud computing, finalized and transcribed for review. The secondary data collection method was collecting data from multiple interviews, organizational documents such as infrastructure builds, and server farm layouts encompassing specific criteria required for the study to meet triangulation for data analysis.

Mitigating bias is different in each research project, although maintaining focus and asking deliberate questions can result in unequivocal responses, thereby minimizing bias. Similarly, by acting as the primary instrument, collecting data helped me learn more about the participants, facilitate better decision-making, and improve quality through issues resolved based on overall feedback. Using data collection instruments as a researcher is deemed reliable if the researcher can consistently produce identical results after repeatedly applying to the same subjects or groups (Bastos et al., 2014). Likewise, with previous methods, the specific number of observations necessary depends on the in-depth research questions and overarching approach used to gather that information

(Paradis et al., 2016). Through semistructured interviews, data gathering will be enforced by the researcher collecting qualitative primary data.

It is essential to understand the intent of each question asked. This way, the interviewees fully confirm whether the question was answered or should be pursued further (Proeschold-Bell, 2018). By identifying the commonalities of research, Dixon-Woods created a checklist of research questions to assess each question's clarity and appropriateness, the appropriateness and description for sampling, data analysis, and data collection, and levels of support in addition to evidence claims, and data coherence (Leung, 2015). The researcher ensured member checking was employed to verify that all participants could honestly verify the data's accuracy against their experiences. Member checking also included the changing of interpretations testing its validity using credibility and trustworthiness within a specified timeframe; similarly, the ethical concerns of returning data to its participant, the dilemma of assimilating and anticipating disconfirming voices, lastly, deciding who is ultimately held accountable for the overall interpretation (Birt et al., 2016). During the principal interview, semistructured interviews will ensure the interview protocol is on the right path. The researcher will guarantee that each participant in the study will entertain the same interview questions.

Performing research using validity entails what a particular instrument measures and how well it works. In contrast, reliability covers the faith that one must have in data obtained from instrument use and to what degree any measurement tool controls for errors (Mohajan, 2017). Aligning with validity and reliability, member checks enable researchers to transcribe information gathered, in addition to the population being

studied, ensuring appropriate representation of established credibility for each researcher, their culture, all while validating the study (Arora, 2017). All data gathered from the participants was aggregated, reviewed, and transcribed for follow-up interviews to ensure correctness and established goals were met. This member checking procedure was a technique compiling all data and allowing each volunteer to review their responses for correctness and approval from the participant. Final confirmation solidified all participant's results, thereby leading to data saturation. This member checking follow-up allowed the researcher to ask certain questions about specific points made, which stood out from each face-to-face, telephone, or Skype interview, allowing the participant to expand with any additional or specific meanings to their comments. Like data saturation, member checking was performed until no additional (valid) information could be shared. All findings were dispersed to the volunteer in the form of a transcript review allowing the volunteer to review data through a summary, providing them an opportunity to provide further data or reach data saturation. The interview protocol listed as Appendix B, describes the questions the researcher asked, and its pattern to ensure data consumption was reached.

Data Collection Techniques

This section will detail the data collection techniques used to collect the data representative for the research. The researcher incorporated face-to-face, telephone, or Skype interview questions during the initial data collection method, ensuring the semistructured method is reached. Before proceeding any further, interview questions were not shared with any participants until all cooperation letters were signed and

returned with their final declaration. When deploying data collection techniques, data based on several variables are often less robust, requiring the collection of additional variables in the future, and are subject to availability issues and data quality, requiring additional data preprocessing and cleaning (Shmueli et al., 2019). After receiving the consent forms, all research questions were finalized in preparation for email reminders. During the interviews, it was imperative to acknowledge that interviews were insightful and provided rich anecdotal evidence of how people honestly feel and act and provide persuasive direct quotes and insights from participants.

Initially, 10 to 12 participants were randomly chosen to complete telephone or Skype interviews. Overall, the study interviewed a maximum of 22 volunteers to round out the data gathering for a final tally. Each interview disc was initialed, signed, and placed in a 500lb capacity steel vault in the researcher's basement until each tape is destroyed. The researcher will be the only individual with access to this safekeeping of all participants' data responses safe and secure. The advantages of face-to-face, telephone, or Skype questions in qualitative research is the facilitator remains central to the dialogue and can quickly respond to any questions or concerns, thereby creating a comfortable and relaxing environment for unaccustomed participants (Nyumba et al., 2018). Another advantage of semistructured interviewing is that the questions are structured, adaptable, and flexible (Szolnoki & Hoffmann, 2013). As noted in Appendix C, all research questions covered each volunteer's observations and opinions about military cloud computing and data storage with third-party cloud computing vendors. For the study, it was key that the only data entered into the matrix is that of the participants,

and no one else's preventing bias. If data saturation is truly achieved, the volunteers will no longer expand on anything new to the subject after the initial completion of each face-to-face, telephone, or Skype interview reviewing research questions for military cloud computing.

Data Organization Techniques

The data organization approach planned to implement data included storing all emails and printed research questions completed by each volunteer in a secure vault, transferred data onto a DVD (encrypted), and any notes transcribed from emails passed amongst the researcher and participant. Each DVD will be stored in its own location within the safe, so there will be no possibility of confusion or mislabeling. After reviewing each research question response, a reference journal will be created to identify significant points the researcher may have overlooked or simply did not make enough comments during the initial review. During data organization, researchers investigating their research data management need to ensure best practices of research reporting ensuring the highest quality of their personal research outputs, which include both datasets and publications (Perrier et al., 2017).

Focus and attention must be obtained to evaluate each participant's responses to the research questions provided. This attention to detail ensured follow-ups with a detailed transcribed document capable of being reviewed and approved by all volunteers participating in the study to ensure data accuracy in addition to data saturation. Encrypted DVDs were created for all participants providing no cross-contamination impacting their results. In the end, all hardcopy notes, journals, and transcribed manuscripts were stored

in a private 500lb safe in the basement. This data will be stored for 5 years before being destroyed or deleted unless directed by the university to do otherwise. This information should provide the participant with a more satisfactory understanding of the security lockdown procedures and provide comfort, knowing this sensitive data is secure. As previously stated, all raw data will be secured for 5 years at a minimum and will be reiterated on multiple occasions to show the researcher is practicing up-to-date security practices.

Data Analysis Techniques

For this study, a qualitative single case study was implemented using semistructured interviews, increasing the likelihood of validity and triangulation. The researcher used methodology by explaining the methodological approach, describing the collection methods, describing the methods of analysis, and finally evaluating and justifying all methodological choices. The researcher's in-depth studies were rigorous because of the specific time required to review and consolidate each phase of data tables, becoming shorter as each user produces more condensed and precise presentations of this data (Watkins, 2017). A methodological study analyzes or describes methods (conduct, reporting or analysis, and design) whether in a published or unpublished methodological study (Mbuagbaw et al., 2020). The use of methodological triangulation facilitates the validation of researcher data through verification from one or more sources, thereby testing the consistency of findings gathered from different instruments, increasing the opportunities to control some threats or cause influencing these results (Green, 2018). Similarly, methodological triangulation uses a minimum of 2 various collection methods

to analyze phenomena comparable to each other. It is easier to identify methodological triangulation if an issue arises; there is strength in additional research to help work through that flaw or weakness, causing questions. The researcher also plans to use information that methodological studies deem useful to editors, publishers, students, etc. Like any catalogued empirical studies used in the past for review or reach-back. Additionally, to assist in the analysis of enhancement and its interpretation of findings, member checking helped the researcher create an established tenet of credibility within trustworthiness. Implementing data analysis demands attention to compiling data's ethical concerns in domains using human-subject data (Carpenter, 2017).

Data saturation was employed in this study to solidify the researcher's findings. Data saturation is described as the overall quality and quantity of data or information gathered from a study. Data saturation was achieved when the volunteers could no longer provide new data, causing the collection of information to cease. Collecting invaluable data from individual participants allowed the opportunity to review transcribed notes from each volunteer's research questions to return to the engineers and architects in time to verify and solidify their final responses guaranteeing data saturation. Data saturation is also sought to enrich the researcher's study by gathering the crucial data ensuring rigor in the process. In context to the interview questions, each participant was engaged and asked additional questions accumulated from the face-to-face, telephone, and Skype review to exploit data saturation to its fullest. After all the interviews were completed, the researcher reviewed and analyzed the data ensuring each participant answered each question in totality. Furthermore, the researcher used multiple strategies for data

accumulation, focusing on well-pronounced, specific outlooks covering the phenomenon, including interviews, journaling from detailed research procedures, and perceptions. Data saturation cannot be successfully achieved unless all practical information is emanated from the volunteer to the researcher.

One method utilized by the researcher was the triangulation method allowing organizational documents, telephone discussions, and each interview focusing on the document analysis from each report created. After the researcher collected their data, all information was transcribed from audio recordings to written notes gathered during the face-to-face interviews. This is one reason the choice to select NVivo was quickly decided. One of the most important capabilities NVivo can offer the ability to import full audio recordings into a repository while partitioning them into separate audio excerpts, proving extremely vital. The benefit of using methodological triangulation in research offers any individual four options to choose from, allowing the researcher to make one final choice to test the validity throughout the merger of data from different sources. According to Carter et al. (2014), the four methodological triangulation choices are data source triangulation, investigator triangulation, theory triangulation, and methodological triangulation. Qualitative researchers need to consider what "quality" means within a study conducted using a specific research design because articulating how they approach quality is truly complicated by multiple qualitative research approaches (Roulston, 2018). Additionally, researchers differ in the emphasis placed on the workings of triangulation. However, some investigators see it as critical to creating corroborating evidence. In

contrast, others focus on the potential to provide numerous sightlines, including multiple contexts enriching the understanding of research questions (Salkind, 2010).

NVivo can support future projects based on its playback ability for audio/video files, organize unstructured data, import citations, or other bibliographic software for literature reviews. NVivo offered a computer-assisted tool used to analyze strong evidence-based suggestions. Ultimately, implementing NVivo provided a pragmatic and robust way to manage the multiple complexities and nebulous reality of leading qualitative evidence synthesis (Houghton et al., 2017). NVivo offered many options to assist and minimize outside distractions with the use of the following practices: all notes or random tidbits are stored in one location, NVivo provided an organized, structured analysis approach, allowing the researcher to work with various types of qualitative data, NVivo makes sub-grouping of its analysis easier, and NVivo assists the researcher to be more efficient. Lastly, NVivo has an auto coding capability, which functions, making it completely manageable while coding the data itself. It is these basic practices the researcher used and molded to support their study and overall findings.

The researcher used each volunteer as one of the sources to implement data triangulation. Secondly, triangulation can lead to meta-interpretations and the complexity of a human's behavior that's studied from numerous standpoints. Third, the researcher used methodological triangulation, which equates to the final tool implemented when all interview data, in its entirety, has been reached, which will provide an in-depth approach to the triangulation of approaches by combining various procedures. Data triangulation assists researchers by using multiple methods to collect data about the same topic

assuring its validity through multiple samples and methods. In research, data triangulation can potentially reveal that of a social phenomenon's convolution by providing a dynamic picture amongst in-depth interviews along with a slower interview approach enhances data quality (Jentoft & Olsen, 2017). Noble and Heale (2019) delved into triangulation by simply combining theories, methods, and observances in research, which can assist with the fundamental biases resulting from the use of single observances or methods are overcome.

Triangulation can use the combination of one or more methods to achieve a result and be used to emphasize and determine the researcher's completeness of data. The data triangulation method focuses on overcoming issues with validity or biases during each stage of valid research promises and processes to help approach identified intricacies by combining multiple perspectives. The researcher uses methodological triangulation to achieve at least one of the 3 frequently rationales sought. The first rationale is completeness, which identifies each research method comes with inherent flaws, the second rationale is contingency, driven by insights of how/why strategies are chosen; lastly, the final rationale is confirmation improves the capability of its researcher's to finalize conclusions from their studies resulting in more robust and generalizable findings (Jack & Raturi, 2006). In research, each researcher will learn that all methods have their strengths and weaknesses. When employing methodological triangulation, the idea is that convergence of several methods entering a single conclusion firmly supports that conclusion rather than one of the methods finally arriving at a conclusion (Heesen et al., 2016). However, through the combination of multiple theories, data, and methods,

investigators, learned that individual strengths from each component should be capitalized upon (Schwarzenegger, 2017).

Reliability and Validity

When conducting qualitative research in search of reliability and validity, human emotions and their perspectives from both researchers and subjects are, at times, considered objectionable biases confounding outcomes in research; it is these same elements that are considered inevitable and essential, if not treasurable, as they invariably enhance colors and dimensions to enrich the number of findings (Leung, 2015). When using a single case study, the employment of data triangulation with intentions to present similar conclusions increases the study's overall validity. Building upon a structured and well-defined qualitative project requires meticulous attention to detail. Two aspects make the difference between poor research to ensure that fellow researchers accept their findings as trustworthy and credible. Reliability within a qualitative project seeks reliability, meaning it will help understand a clear situation that would otherwise be confusing. The validity, in some scholar's viewpoints, does not make sense concerning itself with the "truth" or "falsity" of observations concerning external reality, which seems to be a major concern of validity (Trochim, 2020).

Dependability

Dependability in qualitative research is important to overall trustworthiness since it establishes the researcher's findings as repeatable and consistent. In research, dependability helps promote valid proof that this research's conclusions can be repeated for clarity purposes (Amankwaa, 2016). The researcher ensured dependability by

following the member checking protocol during the review or summary of the findings finalizing honest and accurate results. Likewise, dependability is an important asset to trustworthiness since it establishes the research findings as truly consistent and repeatable. Researchers want to ensure that if they are verified by other scholars reviewing their data. In research, dependability denotes the reliability and consistency of their findings. The degree to their research procedures is documented, permitting outside researchers to follow, critique, and audit the entire research process itself (Moon et al., 2016). It is proper to maintain some sort of audit trail or data compilation, or the dependability may not be assessed. Its trustworthiness and dependability of their study could be diminished. For scholars to review a qualitative study's dependability, a researcher looks to verify if the study's owner was careless or made simple mistakes in collecting data, conceptualizing the study, interpreting their findings, and finally reporting results (Williams, 2011).

Credibility

In research, credibility is the number one criteria or aspect which must be established and is normally seen as the premier aspect a researcher uses to establish trustworthiness. Triangulation, in addition to member checking, helps fully establish credibility and contributes to trustworthiness. Synthesized member checking can help introduce the co-constructed approach of knowledge by allowing participants an opportunity to engage and contribute to the interview and interpret information months after their semistructured interview (Birt et al., 2016). Credibility can demonstrate the overall truth of research findings, especially when triangulation is concerned. That is

triangulation results in more factual findings than one individual approach. Credibility in research can be defined as the confidence placed within the truth of that researcher's findings and establishes whether the findings represent plausible data drawn from the researcher's original data and correct interpretations of the participant's original views (Korstjens and Moser, 2017). A researcher is seeking the value of quality over quantity in this research approach. Quality is sought because the readers or participants can only reasonably judge the results' finality or credibility. Researchers use credibility as a spare for internal validity. They are deeply rooted in the value of truth, asking if the researcher articulated or developed certain confidence levels with their findings focused on the phenomenon investigated (Lemon & Hayes, 2020).

Transferability

Although purposive sampling is the better sample match for the research's aims and objectives, improving the studies rigor and its trustworthiness of the overall data and results (Campbell et al., 2020). The researcher ensured transferability by describing the detailed research methodology, purposive sampling, and research context (Muthathi et al., 2017). The researcher will consider the sample subjects' characteristics, which are immediately related to each research question. Transferability is established, providing readers significant evidence that the research and its findings cannot independently prove the study's findings and applicability. Transferability is also demonstrated through the practice of data collection. When a researcher implements transferability within their project, it is important to identify the principles and criteria for selecting specific candidates while detailing the participant's key characteristics so the final results'

transferability can be accessed. Transferability is critical to applied research because policy and leadership rely on data, recommendations, and conclusions from a small number of research projects; it is these projects which heavily rely upon the evidence through a range of contexts, which makes it different from the one where applications will be created (Moon et al., 2016). According to scholars, researchers must make a concerted effort to which they cannot definitely prove that their outcomes based solely on the interpretation of data are transferable. However, they can establish a strong likelihood. The participant's details were recorded using data collection and accurately documented for research purposes to delineate the use of transferability.

Confirmability

Confirmability focuses on establishing the researcher's findings, and interpretations are definitively derived from data, requiring the researcher to demonstrate just how conclusions and their interpretations are reached (Nowell et al., 2017). Using qualitative research, participants' perceptions and actions are scrutinized for expressions of meaning internal to a given context, consistent with selected qualitative methodology practices the researchers interpret each participants' expressions through. Using triangulation, the researcher understands the phenomenon being studied and ensures the findings will be robust, comprehensive, rich, and well-developed. Additionally, member checking will support triangulation by allowing its participants to clarify their initial intentions, allowing errors to be corrected, and finally providing additional data if necessary. Auditability, which is commonly referenced as confirmability, is identified as orderly record keeping for every individual methodological choice; for example, a

detailed record of each source of information, decisions, sampling, and expository systems of their execution (Amankwaa, 2016; Cope, 2013). For a researcher to achieve confirmability, these researchers should demonstrate the results are clearly tied to conclusions by any means they can follow and replicate their process (Moon et al., 2016). Additionally, for researchers to achieve confirmability, they must take steps to validate their findings emerging from the information and not their predispositions. Researchers can make every effort possible to document their verifying procedures and double-check the entire research project's data. Throughout the interview question reviewing process, new data may tend to seem redundant if already collected; thus, during interviews, the researcher must focus on replicating data that he/she may begin to hear over and over (Saunders et al., 2017).

Transition and Summary

Section 2 identified the purpose statement and quickly delved into the researcher who acted as the prime research author. Additionally, the research method and its design concerning relation to the ethics of the research were discussed. Data saturation is already implemented into the projected interviews, and one focal point the researcher ensured was practiced, identified, and enforced in each research question. Data analysis and data collection were also covered, identifying the transition from transcribing manuscripts over the telephone, ensuring data saturation. The plan was to use NVivo to organize all organized data allowing me to specify each finding which aided significantly. Lastly, reliability and validity were covered in-depth, including member checking. In section 3, the researcher spoke to the overall study results and greatly delved into the findings.

Section 3: Application for Professional Practice and Implications for Social Change

This section contains derived information from the qualitative study with findings and their impact which can be useful to any follow-up professional practices or studies. I discuss the purposeful data gathered during my study with the intent to provide opportunities for social change while making recommendations for further professional studies. Finally, I provide solid recommendations for further studies in addition to the reflections of this study.

Overview of Study

The purpose of this qualitative single case study was to investigate strategies military leadership uses to implement third-party cloud computing for data storage. The invaluable data received originated during the semistructured interviews, telephone, and in-person interviews, and organizational documentation received from multiple volunteers for unclassified infrastructure environments. In this section, I summarized why I conducted this specific study and addressed investigational strategies the military incorporated to implement third-party cloud computing data storage.

Presentation of the Findings

The primary research question for this study was as follows: What strategies are senior IT military leadership using to implement third-party cloud computing for data storage? All findings are presented in this section, and the four conclusive themes are identified during the data collection. The population I used in this study was cloud administrators, engineers, and architects within a large Midwestern city with a minimum of 3 years of cloud computing knowledge and 5 years of total IT experience. I

successfully conducted 16 face-to-face and semistructured interviews, 2 telephone interviews, and four Skype interviews. Each interview was member-checked to ensure the transcription was accurate, thereby enhancing the process of methodological triangulation. In turn, methodological triangulation was employed to analyze data sources identified from semistructured interviews and organizational documentation analysis. The interviews were supplemented with purposive sampling. Members were not required to be on active duty or veteran's status to participate in the study. They did require DoD experience in one of the categories mentioned above. Four major themes arose from the invaluable information gathered from each participant. The themes were as follows:

1. Working relationships amongst AWS vendors and active duty or contractor personnel.
2. Strength of newly created security practices when both teams are combined.
3. All training/learning curves are considered with the new cloud data storage training.
4. Continuous safety and improvement of the overall infrastructure.

All four significant themes afforded opportunistic strategies for senior IT military leadership to implement third-party cloud storage. In support of these themes, all unclassified infrastructure documentation contributed to the overall security and hardening of the cloud installation and points of potential vulnerabilities the third-party vendors could recognize and mitigate immediately. Knowing and understanding the security mindset each third-party vendor brought to the table was valuable and refreshing.

Encompassing all internal military DISA regulations and requirements bundled with AWS GovCloud practices security strategies is a culture built for future success.

Theme 1: Working Relationships Amongst AWS Vendors and Active Duty or Contractor Personnel

Amongst the four themes identified, Theme 1, working relationships amongst AWS vendors and active duty or contractor personnel, was one of the most recognized occurrences within the 22 volunteers associated with this study. Both AWS and military teams include administrators, engineers, and their architects. Both teams, identified above, bring a constant to the current military infrastructure from a professional and technical perspective: cloud computing security and safety. Participants 11 and 19 injected their professional viewpoints as 2 of the strongest, secure environments within cloud computing are now only going to improve with overlapping practices and procedures implementing mitigatory prevention. In layman's terms, this current environment is a dynamic infrastructure security-wise, but it is more efficient with the support and addition of AWS security practices. According to the Undersecretary of Defense, Christopher Lowman, change is uncomfortable, but as previously mentioned, the team needs to get comfortable with being uncomfortable (as cited in Ferdinando, 2018). During the interviewing process, one of the main themes was the need for a one-team-one-fight mentality if this indoctrination was going to be taken seriously, ultimately leading to a full-fledged success. Participant 2 made it immensely clear that regardless of an individual's race, religion, or nationality, they were given a fair and equal chance to succeed, which is a positive approach for such a large corporation. This professional

practice simplifies this technician in making friends and creating those rapports because everyone is on the same team expecting successful results.

Each technical team negotiated an extremely rigorous letter of intent, bound to hold both military and AWS personnel accountable for their current, future, and even past actions leading up to this joint venture. During the interview, Participant 8 painted a clear picture that the technical trainers guaranteed everyone would learn at the same pace and were encouraged to ask questions for clarity or preparedness. It was agreed upon that members of both parties would limit all training, physical hands-on/on-the-job-training, any technical or vendor-specific communications amongst one another to the data center and training centers. This decision was made to ensure everyone did not get ahead of themselves when it came to training, which kept the team focused on the previously agreed guideline regimen, thereby strengthening the trust and new rapport between both parties. Outside of each zone, it was imperative that everyone signed a legally binding document forbidding outside discussion, possibly leading to leaked AWS practices. Likewise, participant 20 was not prepared for the course to be as seamless as it initially started. Participant 20 mentioned he had been in the military for many years and had always heard the team trainers say they would start slow. Until that point, it had never occurred until now, inspiring even the most hesitant of people enrolled.

These professional relationships between the AWS technical training team and the military-technical trainers must be patient, understanding, and mature when learning new technology and allowing rapports to grow in time. While learning how both the AWS engineering teams, military contractors, and service members planned to work together

was rather simplistic when reviewed. Initially, only the senior technical engineers and architects met before teaming was initiated. The standard for each setting was respect, open-minded communication, and future expectations. These goals allowed each team to pinpoint their concerns and understand how each entity planned to meet, adjust, and manipulate their training plan should it require amending to meet requirements for training purposes. Two hand-drawn infrastructure plans were created during interviews contributed by Participants 14 and 3. Both explained how impressed they were when the AWS GovCloud team took their expertise and quickly added it to their training regimen. Participants 14 and 3 promptly realized that the GovCloud team was there to provide a more suitable learning environment, explaining the physical and virtual approaches each team had planned to present and identify as a building block for engineers. Tripathy (2016) reported that every team is represented by various opinions, talents, ideas, and cultural backgrounds. However, there is a requirement that each individual accepts one another, recognizes one another's abilities, and works together mutually. I was not privy to the actual drawings but received a rather conclusive idea of how the current enterprise was functioning vice the changes being made for success.

The interviewing process revealed some very real and, at times, personal fears, and excitement about working with third-party vendors like AWS. One of the largest concerns was the expectation that each contractor or soldier did not want to feel as if they were slow in gathering the material presented to each team during training phases. There was also concern about a lag or a lack of understanding from a senior technical soldier, and how they should approach the AWS instructors and ask them to repeat a specific

training process without hindering the entire phase itself. The senior technical instructors explained that a water/bathroom break would occur every 90 minutes. These breaks would allow any military or novice AWS technician to speak freely to the technical instructors asking them to repeat a specific portion of the curriculum so they would understand and absorb it more freely. In other words, if team members were to stop the class and ask questions for clarity, the question in point could change the timeline of the schedule dependent on the instructor's explanation, etc. This would allow other teammates to start internal conversations while the question(s) were asked, thereby causing a significant distraction as a whole, detracting from the training altogether. Participant 15 admittedly acknowledged that she was born with a learning disorder and was always one of the last students or soldiers to finish her work as she grew up. To her surprise, she intently listened to every word each instructor had to say. In the end, she became great friends and colleagues with 2 of the technical trainers breaking the military and third-party bounds with hard work and respect.

At that time, it would prompt the instructors to slowly backtrack and teach that individual curriculum from a different perspective allowing a different viewpoint for those men/women who did not initially absorb the training the first time, thereby increasing cloud understanding and knowledge as a whole. Participant 6 shared that she was struggling with some of the technical jargon AWS taught to the group and challenged one of the instructors to approach the curriculum differently after returning from break. After that portion was completed, the class was asked if the second delivery

was more fluent and understandable than the first. Approximately 3 quarters of the class agreed it was easier to follow and more streamlined.

It is apparent that both technical teams (AWS and military) were seeking an initial change or approach to their training regimen, and both the AWS instructors and the military training team obliged. After a week of data aggregation and transcript creations, the interviewer specifically emailed all transcribed data to each participant requesting him/her to review it for continuity. At that time, I touched base with Participant 18 to verify and validate the face-to-face interview they shared. I was able to solidify member checking with Participant 18 by having her review the transcripts he emailed her and finalizing her comments. Member checking in this specific scenario substantiated the results for accuracy and completeness was an ultimate success. The participant felt the datum was surmised almost as fluid as she remembered explaining the scenario. Participant 5 added that combining practices exemplifies the best of the best. It prompts both parties to join teams, although disparate, to create a cloud computing infrastructure with the most stringent of security practices and expectations. Within TPB, an individual's expectations are the probability a particular behavior will result in a specific outcome like the AWS instructor. In this case, the professional asked the leading cadre member to renegotiate the training and approach it from a new angle with a fresh angle of attack helped tremendously. The anticipated outcome reinforced the necessity that working with, and alongside equal peers can result in positive encounters.

Table 1

Frequency of Theme 1, Vendor/Government Relationships

Source of data collection			D	
Sources of Data	**Valuable Comments**	**Teams Vested**	**Total Success**	**Growth and Stewardship**
Participants	**16**	**20**	**17**	**14**
Document	**7**	**11**	**20**	**19**

Note. Theme 1**, **Vendor/Government Relationships, d = data collected from.

NVivo's word aggregation for data analysis tracking and word recognition brought together some exciting keywords recognized as common or recurring. When the participants were asked to describe a bold, differentiating keyword that came to mind combining both AWS GovCloud and government professionals, 40 top descriptions came to the forefront almost immediately. Whether I was a novice, experienced, or senior member of one of the two teams actively participating, it was their position that descriptors like policies, success, training, and security came to mind. As the software continued to build the cloud (word) aggregator, I discovered the correlation between the descriptions and the theme. Each contributing word explained the factors of 2 dynamic teams working together to assemble, train, mold, and deploy competent technical cloud computing engineers and architects pursuing the next evolution of data storage via third-party vendors. Nearly 55% of the descriptive definitions were a one-to-one relation supporting the theme from the direct responses received. About 25% of the definitive meanings were linked to the theme but did not possess the ideal description the researcher felt was lucrative as the direct responses.

This particular theme aligned with current literature because of disparate technical teams migrating to incorporate cloud computing into a definitive infrastructure. For example, data have shown that working relationships amongst AWS vendors and active duty, or contractor personnel implementing security technologies that can enhance the businesses' infrastructure before cybercrime incidents occur (Tsakalidis et al., 2019). Comments like these from internal professionals reveal from from personal and professional experience that two disparate teams can successfully migrate while building a solid rapport with one another. These rapports build continuity and honesty through training and proven technical capabilities. I learned that senior military leadership had all participants write down in their own words what benefits and or hesitations each had of the upcoming training taught by senior technical experts. This documentation was shared during the interviews. Approximately 65 to 70% of the class felt the combination of both extremities (civilian sector and military) would not combine well but felt that they would succeed in the end. This information is represented in Table 1, Theme 1 of the study.

Additionally, this theme aligned with the current literature because of the personal and professional rapports built within each team's training. It is much easier to create a rapport with professional co-workers allowing everyone to understand their expectations, thereby making the learning process more open and accepted. That said, Tran et al., (2018) detailed that through friendship, employees should rely on their immediate leaders or supervisors for exchanges of technical skills associating a higher level of integrity and trust, obligation, respect, and support through encouragement. Like security or infrastructure safety, communication is just one of many items that assist both technical

team members and their students to effectively engage one another with respect, commonality, and professional courtesy. These approaches can assist in the strengthening of rapports from third-party vendors to the contractors and military personnel learning this new cloud computing technology.

This theme aligns well with TPB because daily behaviors and their expectations to succeed are called upon to drive the mission forward, validating Ajzen's TPB theory. For example, similar to the behavioral intention of the TPB theory, motivational factors dramatically influence any given behavior when a stronger intention expects to succeed. It is likely followed by the remainder of the group behaving the same to meet success. This positive outlook, although seemingly starting grim, supports one of TPB's six constructs for attitudes. In this scenario, attitudes refer to the degree to which an individual either poses a favorable or unfavorable behavior of interest in an endeavor. Strengthening personal and professional rapport in the workplace solidifies what the theme identified earlier. Likewise, as explained in the previous sentence, attitudes can impact an endeavor or a simple training routine accompanied by many, whether favorable or unfavorable. If the group's attitude is positive, the initiative will favor that committed relationship. If not, the working rapport could suffer because a few technicians do not feel the training or is going as planned, causing a toxic environment. Identified by Participant 3, attitudes reigned throughout the initial briefing leaving several of the group on the fence. Still, after multiple meetings and gatherings, the relationships started to click, and technical aspirations were achieved, providing excitement changing attitudes completely.

Another supporting behavior complementing theme 1 and its sources of data is that of social norms. At its simplest, social norms identify customary codes of specific behavior detected in groups or larger cultural contexts. Social norms classify as normative in distinct groups of people. The military personnel and AWS technicians were no different in their expectations besides the clothing and uniforms identifying their roles. Each participant interviewed had very deliberate and personal responses painting exact pictures of how they felt when the training started. It was these basic social norms that they adhered to since many of them mentioned they were speaking amongst their peers and trying to understand their approach and why they felt the training was going to be successful. This information firmly pointed to the perceived power expectation in TPB. Perceived power is the perceived presence or factor that facilitates or impedes the actual performance of a behavior. Meaning, perceived power points to an individual's perceived behavior over each factor. These attitudes and approaches towards the first theme specifically exemplify the strength of these technicians wanting to succeed and how their behavior positively impacted others. From the collection of this data, the findings show that both military and AWS technicians are pushing for success and technical expertise in the end. Although participants had mixed emotions, in the beginning, continued positive support followed by improved training for all personnel concluded in positive outcomes and overall success. These positive approaches can improve the overall success of the project if continuity and repetition are enforced.

Lastly, TPB is known as certain beliefs about the actual presence of factors facilitating or impeding the performance of that behavior. Multiple participants requested

to change their transcripts because they wanted to reword their initial entries and sound more robust in their explanations. The researcher was able to verify data triangulation by using face-to-face interviews and semistructured interview questions while approaching the participant in different contents, thereby breaking from the norm, and differing in sampling strategies.

Theme 2: Strength of Newly Created Security Practices When Both Teams Are Combined

It is not a secret nor a surprise that corporations and manufacturers alike implement and practice some active security in their daily mission planning. With that, every team within a small, medium, or large enterprise will always have fresh interns and senior members who have been with the company for years and years. Participants 1 and 4 commented explicitly on the attention to detail and the severe approach both the GovCloud and military security teams took to migrate these plans. Whether new to the team or not, each member has their viewpoint and approach to how they practice security and plan to shuffle and employ their new company's security expectations. According to participant 7, military contracted teams have solid and technically specific security practices developed for their expectations. Though proprietary, one can expect each company's expectations to be similar because they all expect 100% success with zero outages and deviations from the daily approach (if possible). Throughout the globe, in highly contested areas today, soldiers face realistic cybersecurity offensive operations; these security occurrences are used to intentionally disrupt, dismantle, or degrade the military's ability to accurately make effective security decisions at war which includes

the most impactful and everlasting deployment of cloud computing as a technical strategy (Puckett, 2020). Without applying controlled security practices in place, randomly running incoherent scans or mitigation processes is ineffective without a strategic plan to follow through after the process is complete.

Lackadaisical practices lead to failures in mission planning, thereby threatening the security and safety of each enterprise. Participants 19 and 22 were chosen to help migrate AWS GovCloud and military security procedures before technical trainers taking the helm. Due to the responsibility and expectations of many companies worldwide dealing with real-world technical scenarios, all guidelines and policies must be adhered to distinctly. In case of severe threats from malicious entities amongst and beyond the scope of corporations, the company could implement extreme measures like blocking firewall ports or shutting internet access down completely, including their network (Entrepreneur, 2020). With new cloud technologies, security is second-hand within their infrastructure using STIG hardening, DISA lockdowns.

Additionally, participant 9 quickly recognized the rapport and communication each team was displaying. Participant 9 advised the researcher that he had been on joint operations (Army and Air Force, Marines and Navy, etc.) and had not seen 2 disparate team's gel so quickly from a personal and professional standpoint. In addition, the strength of 2 separate entities, one military, and one commercial, will be able to consolidate 2 successful practices supporting cloud computing devices and their proprietary data storage approach.

Dudash (2016) asserted that 3 key ingredients or recommendations promoting the DoD's transformation to make the best of cloud computing are: implementing a new DoD private, secure cloud, standardize basic security categorizations, and implement a minor security risk commercial cloud solution. As advertised, security is inherent for this migration's success to meet the mission's requirements while continuing to fulfill DISA's recommendations. The researcher asked 3 high-ranking technical military leaders to create a brief infrastructure document or freehand drawing of how the current practice is working, considering its security practices prevent incoming attacks against external threats. All 3 participants, 1, 3, and 19, quickly drafted their nearly identical responses, which they described as unclassified, and transferred to AWS GovCloud experts.

Table 2

Frequency of Theme 2, Combined Security Practices for Migration

Source of data collection			**D**	
Sources of Data	**Migration of Security**	**Willingly Accept New Training Rigors**	**Acclimation Issues**	**Growth and Acceptance**
Participants	**16**	**20**	**17**	**14**
Document	**4**	**8**	**18**	**16**

Note. Theme 2, Combined Security Practices for Migration, d = data collected from.

Using NVivo assisted in answering specific questions learned from the participant's responses throughout the data collection process. In the end, about 80% of those common themes came to light after having these members review their transcripts for mistakes or potential updates to add to the study. Meaning, in the beginning, a substantial percentage of the participant pool agreed that AWS GovCloud and the

military (government personnel) could actively mingle amongst one another and combine to have an effective cloud computing dynamic every senior leader expected. Of those polled, approximately 59% of the interviewees agreed that security practices combining 2 disparate security programs could create a near-flawless secured environment. In other words, with the military's best practices and AWS GovCloud's commercial experience, there would be little to no reason this joint venture would not succeed unless some internal entities with malicious intentions promote failure. As the researcher progressed, an elevated response came to light which was not initially expected. 23% of the volunteers described some hesitancy towards the migration of both professional teams. As the interviews progressed, the researcher made every attempt to have these members expand on their decisions. The mere thought was military personnel and third-party vendors may not work together due to each other's expectations. Lastly, 8% felt they had a strong opinion towards a different response but would instead be represented by a not applicable reply making every attempt to remain neutral towards the scenario.

This theme aligns with the current literature due to many databases throughout (Walden database, Google, etc.) offering many substantiating articles supporting this study. For example, according to Whitehead (2020), migrating organizations must determine their testing level based on best security practices ensuring that these tools, processes, and practices are up to standard; ideally, the essential security tests should incorporate vulnerability assessments, penetration tests, and random cyber-hardening tests ensuring the migration meets all party's needs. Combining 2 disparate practices can be successful, but leadership must ensure that they do not lose sight of the combination of

approaches melding into one, causing a temporary, weak point in the infrastructure. Therefore, both AWS GovCloud and the military communications squadrons must make every effort to avoid cloud sprawl. In the most accessible terms, cloud sprawl identifies when an individual or group of cloud engineers combine cloud practices but mistakenly leave out important practices like substantial documentation, insecure or non-compliant procedures, or worse. Another viewpoint that proves this theme aligns with the current literature is the empirical research found amongst researchers describing their methods, data and sampling strategies, and overall data analysis results. With the identification of literature reviews discussing previous studies or methodologies recreating their research process via analytical tools, the information continues to aggregate for future researchers seeking similar topics.

A second reason this theme truly aligns with the current literature comes from a real-world scenario that occurred during the technical training course given by AWS GovCloud and the military team. A military team member used to work for AWS as a cloud technician before joining the military. It was noticed during the initial training that several security anomalies and started to check backlogs immediately. Out of the employee's scope of responsibility, it was identified that the system used for their production environment had been hacked. Upon recognizing this drastic issue, the military member used previous AWS cloud computing knowledge to initiate, navigate, and ultimately mitigate the issue by the close of business. This issue unknown to the military would shut down firewall ports and temporarily disable the DMZ for short periods causing real-world hardware and virtual machines to display vulnerabilities only

senior AWS technicians knew about. This senior engineer recognized and reacted to the vulnerabilities providing secondary and tertiary firewall corrections to combat any failures should they arise.

Spillages within military confines can impact data storage and increase real-world knowledge accessed by third-world threats. Also, to keep true to the non-disclosure agreement (NDA) document he signed while leaving AWS, he ensured he had others' help but did not give them direct guidance about correcting the issue. If he had, that would have ignited a significant security violation and actual breaking of the NDA. Afterward, he advised he was recognized by both parties and was given a bonus by the military, which provides monetary payments to any soldier, which helps saves lives, data, or infrastructure, thereby avoiding future flare-ups. Although rare, this participant saved the technical teams an unimaginable amount of money due to legacy software practice still in place and working within the military's production environment kept showing signs of degraded use and intermittent failure. Secure cloud computing organizations failing to address their security challenges or shortfalls show by 2020, one-third of all successful attacks against enterprise systems will be initiated through shadow IT resources (Nissim et al., 2019).

This specific theme aligns with TPB because the subjective norm is an individual's perception of a particular behavior merely influenced by a peer's, spouse's, or teacher's judgment. In turn, TPB strongly supports this reaction and the participants' overall outlook to ultimately change their minds to meld with the remainder of the group. In its most accessible form, subject norms are a person's belief about whether their peers

and those of importance concerning the person feel he/she should engage in a specific behavior (LaMorte, 2019). Subjective norms are the expectation or otherwise subjective probability that an individual and/or group can approve or disapprove of the actual behavior under consideration. Military instruction is disciplined, directive, and controlled and should provide for an easier learning curve and overall, technically capable session if most of the participants provided AWS with an opportunity to deliver their knowledge, thereby increasing expertise and hands-on knowledge. AWS is a globally recognized cloud computing expert known for its technical expertise, knowledge, and capabilities. AWS' technical capabilities are known since AWS was awarded the first 600-million-dollar contract to a military organization striving to compete in the GovCloud industry.

Although unclassified, it was still a controlled document that every participant commented on. In their opinions and approach made the researcher's data more significant and realistic. In today's society, perhaps the most considerable resistance to adopting the cloud in IT centers concerns legal issues and data security; fortunately, many providers like Amazon and Google have made long-term commitments to create best practices in addition to securing customer data and overall privacy (Kuo, 2011). About TPB, several military technicians did not want to feel they were headed for a successful endeavor but continued the path due to their loyalty to the team and the overall mission. This behavior is what TPB refers to as perceived behavior control. PBC is best identified as an individual's conceptualized behavior, decision, or conscious plan to exert effort, therefore purposely engaging in a particular behavior (Conner, 2001). It is not rare

for technical professionals to not see the entire picture or fathom an outcome that is favorable, so immediate doubt is cast, causing unhealthy approaches to modern practice.

These responses explained an ideal training scenario where both disparate entities came in prepared but unexpected of one another's approach to the general practice and push from senior military leadership. After months of studying and learning the technical portions of the alternate teams AWS training, the security and migration transformed into an infrastructure capable of maintaining the AWS GovCloud as a whole. Through the assistance of purposive sampling, notice the availability and importance and overall willingness to volunteer, in addition to their ability to communicate opinions and experience in an articulate, reflective, and expressive manner (Palinkas et al., 2016). This approach provides viewpoints from 2 technical entities meeting one another in an unknown environment without prejudice or hesitation. These findings confirm the data analysis results leading to a successful security migration for all involved.

Theme 3: All Training/Learning Curves Are Considered With the New Cloud Data Storage Training

Whether employing 40 members or 400,000 employees, training in any corporation is responsible for learning about the company's culture, expectations, safety, sexual harassment policies, etc. Failure to train and adequately discipline any new employee can lead to violations, data inconsistencies, security violations, and so on. Participant 7 spoke of the training they experienced while transitioning from military engineering responsibilities to new AWS expectations, which was a giant leap from her declaration. It was made clear that both the military and AWS GovCloud took the time

and effort to commit a program that allowed both parties to engulf themselves in each other's training playbooks, thereby allowing a different set of professional eyes to review and determine where the program would go from this point. At this juncture, a training plan was implemented and dispersed to all technical supervisors and SMEs for their review before ensuring each training member had their copy. The review of these plans allowed several iterations of changes and necessary updates, proving that both parties were well vested in their upcoming venture and expected nothing short of success in the end. Investing in total team building is one of the most deliberate and effective ways a company can promote communication, trust, innovation, and unity while introducing strong teamwork, contributing to morale, productivity, and efficiency (Hall, 2019). This theme was well represented for the third theme of this study, but it narrowly beat 2 others themes out of position, which was equally solid and informational for the outcome.

Participant 21 specifically spoke to the hours of in-depth time and patience it took for all military and GovCloud technical supervisors and trainers to come together; thus, ensuring that all academia covered in this newfound practice but technical, explanatory, inclusive, structured, and most importantly, met all security guidelines and regulations. Upon completion of the training curriculum, the most junior members of each team (military and GovCloud) were separated from their peers and trained by a member of each party. They were given seven days apiece since there were zero distractions and nothing but time and effort remaining. Within those seven days, 2 different members arose from the guided curriculum as basic SMEs in the arena of cloud computing storage.

This practice and opportunity proved that the documentation was valid and would suffice for this million-dollar deployment plan soon to occur.

Having spoken to 22 other professionals in all aspects of their technical careers, it was a vital moment when the researcher learned that an extremely high rate of the participants candidly admitted that this training was the most conventional and up-to-date guidance they had received to date. These accolades proved to be a massive compliment for both teams considering they are coming into this program with no experience or knowledge of one another's past, experience, or ability to migrate with other members that are not military or AWS GovCloud employees. Participants 9, 14, and 18 said they genuinely believe combining both novice teams will allow them to feed off one-off one another, leading to a solid youth expectancy. Within a few short months, the infrastructure underwent a transformation that is still one of the most successful cloud projects the DoD has granted since the military started bidding on third-party cloud computing contracts.

It is not unknown that the military and its 5 branches train their personnel worldwide in preparation for any unexpected threat that may cause harm or damage to the United States of America. Similarly, global corporations like Google, Microsoft, and Amazon are some of the world's first cloud computing corporations to break into military cloud usage. These military contracts did not simply fall into the laps of these corporations. Each entity’s contracting office worked tirelessly to bid like all remaining businesses and were the successful choices. Now, 2 disparate entities are gathering to build an elite team of cloud computing specialists worthy of working on a military

installation with men and women in uniform protecting the information vital to our national security. This data storage practice will be the first deployed by a third-party vendor and a steppingstone for the military and internal practices. Many hurdles must be overcome before a training regimen, and ultimately a learning curve can be devised for the men and women attending and learning from this top-tier training. Once the security posture has been decided, then the curriculum will be introduced to the class and reviewed in its entirety before moving forward. Interestingly, each interview participant had an incredible amount of information to offer for this effort. It was essential data for the researcher to receive. Participant 5 has been a part of the Air Force for nine years and participant 14 has been around 7.5 years. The researcher asked if they were provided documentation and he stated that they had which was the overall guideline to the six-month training course.

Participants 5 and 14 were 2 mid-level technicians with aspirations of success but were also not going to believe everything AWS GovCloud trainers were providing without proof and confirmation. This identifier explains how participant 22 felt when he completed his first week of AWS cloud training. He made it a point to identify that he has been in the military for almost seven years and believes this to be the most exact guideline he's ever used. According to his view, he felt the training was going to start with an injected form of motivation and slowly fade into a slower approach. To his dismay, the training stayed focused and compliant with the guidelines as everyone learned from the delivery. Lastly, participant 8 felt that his attitude is in the middle of the

road helped to sway his since he was open to change if the approach was true and called for a positive result.

Table 3

Frequency of Theme 3, Training and Learning Curves using Cloud Data Storage

Source of data collection			**D**	
Sources of Curriculum	**Potential Security Issues**	**Bad Habits Terminated Immediately**	**Open-Minded Learning**	**Abide by all Guides or Deviations**
Participants	**17**	**21**	**16**	**20**
Document	**3**	**17**	**11**	**15**

Note. Theme 3, *Training and Learning Curves using Cloud Data Storage, d = data collected from.*

For this group of data statistics gathering, all 22 participants were broken down by their cloud computing experience in addition to their overall IT experience. That said, 3 groups were devised consisting of novice, experienced, and senior technicians. Additionally, four questions were combined into one overall group for this exact scenario referred to as categories. Category 1 was how do you feel the training/learning curve will begin when mistakenly creating security issues? Category 2 asked, how is AWS GovCloud training supposed to alleviate bad habits during training? Category 3, where and when will the group finally fall into their characters, thereby becoming open-minded for learning? Lastly, in category 4, will the entire group adhere to the curriculum guides or deviations of any kind? As expected, the researcher thought all 3 groups would rate reasonably similar in their initial starting thoughts, and they did not disappoint. First, the novice group placed them the highest, leaving the gate. In an unexpected twist, both novice and experienced technicians showed higher levels of success at the onslaught of

training than everyone else. It seems the groups had faith in the novice teams and did not expect any issues (minor/major) to arise in the security realm. Second, when asked how these administrators would face bad habits or practices, the senior experts made it abundantly clear that everyone was learning at the same pace. No one had the opportunity to veer from the curriculum, causing threats. Third, is open-minded learning easy? Learning is only as complex as the individual partaking in the course makes it. Fourth, will the team be able to abide by all curriculum deviations? Most of the group felt that all teams would have become proficient in the teaching approach in six months and abide by what is taught.

This theme aligns with the current literature because learning curves should be recognized and taught to meet the expectations of the class and its students. According to Loerch (2016), through training and experience, organizations and their individuals can learn to perform tasks efficiently, reducing the total time required to output a unit comparable; thus, this intuitive and straightforward idea is expressed mathematically through learning curves. Secondly, this is why AWS technicians and the military trainers both decided to separate a small group for individual training to ensure the curriculum was efficient and understandable. The simple fact that they were novices in the career field of cloud computing made the documentation more credible. These novices only spent seven days dedicated to their technical instruction before taking an initial test to display their understanding and advancement. All junior team members passed, which was an incredible sign of sufficient training and reusable instructions for anyone to use and learn from.

Due to these responses, this theme aligns with the current literature considering multiple participants explicitly described the time both entities (AWS GovCloud and military) took to abide by objective timeframes allowing each individual the opportunity to learn at their own pace. According to Hirschmann (1994), learning curves in a place of business-like IT or other technically evolved professions require additional improvements always possible over time and is encouraged. The engineers interviewed were highly pleased and impressed with the level of satisfaction, competency, and status of technical ability is provided in such a short accumulation of data from both teams. In this case, methodological triangulation was met by observing the participant's behavior during the interview and writing down the body language and key signs given to the researcher. The researcher remembered the responses and paraphrased a couple of questions he felt were strongly responded to while reviewing the transcript and commented on any deviations he experienced from the first conversation to the second. Surprisingly, several parties were very stoic and were happy with the transcribed results.

This theme speaks to both parties' ability to learn to adhere to and successfully adapt to the learning curve brought into the infrastructure for all to follow. This adherence to training guidelines proved to be a success. It allowed one of the first major cloud computing migrations within the United States a success for AWS GovCloud and the military.

In TPB, behavioral beliefs or belief strength can play a vital role in individuals' daily demeanor or expectations of carrying out their day. Both architects and engineers from the military and GovCloud technical teams initiated this concept through long hours

of planning, positive expectations, and hopeful fruition in the end. The stronger one's belief in behavioral beliefs, the greater this perceived probability the behavior produces any given outcomes. According to Ajzen (2011), the more favorable the outcome, the stronger the behavioral impact of the belief for the attitude. In this specific example, both teams intentionally set out to accomplish a goal that they knew would be followed with open hearts and minds should the curriculum and training satisfactorily meet the expectations and technical rigor each SME was capable of implementing. In turn, after multiple reviews of the training, both parties broke into 2 different groups aligned with training guides and high expectations.

With the implementation of TPB, TRA explains customer's behavioral intentions by assuming each intention is the single most reliable and essential predictor; thus, all humans should be rational while making systematic choices (Paul et al., 2016). Using this approach, the participants must entrust their AWS GovCloud technical instructors and understand that their chosen approach has to be the most effective and beneficial considering the hundreds of millions of dollars AWS spends each year in cloud computing transformation and courses alone. TPB also teaches us that the attitude construct plays an immediate antecedent predicting an individual's intention to participate in particular behaviors (Redda, 2019). Similarly, TPB teaches us that the more positive an individual's attitude is towards a theme, the stronger the participant's perceptual behavior will become. This explanation speaks volumes both the AWS GovCloud team and the military infrastructure team with civilians and contractors that 2 disparate beliefs and practices can solidify when combined, turning a training environment into an acceptable

learning atmosphere. This atmosphere successfully met all operations learning curves while adhering to a strict yet sustainable schedule to appease the attendees and senior leadership's goals.

The researcher asked for a copy of the training guide, which was quickly delivered, and it became obvious that this was not an ordinary training approach to learn cloud computing first-hand. The researcher has never seen a detailed, exact document and simplistic to follow for all trainees. Each day was broken into variations of cloud computing history, actual hands-on learning, and quizzes to ensure all in attendance were learning and complying with the ongoing schedule AWS GovCloud had created. TPB teaches us that reflecting favorable or unfavorable feelings concerning particular behavior is just as important a determinant influencing their intention to use (Yang et al., 2017). The positive result is what TPB portrays in this research. This research confirms that the AWS GovCloud training met the learning curves and manipulated the structured teaching to comply with everyone's approval promoting success in the classroom.

Theme 4: Continuous Safety and Improvement of the Overall Infrastructure

In today’s technological society, continuous safety, and improvement sound like the beginning of a mission statement fit for many IT companies and organizations alike. Safety is not a flexible practice that any company cannot enforce or ensure 150% is dedicated. Participant 1 spoke of the practices the military uses daily to ensure the safety and security of their soldiers and is surprised that AWS GovCloud safety is very similar. Safety is the #1 priority for most employers or considering the men and women of each corporation makes a successful business move ahead while meeting mission

requirements. Two, continuous improvement is another term that walks together with safety. If the business is not constantly striving for safer practices and improvements to the daily mission, then a simple scenario is being overlooked, which could hinder any well-oiled machine in the future. After the researcher completed his data gathering from every participant, the data transferring, data transcription, and storage began to follow. Participant 11 read his transcript, which was emailed to him within a two-week window, and made it clear that this was the quickest and most accurate transcript he's experienced in his four interviews with doctoral/Ph.D. candidates. Within a matter of seven to eight days, it was evident that the safety of the environment and those within it was a dominant decision and the want or sheer desire to continue improving upon what was already known as the fourth and most popular theme.

Purposive sampling allows the researcher to be more judgmental or subjective about their candidates since these men and women will be delivering the data required to satisfy and ultimately prove their study for the conclusion. It was learned that data transcription proved to be an invaluable tool because each participant read their transcripts and thought the accuracy was outstanding. The researcher advised them that the transcript was a verbatim transfer (exact) of the actual interview. It was a pleasure working with these professionals because they now know that any doctoral candidate from this point on is simply seeking great and valid information to prove or disprove their study is viable for future use. With that, participant 21 said Amazon and AWS also have their safety strategies plainly articulated and placed into existence for the safety and security of the company and its global infrastructure.

Table 4

Frequency of Theme 4, Safety and Improvement of the Overall Infrastructure

	Source of data collection		**D**	
Sources of Data	**Mission Safety**	**Safety is a Mindset Continuously Practiced**	**Infrastructural Safety Improvements**	**Employ Integrity at all times**
Participants	**22**	**19**	**18**	**21**

Note. Theme 4*, *Safety and Improvement of the Overall Infrastructure, d = data collected from.

The military has structured and conclusive safety barriers which range from the physical realm to the virtual world and beyond. Regardless of its focus, safety, overall security, and continuous improvement of internal infrastructures matter greatly. Organizations around the United States and beyond understand and acknowledge that safety and overall infrastructure support are not a process reached and then placed on the shelf for later review should something need to be changed or updated. Safety, like personal and professional growth, continues to occur and improve themselves as times change and mandated requirements arise, meeting every expectation. The volunteers had an excessive amount of information to pass along concerning this final viewpoint. From the initial interview, novice personnel felt that mission safety was paramount and should be considered a baseline for future goals and plans as far as total success was concerned. When it came to safety being a mindset for the team to focus on, the experienced professionals saw the reality of safety being a mindset throughout the group, thereby seeing minimal future improvements since it already plays a vital role in the daily structure. The group's views changed when asked if infrastructural hardening and safety

would play a critical role in training. It was viewed differently from the novice personnel vice the experts because novice admins felt there is always room for abundance. In contrast, the experts thought they needed to manipulate their current hardening procedures with AWS GovCloud practices injected for more substantial prevention. Lastly, integrity was agreed upon by 95% of the group, making it a landslide decision.

This theme aligns well with the current literature because the safety and security of an overall infrastructure are not merely occurring in one location. Still, multiple areas worldwide, ensuring employees, their assets, and all other items are safe and secure. In turn, the senior members of the engineering group specifically mentioned having served in the Middle East or elsewhere around the world on one or multiple tours. A handful of these participants described unsafe stories involving scenarios that could have resulted in life-threatening results without prior training and situational awareness. It is imperative to understand and inherit safe practices as all professionals grow personally and professionally while maintaining a strong attitude towards success. Varia (2013) explained the most feasible way to approach the practice and regulatory compliance with a safe and secure infrastructure is to emphasize the continuous updates, reviews, and improvements and adhere to the approach customers manage their information security in the AWS GovCloud. Continuous safety and improvement are a theme that everyone needs to abide by for security, well-being, and environmental safety all around.

This theme also aligns with the literature because safety and security of the overall production environment falls underneath the protection of the infrastructure thereby receiving all updates, security posture guides, etc. AWS GovCloud has their

internal practices as does the military. Referencing military safety concerning an infrastructure, both synthesis and inference have been achieved to formulate goals while focusing on the armed force information security system; this system will play a role in an increasingly important part in shaping the security of a newly introduced cloud computing environment which must be treated as a top safety and security priority (Stugocki & Walkowiak, 2021).

This particular theme aligns with TPB for multiple reasons. TPB's perceived behavior control is defined as an individual's subjective probability of an inhibiting factor or a given facilitating factor being present within the situation of interest (Ajzen, 2020). In layman's terms, Ajzen describes PBC as reflecting an individual's beliefs regarding the access of specific resources and the opportunities required to perform a behavior. After reviewing many of the participant's qualifications, many had one skill set or a fraction of another, which the researcher felt would have made the data less dynamic, and bias was not used or even considered because the researcher was fortunate enough to gather the optimum qualified candidates for the study. Like an individual's perspective, behavioral beliefs refer to the once perceived advantages and disadvantages of performing a specific behavior (Yuriev et al., 2020). These candidates are the ideal reason the researcher took such an in-depth review of all participants and examined them for their potential contributions to the study and the invaluable they were capable of providing the study.

Using TPB can tend to focus on the positive attitudes and outlooks quite often. That said, TPB describes attitudes as an individual's defined evaluation of said object and a defined belief creating a link between some attribute and that object leading to behavior

due to intention (Lai, 2017). The picture these participants were painting lacked structure and simply everyone for themselves etiquette, which is entirely unacceptable in today's fast-paced IT environments. Therefore, the researcher was pleased with the responses since they told a story with sincerity, truth, and emotion. TPB speaks to descriptive norms, which are people's actual perceptions of what others would do in any situation, regardless if it is socially sanctioned. These norms of TPB prove engineering teams from both sides can absorb and understand that 2 extremely junior co-workers could jump feet first into the fire with results short of nearly perfect. Meaning, other engineers and administrators can now look and say both Joe and Sarah were able to succeed, and they know the least about our programs, so there is no reason that we should not follow because they have already done so. Having chosen purposive sampling was a great choice and a benefit in that the selection process for identifying the participants was not easy. The researcher had approximately 60 people contact him through LinkedIn, email, and voicemails. This turnout was nowhere near expected, but it was quickly identified that every individual candidate was not fully qualified for the position.

In TPB, many items capable of supporting the study and the theory were advertised. Still, not all fit the rigor and increased expectations the researcher sought to confirm or extend his study in this subject (Lee, 2017). Safety is a practice that 10 organizations approach in 10 different ways. These various approaches do not mean their methods are not correct or even valuable. It simply shows that each major corporation has a team of engineers, architects, and senior leadership that congregate and decide the most important item in keeping the safety and security of their people and possessions.

Secondly, when employees knowingly understand that senior leadership is taking a finite approach to their safety, it is truly a motivational boost and understanding that they are in good hands. Like subjective norms, they are also important to a researcher because positive support from persons, individuals, or particular organizations with meaning becomes greater; thereby, their attitude improves (Peng et al., 2014). Safety and security of oneself and their family provide comfort, which may result in the employees working harder to show their appreciation. The researcher concluded that 94% of the attendees favored the overall approach that senior military leadership does, and success will prevail when combined security infrastructures and practices. This data gathering proves to the researcher that the data confirms the security of this practice is efficient and well-planned for the current and upcoming events.

Application to Professional Practice

The actual findings contributing to this study were the Military Breaking Boundaries Implementing Third-Party Cloud Computing Practices for Data Storage. The overall IT effect is if the military continues to implement legacy practices without considering safer alternatives, data storage could be compromised due to a lack of safety thresholds. Fortunately, senior military leaders have indulged in AWS GovCloud training allowing third-party vendors to visit military facilities with aspirations to educate and train novice, expert engineers and architects, providing them with the necessary capabilities to strengthen their infrastructures with current policies and practices. These vital cloud infrastructures help achieve tremendous economies of scale throughout the DoD while minimizing the multiple risks many would associate with cloud computing.

(Dudash, 2016). Researchers can potentially benefit from using these findings by delving into any up-to-date practices or procedures which would maximize the future use of GovCloud third-party data storage computing for all to practice. Next, the researcher's study controls enable senior military leadership to move forward without hesitation. Like TPB practices, as a general rule in research, the more favorable the volunteer's attitude and subjective norms are, the stronger their perceived control, the stronger the individual's intention to perform a behavior should be (Suh & Hsieh, 2016). This success proves that military installations and external third-party like AWS GovCloud can work in tandem to identify, create, and deploy a significant instance capable of improving IT infrastructure with the assistance of cloud computing practices. Favorable attitudes promote the want and desire to learn instead of devaluing the third-party practice because that entity is disparate from the military. This study will allow future military branches to look back at and understand the success both the Army and Air Force partook.

Implications for Social Change

Information acquired from this research could positively impact military units' social change by updating expected production and test environments with hardened DISA regulations AWS GovCloud currently employs. This current data kept in a secured data storage is vital to national security and the safety and security of men and women all over the globe currently defending their country. In the past few weeks, ransomware attacks have created havoc on public and privacy industries running into the hundreds of millions of dollars encompassing the past few years. Promoting a safe and secure infrastructure allows administrators, engineers, and architects alike to continue providing

mission-critical safety from a premiere cloud company like AWS GovCloud. Successfully controlling and securing this data is a significant venture and an opportunistic time for AWS to continue practicing its strategic safety mission for all to view. According to Seffers (2018), if a warfighter has a laptop or mobile device and an Internet connection, they can access their cloud services from anywhere in the world.

A secondary implication for social change is the heightened awareness of 2 disparate practices and procedures coming together to create one unified cloud computing service, which can be second to none from the viewpoints of senior military leadership. Lee (2017) states subjective norms that each individual is exposed to, or privy will have a true impact on their intentions in recognition of the man being, by his nature, a social creature, so they will no doubt care about the opinions of what others think, or in fact, believe. Senior military leadership will be privy to this study once it has been finalized and published. The researchers hope that at least one of these high-ranking leaders with movement potential will read, understand, and approach third-party cloud computing the same way each participant involved does. The military is a highly disciplined and directive society that believes in the practice that senior leadership, whether enlisted or officer, will lead by example, promoting the most successful and secure missions throughout each military sector. For the senior military leadership seeking change and improvements capable of securing and implementing cybersecurity and other additional practices, those figureheads leading the charge can now recognize and affiliate themselves with future projects from this success case. This senior military leadership will review, observe, and potentially contact the current military organization this AWS

GovCloud helped build and inquire about the responsibilities and other expectations they have doubts about. This social change can and will continue to make a remedied effort if those choosing to follow this path accept the learning curve and the opportunities this third-party vendor can provide in writing.

Recommendations for Action

In this scenario, the most highly recommended action is implementing third-party cloud computing with data storage on one military organization at a time. From this point forward, word of mouth provides fruitful for organizations like AWS GovCloud the opportunity to expand its various services to global organizations and military installations around the world. The subjective norms determined by an individual's normative beliefs determine whether important people like friends, teachers, or parents disapprove of their particular behavior and their specific appraisals of that behavior (Guerin & Toland, 2020). This success story will be one that AWS GovCloud uses to sway alternate parties to consider their product and will be able to show effective timelines, prices, training regimens, etc., for the senior military leadership to follow and adhere to quickly. This cloud computing data storage implementation is no longer an idea, and multiple parties can peak this success at different levels. Generals trust other men and women in their capacity. They can have serious conversations with them about their approval to move forward, which may be the reason alternate military installations may finally take the course of cloud computing as a whole. As this data storage practice continues to grow and the dangerous external hacking parties from third world countries continue to access and override our infrastructures, some corporations may need to

bypass their current roles in computer security and rely on more significant entities with a proven track record.

Senior military leadership will eventually recognize and absorb the success they have recently experimented with, and the knowledge and expertise through technical know-how these civilians, contractors, and military personnel acquired over time. Moreover, researchers found that people's subjective norms commonly turn towards specific groups for their judgments or standards towards a particular behavior (Sun et al., 2020). Senior military leadership must sit down with their senior technical engineers and architects within a specified period and have lessons learned briefing collected and created for base installation senior leadership (Generals/Flag Officers). This will allow everyone to understand how the project initiated was months or years ago and has grown into a safe, secure, and near-impenetrable infrastructure. Normative beliefs refer to an individual's beliefs that are accepted by specific people or groups and dictate whether behaving in a particular fashion is appropriate (Fang et al., 2017). Senior military leadership will eventually become curious and want to partake in the cloud computing data storage implementation if their organizations require it and can afford the time, security, and services of AWS GovCloud as a whole. Cloud computing combined with avid cybersecurity procedures and stringent DISA standards can make for one of the safest and hardened locations in IT.

One last item military commander’s can lean upon for future implementations besides the previous success factors is the knowledge that this AWS traveling team will already have a current security clearance required to undergo training on a military

installation. Without the proper security clearance, regardless of the rank of the senior military leader in charge, no efforts will be accomplished until these security requirements are in place and complete.

Recommendations for Further Study

The findings the researcher provided to support this study ultimately provide additional research in the ever-increasing practice of GovCloud and cloud computing as a whole. This in-depth qualitative study focused on the desire to expand data storage limitations implementing third-party vendors never previously attempted to date. The limitations within this study contributed to a lack of knowledge concerning cloud computing and the lack of understanding from negative publications spread across the Internet. Secondly, these negative experiences swayed senior military leadership to stray from this practice in their infrastructure. The researcher learned it would be more beneficial to interview participants external from the local military installation instead of interviewing active-duty personnel who are currently stationed here, potentially causing a job conflict due to their participation. Seeking volunteers online provided an opportunity not considered before. Although a tremendous amount of information was gathered, and the researcher is highly pleased, it is necessary that future cloud candidates expand their knowledge and overall reach from one of the military bases to 3 or 4 different bases within the city limits. This aggregation would paint a larger picture than one installation started with.

In future studies, the researcher can use the cloud computing studies, which are coming to fruition regularly thanks to the military allowing their communication

squadrons to delve into more up-to-date practices knowing the previous attempts proved successful and safe. As AWS GovCloud grows, their knowledge base of military installations and government entities, although disparate, is also increasing. It is information and trust in a global like AWS that users seek to support their cybersecurity teams through stringent security and DISA guidelines.

Reflections

The past six years have proven the most challenging within an academic environment I have ever experienced. Initially entering the program, I felt like a strong writer, but I quickly learned I had so much more to learn and understand to become the scholar/practitioner I strove to be. Unfortunately, I had to take a two-year hiatus due to life changes and a divorce I never planned for. I learned a lot of information during my first attendance at Walden, but the dual enrollment opened my eyes and kept me focused. I initially felt I would not be accepted into the program since I left at the beginning of my doctoral study. After speaking with Dr. Case and Dr. Duhainy, more so Dr. Duhainy, I knew I could return and make a solid showing to complete my study. I intentionally changed my purpose statement to make it more manageable, thereby providing more research to support my study. My conceptual framework was straightforward, but I also explained why I chose that specific framework. Finding a theory was also tricky, considering I tried to incorporate ideas I had but could not implement them on paper for one reason or another.

I felt the most time-consuming and challenging portion of the study was the overall proposal. I initially wrote the proposal in seven days and felt strong about my

initial draft. As I continued to add to it, I understood it required much more work than initially employed. I felt about 65% of the proposal was extraordinarily strong, but the last 35% shook me after countless corrections from my committee. At this time, I lost an immediate family member, and I had to reach deep and ask myself if this was something that I truly desired deep down in my soul. After several decisions to leave, Dr. Duhainy gave me a call and made me realize things that had not crossed my mind. His leadership and ability to recognize a student were struggling, and he made it right with his wisdom and patience.

Finally, I received my IRB approval and started interviewing, one of the most valuable interactions I have ever had. Learning from these IT professionals taught me their point of view and what makes them happy, in addition to what they felt would drive the program to success. In all, it has been a roller coaster ride that I would participate in again, but I would have to tighten my seatbelt a bit more for stability.

Summary and Study Conclusions

Attempting to solidify a study within the bounds of a military installation is difficult at the least. There are security requirements, background checks, and multiple other necessities a researcher must adhere to and gain before moving forward with another study of this nature. It was a pleasure to support and defend the use of cloud computing supporting government personnel using third-party data storage. It is a profession that continues to grow and is now on many military branches ' radar simply from the countless articles of branches seeking the most affordable and economical option for the infrastructure and its future. It would be helpful if future practitioners

delved into additional opportunities that men and women in uniform and those who previously served can utilize in their current production environment. With the assistance of a fierce cybersecurity plan and the ongoing AWS GovCloud practices, the sky is the absolute limit for those willing to put in the effort and time necessary. With the onslaught of cloud computing practices ever-growing, opportunities abound just waiting to be researched and defended. The researcher hopes to be able to look back at this study and overall practice in 10 years and recognize a dramatic shift in the viewpoint of senior military leadership and those men and women seeking to enforce this practical knowledge in the many years to come. Like those who have learned to become efficient and expert architects and engineers, cloud computing, not to mention AWS GovCloud practice, is merely a call away to prepare and endure a new technological opportunity offered to anyone interested.

References

Abdullah, S., & Abu Bakar, K. A. (2018). Security and privacy challenges in cloud computing. *2018 Cyber Resilience Conference (CRC)*. https://doi.org/10.1109/cr.2018.8626872.

Adhabi, E. A., & Anozie, C. B. (2017). Literature review for the type of interview in qualitative research. *International Journal of Education*, *9*(3), 86. https://doi.org/10.5296/ije.v9i3.11483.

Ahmadi, M., & Aslani, N. (2018). Capabilities and advantages of cloud computing in the implementation of Electronic Health Record. *Acta Informatica Medica*, *26*(1), 24. https://doi:10.5455/aim.2018.26.24-28.

Ainsworth, Q. (2020, June 1). *Data Collection Methods*. JotForm; JotForm Inc. https://www.jotform.com/data-collection-methods/.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-t.

Ajzen, I. (2006). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned Behavior1. *Journal of Applied Social Psychology*, *32*(4), 665-683. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x.

Ajzen, I. (2011). Behavioral Interventions Based on the Theory of Planned Behavior. In Umass.edu (pp. 1–5). Icek Ajzen. https://people.umass.edu/aizen/pdf/tpb.intervention.pdf.

Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health*, *26*(9), 1113-1127. https://doi:10.1080/08870446.2011.613995.

Ajzen, I. (2012). The Theory of Planned Behavior. *Handbook of Theories of Social Psychology: Volume 1*, *1*(1), 438–459. https://doi.org/10.4135/9781446249215.n22.

Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies*, 1-11. https://doi:10.1002/hbe2.195.

Alam, M. Z., Kousar, S., & Rehman, C. A. (2019). Role of entrepreneurial motivation on entrepreneurial intentions and behaviour: Theory of planned behaviour extension on engineering students in Pakistan. *Journal of Global Entrepreneurship Research*, *9*(1), 1-20. https://doi.org/10.1186/s40497-019-0175-1.

Alani, M. M. (2017). Prioritizing cloud security controls. *Proceedings of the Second International Conference on Advanced Wireless Information, Data, and Communication Technologies - AWICT 2017*. https://doi.org/10.1145/3231830.3231831.

Ali, K. E., Mazen, S. A., & Hassanein, E. (2018). A proposed hybrid model for adopting cloud computing in e-government. *Future Computing and Informatics Journal*, *3*(2), 286-295. https://doi.org/10.1016/j.fcij.2018.09.001.

Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *37*(1), 101419. https://doi.org/10.1016/j.giq.2019.101419.

Allen, M. (2017). *The sage encyclopedia of communication research methods* (Vols. 1-4). Thousand Oaks, CA: SAGE Publications, Inc. https:/doi: 10.4135/9781483381411.

Almalki, S. (2016). Integrating quantitative and qualitative data in mixed methods research—challenges and benefits. *Journal of Education and Learning*, *5*(3), 288. https://doi:10.5539/jel.v5n3p288.

Alzahrani, H. (2016). A Brief Survey of Cloud Computing A Brief Survey of Cloud Computing. In *Global Journal of Computer Science and Technology: B Cloud and Distributed* (pp. 10–16). Global Journals Inc. (USA). https://globaljournals.org/GJCST_Volume16/3-A-Brief-Survey-of-Cloud-Computing.pdf.

Amankwaa, L. (2016). Creating Protocols for Trustworthiness in Qualitative Research. *Journal of cultural diversity*, *23*(3), 121–127.

Amazon Web Services. (2020, January 1). *AWS GovCloud (US) - Amazon Web Services*. Amazon Web Services, Inc. https://aws.amazon.com/govcloud-us/?whats-new-ess.sort-by=item.additionalFields.postDateTime, &whats-new-ess.sort-order=desc.

Anand, A. (2017). Cloud Computing and Cloud Related Security Issues. *International Journal of Advanced Research in Computer Science*, *8*(5), 1881-1886. https://search-proquest-com.ezp.waldenulibrary.org/compscijour/docview/1912631341/F4C6C7BE842546B9PQ/5?accountid=14872.

Andoh-Arthur, J. (2019). Gatekeepers in Qualitative Research. In P. Atkinson, S. Delamont, A. Cernat, J.W. Sakshaug, & R.A. Williams (Eds.), *SAGE Research Methods Foundations*. https://doi:10.4135/9781526421036854377.

Arora, A. B. (2017). Member checks. *The International Encyclopedia of Communication Research Methods*, 1-3. https://doi:10.1002/9781118901731.iecrm0149.

Arce, D. G. (2020). Cybersecurity and platform competition in the cloud. *Computers & Security*, *93*, 101774. https://doi.org/10.1016/j.cose.2020.101774.

Army's cloud office set to fully operate by March. (n.d.). Www.Army.Mil. https://www.army.mil/article/231913/armys_cloud_office_set_to_fully_operate_bb_march.

Arpaci, I., Kilicer, K., & Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services. *Computers in Human Behavior*, *45*, 93-98. https://doi:10.1016/j.chb.2014.11.075.

Aryotejo, G., Kristiyanto, D. Y., & Mufadhol. (2018). Hybrid cloud: Bridging of private and public cloud computing. *Journal of Physics: Conference Series*, *1025*, 012091. https://doi:10.1088/1742-6596/1025/1/012091.

Aspers, P., & Corte, U. (2019). What is Qualitative in Qualitative Research. *Qualitative Sociology*, *42*(2), 139–160. https://doi.org/10.1007/s11133-019-9413-7.

Astri, L. Y. (2015). A study literature of critical success factors of cloud computing in organizations. *Procedia Computer Science*, *59*, 188-194. https://doi:10.1016/j.procs.2015.07.548.

Ataro, G. (2020). Methods, methodological challenges and lesson learned from phenomenological study about OSCE experience: Overview of paradigm-driven qualitative approach in medical education. *Annals of Medicine and Surgery*, *49*, 19-23. https://doi:10.1016/j.amsu.2019.11.013.

Attaran, M., & Woods, J. (2018). Cloud computing technology: Improving small business performance using the internet. *Journal of Small Business & Entrepreneurship*, *31*(6), 495-519. https://doi:10.1080/08276331.2018.1466850.

AWS. (2018, November 13). *Amazon Web Services launches second GovCloud region in the United States*. BusinessWire.com. https://www.businesswire.com/news/home/20181112005823/en/Amazon-Web-Services-Launches-GovCloud-Region-United.

Bacharach, S. B. (1989). Organizational theories: Some criteria for evaluation. *The Academy of Management Review*, *14*(4), 496. https://doi:10.2307/258555.

Bairagi, S., & Bang, A. (2015). Cloud computing: History, architecture, security issues. *International Journal of Advent Research in Computer and Electronics (IJARCE)*, 102-108. https://www.researchgate.net/publication/323967455_Cloud_Computing_History_ArchitArchit_Security_Issues.

Bangi, Y. I. (2018). Prevalence of Mixed Methods Research in Education Journals. *International Journal of Academic Research in Business and Social Sciences*, *8*(6). https://doi.org/10.6007/ijarbss/v8-i6/4182.

Bastos, J. L., Duquia, R. P., González-Chica, D. A., Martinez-Mesa, J. M., & Bonamigo, R. R. (2014). Field work I: Selecting the instrument for data collection. *Anais Brasileiros de Dermatologia*, *89*(6), 918-923. http://doi:10.1590/abd1806-4841.20143884.

Benson, V., & Filippaios, F. (2016). *ECRM2016-proceedings of the 15th European conference on research methodology for business management: ECRM2016*. London, United Kingdom: Academic Conferences and publishing limited.

Bhatia, S., & Malhotra, J. (2018). CSPCR: Cloud security, privacy and compliance readiness - A trustworthy framework. *International Journal of Electrical and Computer Engineering (IJECE)*, *8*(5), 3756. https://doi.org/10.11591/ijece.v8i5.pp3756-3766.

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking. *Qualitative Health Research*, *26*(13), 1802-1811. http://doi:10.1177/1049732316654870.

Bliss, L. A. (2016). Phenomenological research. *International Journal of Adult Vocational Education and Technology*, *7*(3), 14-26. http://doi:10.4018/ijavet.2016070102.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, *9*(2), 27-40. https://doi:10.3316/qrj0902027.

Brading, T. (2020, January 24). *Army's cloud office set to fully operate by march*. https://www.army.mil/article/231913/armys_cloud_office_set_to_fully_operate_by_march.

Bui, D.-M., Huynh-The, T., & Lee, S. (2016). Fuzzy Fault Detection in IaaS Cloud Computing. *Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication*. https://doi.org/10.1145/2857546.2857612.

Butler, B. (2016). 10 must-watch IaaS cloud trends for 2017. *Network World*. https://search-proquest-com.ezp.waldenulibrary.org/compscijour/docview/1850204693/abstract/651E45FC18EC4FDEPQ/23?accountid=14872.

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing*, *8*, 174498712092720. https://doi.org/10.1177/1744987120927206.

Canals, L. (2017). Instruments for gathering data. *Qualitative approaches to research on plurilingual education / Enfocaments Qualitatius per a La Recerca En Educació Plurilingüe / Enfoques Cualitativos Para La Investigación En Educación Plurilingüe*, 390–401. https://doi.org/10.14705/rpnet.2017.emmd2016.637.

Candela, A. (2019). Exploring the Function of Member Checking - ProQuest. (n.d.). Search.Proquest.com. https://search.proquest.com/openview/c43013ecc3381c2ba600e6e2bc76820c/1?pq-origsite=gscholar&cbl=55152.

Carpenter, T. (2017, April 11). *What constitutes peer review of a data set?* The Scholarly Kitchen. https://scholarlykitchen.sspnet.org/2017/04/11/what-constitutes-peer-review-research-data/.

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. (2014, September 1). The use of triangulation in qualitative research. *Oncology Nursing Society*, *41*(5), 545-547. https://doi:10.1188/14.ONF.545-547.

Carvalho, M., Menascé, D. A., & Brasileiro, F. (2017). Capacity planning for IaaS cloud providers offering multiple service classes. *Future Generation Computer Systems*, *77*, 97-111. https://doi.org/10.1016/j.future.2017.07.019.

Cheung, S., & Chan, D. (2000). *The Role of Perceived Behavioral Control in Predicting Human Behavior: A Meta-Analytic Review of Studies on the Theory of Planned Behavior* [Unpublished doctoral dissertation]. The Chinese University of Hong Kong.

Chawki, E. B., Ahmed, A., & Zakariae, T. (2018). IaaS cloud model security issues on behalf cloud provider and user security behaviors. *Procedia Computer Science*, *134*, 328-333. https://doi.org/10.1016/j.procs.2018.07.180.

Chen, T., Chuang, T., & Nakatani, K. (2016). The perceived business benefit of cloud computing: An exploratory study. *Journal of International Technology and Information Management*, *25*(4), 100–121. https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?

Chipidza, W., Green, G., & Riemenschneider, C. (2019). Why do students not major in MIS? An Application of the Theory of Planned Behavior. *ProQuest*, *30*(2), 111-

126. https://search-proquest-com.ezp.waldenulibrary.org/compscijour/docview/2238485976/8956FD04C70B4A1BPQ/2?accountid=14872.

Chou, S., & Hsu, M. (2015). Understanding online repurchase intention: Social exchange theory and shopping habit. *Information Systems and e-Business Management*, *14*(1), 19-45. https://doi:10.1007/s10257-015-0272-9.

Chuang, L., Chen, P., & Chen, Y. (2018). The determinant factors of travelers' choices for pro-environment behavioral intention-integration theory of planned behavior, unified theory of acceptance, and use of technology 2 and sustainability values. *Sustainability*, *10*(6), 1869. https://doi.org/10.3390/su10061869.

Cline, M. (2017). Five lessons from history. *Technology & Social Change*, *3*(11), 51-58. https://medium.com/capital-one-tech/technology-social-change-ff75e1eb1dee.

Coffey, A. (2018). *Http://doing Ethnography*. Thousand Oaks, CA: SAGE.

Cohen, K. (2021, May 13). Addressing cloud-sprawl: combining security best practices with business foundations. Cloud Tech, 31–33. https://cloudcomputing-news.net/news/2019/mar/13/addressing-cloud-sprawl-combining-security-best-practices-business-foundations/.

Cohesity. (2019, June 11). Cohesity Introduces Comprehensive Data Management Capabilities for AWS GovCloud. *Cohesity*. https://www.cohesity.com/press/cohesity-introduces-comprehensive-data-management-capabilities-for-aws-govcloud/.

Conner, M. (2001, April 2). Health Behaviors. ScienceDirect; Elsevier B.V. https://www.sciencedirect.com/science/article/pii/B0080430767038717?via%3Dihub.

Cope, D. G. (2013). Methods and meanings: Credibility and trustworthiness of qualitative research. Oncology Nursing Forum, 41(1), 89-91. https://doi:10.1188/14.onf.89-91.

Coss, D. L., & Dhillon, G. (2019). Cloud privacy objectives a value-based approach. *Information and Computer Security*, *27*(2), 189-220. https://doi.org/10.1108/ics-05-2017-0034.

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. *BMC Medical Research Methodology*, *11*(100).

Dash, S., & Pani, S. K. (2016). E-Governance paradigm using cloud infrastructure: Benefits and challenges. *Procedia Computer Science*, *85*, 843-855. https://doi:10.1016/j.procs.2016.05.274.

Deale, T. (2016). *The Department of Defense and the Power of Cloud Computing: Weighing acceptable cost versus acceptable risk* (52). Department of Research and Publications, U.S. Air Force. https://apps.dtic.mil/sti/pdfs/AD1015712.pdf.

Denny, W. A. (2019). *Senior military leadership in civil support operations: An exploratory study* (27539693) [Doctoral dissertation]. ProQuest Dissertations and Theses Global.

Department of Defense. (2019, December 19). Performance.org. https://www.performance.gov/defense/.

Di Giulio, C., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. H., & Bashir, M. N. (2017). Cloud security certifications. *Proceedings of the Second International Conference on Internet of Things, Data and Cloud Computing*. https://doi.org/10.1145/3018896.3025169.

Dudash, S. (2016). The Department of Defense and the Power of Cloud Computing: Weighing Acceptable Cost versus Acceptable Risk (Vol. 52, pp. 1–51). Air University Press. https://apps.dtic.mil/sti/pdfs/AD1015712.pdf.

Duff, S. (2019, November 21). How to build a winning strategy for backup and recovery on AWS GovCloud. *CloudRanger*. https://cloudranger.com/how-to-build-a-winning-strategy-for-backup-and-recovery-on-aws-govcloud/.

Dulik, M., & Dulik, M. J. (2015). *Security in Military Cloud Computing Applications. http://kit2015.aos.sk/proceedings/pdf/dulik.pdf*.

Why security is becoming more important to businesses. (2020, November 25). Entrepreneur Handbook. https://entrepreneurhandbook.co.uk/why-security-is-becoming-more-important-to-businesses/.

Fang, W., Ng, E., Wang, C., & Ming-Lin, H. (2017). Normative beliefs, attitudes, and social norms: People reduce waste as an index of social relationships when spending leisure time. *Sustainability*, *9*(10), 1696. https://doi:10.3390/su9101696.

Ferdinando, L. (2018, March 14). *DoD Officials Highlight Role of Cloud Infrastructure in Supporting Warfighters*. U.S. Department of Defense; Defense.gov. https://www.defense.gov/Explore/News/Article/Article/1466699/dod-officials-highlight-role-of-cloud-infrastructure-in-supporting-warfighters/.

Ferratt, T., Prasad, J., & Dunne, E. J. (2018). Fast and slow processes underlying theories of information technology use. *Journal of the Association for Information Systems*, *19*(1), 1-22. https://doi:10.17705/1jais.00482.

Fishbein, M., & Ajzen, I. (2011). *Predicting and changing behavior: The reasoned action approach*. Taylor & Francis US.

Gaber, J., & Gaber, S. (2018). *Qualitative analysis for planning & policy: Beyond the numbers* (2nd ed.). New York, NY: Routledge.

Ghiaţâu, R. M., Mâţă, L., Poenaru, A. G., & Boghian, I. (2019). Factors influencing higher education teachers' attitudes towards unethical use of information technology: A review. *Revista Romaneasca pentru Educatie Multidimensionala*, *11*(1), 287. https://doi.org/10.18662/rrem/111.

Gkargkavouzi, A., Halkos, G., & Matsiori, S. (2019). Environmental behavior in a private-sphere context: Integrating theories of planned behavior and value belief norm, self-identity and habit. *Resources, Conservation and Recycling*, *148*, 145-156. https://doi:10.1016/j.resconrec.2019.01.039.

Grant, C., & Osanloo, A. (2014). Understanding, selecting, and integrating a theoretical framework in dissertation research: Creating the blueprint for your "House". *Administrative Issues Journal Education Practice and Research*, 4(2) 12-26. https://doi.org/10.5929/2014.4.2.9.

Green, D. (2018, November 19). *Triangulation | Better Evaluation*. Betterevaluation.org. https://www.betterevaluation.org/en/evaluation-options/triangulation.

Guerin, R. J., & Toland, M. D. (2020). An application of a modified theory of planned behavior model to investigate adolescents' job safety knowledge, norms, attitude and intention to enact workplace safety and health skills. *Journal of Safety Research*, *72*, 189-198. https://doi.org/10.1016/j.jsr.2019.12.002.

Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management*, *33*(5), 861-874. https://doi.org/10.1016/j.ijinfomgt.2013.07.001.

Gustafsson, J., & Gustafsson, J. (2017). *Single case studies vs. multiple case studies: A comparative study* [Doctoral Dissertation]. http://www.diva-portal.org/smash/get/diva2:1064378/FULLTEXT01.pdf.

Haegele, J. A., Hodge, S. R., & Kozub, F. M. (2017). Beliefs about physical activity and sedentary behaviors of adults with visual impairments. *Disability and Health Journal*, *10*(4), 571-579. https://doi:10.1016/j.dhjo.2017.03.008.

Hagger, M. S. (2019). The reasoned action approach and the theories of reasoned action and planned behavior. *Psychology*. https://doi:10.1093/obo/9780199828340-0240.

Hakak, S., Gilkar, G. A., Guslendra, Ritonga, R., & Herawan, T. (2018). Future private cloud architecture for universities. *Advances in Intelligent Systems and Computing*, *672*, 720-729. https://doi:10.1007/978-981-10-7512-4_71.

Halcomb, E. J. (2018). Mixed methods research: The issues beyond combining methods. *Journal of Advanced Nursing*, *75*(3), 499-501. https://doi:10.1111/jan.13877.

Hall, J. (2019, October 25). 3 ways to merge teams - not just companies. Forbes, 12–13. https://www.forbes.com/sites/johnhall/2019/10/25/3-ways-to-merge-teams--not-just-companies/?sh=6d37aced589a.

Hammarberg, K., Kirkman, M., & De Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. *Human Reproduction*, *31*(3), 498-501. https://doi:10.1093/humrep/dev334.

Hanney, S., Kreager, C., O'Brien, J., & Gutierrez, F. (2019, September 10). *Hybrid cloud communication system*. https://patents.google.com/patent/US10412167B2/en.

Hardy, Q. (2018, February 8). *How Cloud Computing Is Changing Management*. Harvard Business Review. https://hbr.org/2018/02/how-cloud-computing-is-changing-management.

Haythornthwaite, C., Andrews, R., Fransman, J., & Meyers, E. M. (2016). *The SAGE handbook of E-learning research, 2e*. SAGE.

Heesen, R., Bright, L. K., & Zucker, A. (2016). Vindicating methodological triangulation. *Synthese*, *196*(8), 3067-3081. https://doi:10.1007/s11229-016-1294-7.

Hemdan, E. E., & Manjaiah, D. H. (2018). Digital forensic approach for investigation of cybercrimes in private cloud environment. *Advances in Intelligent Systems and Computing*, *707*, 25-33. https://doi:10.1007/978-981-10-8639-7_3.

Hennink, M., & Kaiser, B. (2019). Saturation in Qualitative Research. *SAGE: Research Methods*.

Hirschmann, W. (1994, January 1). A Guide to Building More Resilient Business. Harvard Business, 19–56. https://hbr.org/1964/01/profit-from-the-learning-curve.

Histed, S. (2019, February 1). A Walk in the Clouds- The Advantages of AWS GovCloud for VRS. *Votem - Voting for a Mobile World*. https://www.votem.com/cloud-hosting-aws-govcloud-for-vrs/.

Hoffmann, R., Blijlevens, J., Chuah, S., Neelim, A., & Laban, J. (2018). The ethics of student participation in economic experiments: Arguments and evidence. *SSRN Electronic Journal*. https://doi:10.2139/ssrn.3237911.

Hoque, Z., Parker, L. D., Covaleski, M. A., & Haynes, K. (2017). *The Routledge companion to qualitative accounting research methods*. Taylor & Francis.

Houghton, C., Murphy, K., Meehan, B., Thomas, J., Brooker, D., & Casey, D. (2017). From screening to synthesis: Using NVivo to enhance transparency in qualitative evidence synthesis. *Journal of Clinical Nursing*, *26*(5-6), 873-881. https://doi:10.1111/jocn.13443.

Houshian, A. (2017, May 10). Third-party vendor management best practices. *A-LIGN*. https://a-lign.com/third-party-vendor-management-best-practices/.

Hurst, M., & Taccone, N. (2013, December 20). What is ethnography? - Studying cultural phenomena. *Sociology 101: Intro to Sociology*. Study.com. https://study.com/academy/lesson/what-is-ethnography-studying-cultural-phenomena.html.

Hwang, D., Pike, R., & Manson, D. (2016). The Development of an Educational Cloud for IS Curriculum through a Student-Run Data Center. *Information Systems*

Education Journal (ISEDJ), *14*(1). https://files.eric.ed.gov/fulltext/EJ1136305.pdf.

Jack, E. P., & Raturi, A. S. (2006). Lessons learned from methodological triangulation in management research. *Management Research News*, *29*(6), 345–357. https://doi.org/10.1108/01409170610683833.

International Data Corporation. (2018, October 5). IDC report series offers real world insights, advice, and best practices for organizations planning the move to SaaS and cloud-enabled software. *Business Wire*.

Jackson, K. L. (2015). IEEE GovCloud: Making a difference for global governments. *IEEE Cloud Computing*, *2*(4), 54-59. https://doi.org/10.1109/mcc.2015.81.

Jackson, K. L. (2016). Government cloud Achilles heel: The network. *IEEE Cloud Computing*, *3*(3), 72-75. https://doi.org/10.1109/mcc.2016.56.

Jakóbik, A. (2020). Stackelberg game modeling of cloud security defending strategy in the case of information leaks and corruption. *Simulation Modelling Practice and Theory*, *103*, 102071. https://doi.org/10.1016/j.simpat.2020.102071.

Jantunen, E., Gorostegui, U., Zurutuza, U., Albano, M., Ferreira, L. L., Hegedüs, C., & Campos, J. (2018). Remote maintenance support with the aid of cyber-physical systems and cloud technology. *Proceedings of the Institution of Mechanical Engineers, Part I: Journal of Systems and Control Engineering*, *232*(6), 784-794. https://doi.org/10.1177/0959651818772939.

Jentoft, N., & Olsen, T. S. (2017). Against the flow in data collection: How data triangulation combined with a 'slow' interview technique enriches data. *Qualitative Social Work*, *18*(2), 179-193. https://doi.org/10.1177/1473325017712581.

Ji, S., Shao, J., Agun, D., & Yang, T. (2018). Privacy-aware ranking with tree ensembles on the cloud. *The 41st International ACM SIGIR Conference on Research & Development in Information Retrieval - SIGIR '18*, 315-324. https://doi.org/10.1145/3209978.3210022.

Johnson, L. (2018, June 25). Problems in research: Quantitative & qualitative methods. | *Synonym*. Synonym.com. https://classroom.synonym.com/problems-research-quantitative-qualitative-methods-4418.html.

Johnson, M., O'Hara, R., Hirst, E., Weyman, A., Turner, J., Mason, S., Siriwardena, A. N. (2017). Multiple triangulation and collaborative research using qualitative methods to explore decision making in pre-hospital emergency care. *BMC Medical Research Methodology*, *17*(1). https://doi:10.1186/s12874-017-0290-z.

Jones, C. & Laat, M. (2016). Networked learning. In C. Haythornthwaite, R. Andrews, & J. Fransman. *The SAGE Handbook of e-learning Research* (pp. 44-61). 55 City Road, London: SAGE Publications Ltd. https://doi:10.4135/9781473955011.n3.

Jones, J., & Smith, J. (2017). Ethnography: Challenges and opportunities. *Evidence Based Nursing*, *20*(4), 98-100. https://doi:10.1136/eb-2017-102786.

Kan, M. P. H., & Fabrigar, L. R. (2017). Theory of Planned Behavior. *Encyclopedia of Personality and Individual Differences*, 1–8. https://doi.org/10.1007/978-3-319-28099-8_1191-1.

Kanwal, T., Jabbar, A. A., Anjum, A., Malik, S. U., Khan, A., Ahmad, N., & Bakubaid, M. A. (2019). Privacy-aware relationship semantics–based XACML access control model for electronic health records in hybrid cloud. *International Journal of Distributed Sensor Networks*, *15*(6), 155014771984605. https://doi:10.1177/1550147719846050.

Karunagaran, S., Mathew, S. K., & Lehner, F. (2017). Privacy protection dashboard. *Proceedings of the 2017 ACM SIGMIS Conference on Computers and People Research - SIGMIS-CPR '17*, 181-182. https://doi.org/10.1145/3084381.3084424.

Kauer, S., Buhagiar, K., & Sanci, L. (2016). Facilitating mental health help seeking in young adults: The underlying theory and development of an online navigation tool. *Advances in Mental Health*, *15*(1), 71-87. https://doi:10.1080/18387357.2016.1237856.

Kayte, S. (2015). Review and Classification of Cloud Computing Research. *IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)*, *5*(6), 58–62. ResearchGate. https://doi.org/doi:10.9790/4200-05615862.

Kemp, R. (2018). Legal aspects of cloud security. *Computer Law & Security Review*, *34*(4), 928-932. https://doi.org/10.1016/j.clsr.2018.06.001.

Kim, A., Lee, J., & Kim, M. (2016). Resource management model based on cloud computing environment. *International Journal of Distributed Sensor Networks*, *12*(11), 155014771667655. https://doi.org/10.1177/1550147716676554.

Kiriakidis, S. (2016). Perceived behavioural control in the theory of planned behaviour: Variability of conceptualization and Operationalization and implications for measurement. *Strategic Innovative Marketing*, 197-202. https://doi.org/10.1007/978-3-319-33865-1_25.

Kirsh, D. (2019, February 8). *How the Belmont Report clarified informed consent*. MassDevice. https://www.massdevice.com/how-the-belmont-report-clarified-informed-consent/.

Koo, C. J., & Kim, J. (2015). Decision making for the adoption of cloud computing for sensor data: From the viewpoint of industrial security. *International Journal of Distributed Sensor Networks*, *11*(9), 581563. http://doi:10.1155/2015/581563.

Koo, J., Oh, S., Lee, S. H., & Kim, Y. (2020). Security architecture for cloud-based command and control system in IoT environment. *Applied Sciences*, *10*(3), 1035. http://doi:10.3390/app10031035.

Korstjens, I., & Moser, A. (2017). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice*, *24*(1), 120-124. http://doi:10.1080/13814788.2017.1375092.

Kratzke, N., & Siegfried, R. (2020). Towards cloud-native simulations – lessons learned from the front-line of cloud computing. *The Journal of Defense Modeling and*

Simulation: Applications, Methodology, Technology, 154851291989532. http://doi:10.1177/1548512919895327.

Krogh, S. (2013). *Journal of Information Architecture*. (n.d.). Journalofia.org. http://journalofia.org/volume5/issue2/03-krogh/.

Kuo, A. M.-H. (2011). Opportunities and Challenges of Cloud Computing to Improve Health Care Services. Journal of Medical Internet Research, 13(3), e67. https://doi.org/10.2196/jmir.1867.

Lai, P. (2017). The literature review of technology adoption models and theories for the novelty technology. *Journal of Information Systems and Technology Management*, *14*(1), 21-38. https://doi.org/10.4301/s1807-17752017000100002.

LaMorte, W. (2019, September 9). *The Theory of Planned Behavior*. Sphweb.Bumc.Bu.Edu; Boston University School of Public Health. https://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories3.html.

Lasch, K. E., Marquis, P., Vigneux, M., Abetz, L., Arnould, B., Bayliss, M., Crawford, B., & Rosa, K. (2010). PRO development: rigorous qualitative research as the crucial foundation. *Quality of Life Research*, *19*(8), 1087–1096. https://doi.org/10.1007/s11136-010-9677-6.

Lavraka, P. (2011). *Purposive Sample*. Sagepub.com. https://methods.sagepub.com/reference/encyclopedia-of-survey-research-methods/n419.xml.

Lazar, J., Hochheiser, H., & Feng, J. (2017). Critical acclaim for research methods in human computer interaction. *Research Methods in Human Computer Interaction*, v-viii. http://doi:10.1016/b978-0-12-805390-4.09986-6

Lee, T. (2017). Does classical Chinese philosophy reveal alternative rationalities? *Rationality*, 195-211. http://doi:10.1016/b978-0-12-804600-5.00010-6.

Liang, Y., Qi, G., Zhang, X., & Li, G. (2019). The effects of e-Government cloud assimilation on public value creation: An empirical study of China. *Government Information Quarterly*, *36*(4), 101397. https://doi.org/10.1016/j.giq.2019.101397.

Leitner, P., Wittern, E., Spillner, J., & Hummer, W. (2018). A mixed-method empirical study of function-as-a-Service software development in industrial practice. *ResearchGate*. http://doi:10.7287/peerj.preprints.27005.

Lemon, L., & Hayes, J. (2020). Enhancing Trustworthiness of Qualitative Findings: Using Leximancer for Qualitative Data Analysis Triangulation. *The Qualitative Report*, *25*(3), 604–614. https://nsuworks.nova.edu/tqr/vol25/iss3/3.

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

Li, Z. (2017). Design of online vocal music course based on Azure-PaaS platform. *International Journal of Emerging Technologies in Learning (iJET)*, *12*(09), 17. https://doi.org/10.3991/ijet.v12i09.7495.

Lindsley, K. A. (2019). Improving quality of the informed consent process: Developing an easy-to-read, multimodal, patient-centered format in a real-world setting. *Patient Education and Counseling*, *102*(5), 944-951. http://doi:10.1016/j.pec.2018.12.022.

Lnenicka, M., & Komarkova, J. (2019). Developing a government enterprise architecture framework to support the requirements of big and open linked data with the use of cloud computing. *International Journal of Information Management*, *46*, 124-141. https://doi.org/10.1016/j.ijinfomgt.2018.12.003.

Lobo, M. A., Moeyaert, M., Baraldi Cunha, A., & Babik, I. (2017). Single-case design, analysis, and quality assessment for intervention research. *Journal of Neurologic Physical Therapy*, *41*(3), 187-197. http://doi:10.1097/npt.0000000000000187.

Loerch, A. (2016). Learning Curves. Springer Science, 30–64. https://doi.org/https://doi.org/10.1007/978-1-4419-1153-7_526.

Maenhaut, P., Volckaert, B., Ongenae, V., & Turck, F. (2019). Resource management in a containerized cloud: Status and challenges. *Journal of Network and Systems Management*, *28*(2), 197-246. http://doi:10.1007/s10922-019-09504-0.

Mack, N., & Woodsong, C. (2005). *Qualitative research methods: A data collector's field guide*. Research Triangle Park, NC: U.S. Agency for International Development (USAID).

Malawski, M., Gajek, A., Zima, A., Balis, B., & Figoela, K. (2017). Serverless execution of scientific workflows: Experiments with Hyperflow, AWS lambda and Google

cloud functions. *Future Generation Computer Systems*. http://doi:10.1016/future.201710.029.

Malinowski, B. (2016). *HOW-TO GUIDE TITLE*. https://www.herd.org.np/uploads/frontend/Publications/PublicationsAttachments1/1480653184-Ethnography_1.pdf.

Malterud, K., Siersma, V. D., & Guassora, A. D. (2016). Sample size in qualitative interview studies. *Qualitative Health Research*, *26*(13), 1753-1760. http://doi:10.1177/1049732315617444.

Margolis, M. (2017, November 2). *How to build better rapport for better research interviews*. Medium. https://library.gv.com/how-to-build-better-rapport-for-better-research-interviews-869952b6a71d.

Maria, A. L., Sundstrom, B., Faria, A. A., Moxley Saxon, G., & Ramos-Ortiz, J. (2019). Using the theory of planned behavior and self-identity to explore women's decision-making and intention to switch from combined oral contraceptive pill (COC) to long-acting reversible contraceptive (LARC). *BMC Women's Health*, *19*(1). http://doi:10.1186/s12905-019-0772-8.

Mariotto, F. L., Zanni, P. P., & Moraes, G. H. S. M. D. (2014). What is the use of a single-casestudy in management research? *Revista de Administração de Empresas*, *54*(4), 358–369. https://doi.org/10.1590/s0034-759020140402.

Masood, R., & Aslam, M. (2016). Innovative approach ensuring security and privacy in cloud computing. *Pakistan Journal of Science*, *68*(1), 42-47. https://search-proquest-

com.ezp.waldenulibrary.org/compscijour/docview/1782996867/F6B0562FBA314D9DPQ/9?accountid=14872.

Mbuagbaw, L., Lawson, D. O., Puljak, L., Allison, D. B., & Thabane, L. (2020). A tutorial on methodological studies: the what, when, how and why. *BMC Medical Research Methodology*, *20*(1). https://doi.org/10.1186/s12874-020-01107-7.

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2018). Twelve tips for conducting qualitative research interviews. *Medical Teacher*, *41*(9), 1002-1006. http://doi:10.1080/0142159x.2018.1497149.

McLeary, P. (2019). *SecArmy's Multi-Domain Kill Chain: Space-Cloud-AI*. Breaking Defense. https://breakingdefense.com/2019/11/secarmys-multi-domain-kill-chain-space-to-cloud-to-ai/.

McNally, K. (2020). *Library Resource Guides: Literature Review: Home*. Libguides.Csu.Edu.Au. https://libguides.csu.edu.au/c.php?g=476545.

Microsoft. *Public Cloud vs Private Cloud vs Hybrid Cloud | Microsoft Azure*. (2019). Microsoft.com; Microsoft Azure. https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/.

Mohajan, H. K. (2017). Two criteria for good measurements in research: Validity and reliability. *Annals of Spiru Haret University. Economic Series*, *17*(4), 59-82. http://doi:10.26458/1746.

Moon, K., Brewer, T. D., Januchowski-Hartley, S. R., Adams, V. M., & Blackman, D. A. (2016). A guideline to improve qualitative social science publishing in ecology

and conservation journals. *Ecology and Society*, *21*(3). http://doi:10.5751/es-08663-210317.

Morris, J. (2017, August 15). *Education and Positive Social Change | Africa ELI*. Africaeli.org. https://africaeli.org/education-and-positive-social-change.

Mueller, P. S., & Hook, C. C. (2006). Ethical aspects of research involving elderly persons. *Handbook of Models for Human Aging*, 79-92. http://doi:10.1016/b978-012369391-4/50008-4.

Müller, S. D., Holm, S. R., & Søndergaard, J. (2015). Benefits of cloud computing: Literature review in a maturity model perspective. *Communications of the Association for Information Systems*, *37*. http://doi:10.17705/1cais.03742.

Munisso, R., & Chis, A. E. (2017). CloudMapper: A model-based framework for portability of cloud applications consuming PaaS services. *2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*. https://doi.org/10.1109/pdp.2017.94.

Muthathi, I. S., Thurling, C. H., & Armstrong, S. J. (2017). Through the eyes of the student: Best practices in clinical facilitation. *Curationis*, *40*(1). https://doi.org/10.4102/curationis.v40i1.1787.

Nasr, D. M., & Ouf, S. (2012). A proposed smart E-learning system using cloud computing services: PaaS, IaaS and Web 3.0. *International Journal of Emerging Technologies in Learning (iJET)*, *7*(3), 19-24. https://doi.org/10.3991/ijet.v7i3.2066.

Neubauer, B. E., Witkop, C. T., & Varpio, L. (2019). How phenomenology can help us learn from the experiences of others. *Perspectives on Medical Education*, *8*(2), 90-97. http://doi:10.1007/s40037-019-0509-2.

Niepel, C., Burrus, J., Greiff, S., Lipnevich, A. A., Brenneman, M. W., & Roberts, R. D. (2018). Students' beliefs and attitudes toward mathematics across time: A longitudinal examination of the theory of planned behavior. *Learning and Individual Differences*, *63*, 24-33. http://doi:10.1016/j.lindif.2018.02.010.

Nissim, N., Lahav, O., Cohen, A., Elovici, Y., & Rokach, L. (2019). Volatile memory analysis using the MinHash method for efficient and secured detection of malware in private cloud. *Computers & Security*, *87*, 101590. https://doi.org/10.1016/j.cose.2019.101590.

Nleya, P. (2016). Proprietary teaching tools. In S. Danver (Ed.), *The SAGE encyclopedia of online education* (pp. 926-927). Thousand Oaks,, CA: SAGE Publications, Inc. http://doi:10.4135/9781483318332.n293.

Noble, H., & Heale, R. (2019). Triangulation in research, with examples. *Evidence Based Nursing*, *22*(3), 67-68. https://doi.org/10.1136/ebnurs-2019-103145.

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, *16*(1), 1–13. https://doi.org/10.1177/1609406917733847.

Noyes, J., Booth, A., Moore, G., Flemming, K., Tunçalp, Ö., & Shakibazadeh, E. (2019). Synthesizing quantitative and qualitative evidence to inform guidelines on complex interventions: Clarifying the purposes, designs and outlining some

methods. *BMJ Global Health*, *4*(Suppl 1), e000893. http://doi:10.1136/bmjgh-2018-000893.

Nyumba, T., Wilson, K., Derrick, C. J., & Mukherjee, N. (2018). The use of focus group discussion methodology: Insights from two decades of application in conservation. *Methods in Ecology and Evolution*, *9*(1), 20-32. http://doi:10.1111/2041-210x.12860.

Oliveira, T., Martins, R., Sarker, S., Thomas, M., & Popovič, A. (2019). Understanding SaaS adoption: The moderating impact of the environment context. *International Journal of Information Management*, *49*, 1-12. https://doi.org/10.1016/j.ijinfomgt.2019.02.009.

Palinkas, L., Horwitz, S., Green, C., Wisdom, J., Duan, N., & Hoagwood, K. (2016). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *NCBI*, *42*(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y.

Palmer, B. W. (2015, September). Study participants and informed consent. *Monitor on Psychology*, *46*(8). http://www.apa.org/monitor/2015/09/ethics.

Paradis, E., O'Brien, B., Nimmon, L., Bandiera, G., & Martimianakis, M. (2016). Design: Selection of Data Collection Methods. *Journal of Graduate Medical Education*, *8*(2), 263-264. http://doi:10.4300/JGME-D-16-00098.1.

Passafaro, P., Livi, S., & Kosic, A. (2019). Local norms and the theory of planned behavior: Understanding the effects of spatial proximity on recycling intentions

and self-reported behavior. *Frontiers in Psychology*, *10*. https://doi.org/10.3389/fpsyg.2019.00744.

Paul, J., Modi, A., & Patel, J. (2016). Predicting green product consumption using theory of planned behavior and reasoned action. *Journal of Retailing and Consumer Services*, *29*, 123-134. http://doi:10.1016/j.jretconser.2015.11.006.

Peng, J., Zhi-cai, J., & Lin-jie, G. (2014). Application of the expanded theory of planned behavior in intercity travel behavior. *Discrete Dynamics in Nature and Society*, *2014*, 1-10. https://doi.org/10.1155/2014/308674.

Perrier, L., Blondal, E., Ayala, A. P., Dearborn, D., Kenny, T., Lightfoot, D., Reka, R., Thuna, M., Trimble, L., & MacDonald, H. (2017). Research data management in academic institutions: A scoping review. *PLOS ONE*, *12*(5), e0178261. https://doi.org/10.1371/journal.pone.0178261.

Perrons, R. K. (2015). How the energy sector could get it wrong with cloud computing. *Energy Exploration & Exploitation*, *33*(2), 217-226. http://doi:10.1260/0144-5987.33.2.217.

Perry, Y. (2018, November 7). *AWS GovCloud disaster recovery plan*. NetApp Cloud Solutions Homepage. https://cloud.netapp.com/blog/aws-govcloud-disaster-recovery-plan.

Preimesberger, C. (2017). AWS planning launch of new region for its GovCloud service. *EBSCOhost*, 1. https://web-b-ebscohost-com.ezp.waldenulibrary.org/ehost/detail/detail?vid=11, &sid=1d8765f3-9c1d-4437-8b81-3d498b57fcc6%40pdc-v-sessmgr03,

&bdata=JnNpdGU9ZWhvc3QtbGl2ZSZzY29wZT1zaXRl#db=a9h,
&AN=123606668.

Pringle, J., Hendry, C., & McLafferty, E. (2011). Phenomenological approaches: Challenges and choices. *Nurse Researcher*, *18*(2), 7-18. http://doi:10.7748/nr2011.01.18.2.7.c8280.

Proctor, L., Angus, D. J., Blaszczynski, A., & Gainsbury, S. M. (2019). Understanding use of consumer protection tools among internet gambling customers: Utility of the theory of planned behavior and theory of reasoned action. *Addictive Behaviors*, *99*, 106050. http://doi:10.1016/j.addbeh.2019.106050.

Proeschold-Bell, R. (2018, March 12). *Five Tips for Conducting Effective Qualitative Interviews*. Duke Global Health Institute. https://globalhealth.duke.edu/news/five-tips-conducting-effective-qualitative-interviews.

Puckett, P. (2020). *The Army Cloud Plan* (4th ed., pp. 1–21). U.S. Army. https://api.army.mil/e2/c/downloads/2020/09/11/81bb912e/the-army-cloud-plan-2020-final2.pdf.

Råheim, M., Magnussen, L. H., Sekse, R. J., Lunde, Å., Jacobsen, T., & Blystad, A. (2016). Researcher–researched relationship in qualitative research: Shifts in positions and researcher vulnerability. *International Journal of Qualitative Studies on Health and Well-being*, *11*(1), 30996. http://doi:10.3402/qhw.v11.30996.

Rahman, M. S. (2016). The advantages and disadvantages of using qualitative and quantitative approaches and methods in language “Testing and assessment”

research: A literature review. *Journal of Education and Learning*, *6*(1), 102. http://doi:10.5539/jel.v6n1p102.

Rajan, A. P. (2020). A review on serverless architectures - function as a service (FaaS) in cloud computing. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *18*(1), 530. http://doi:10.12928/telkomnika.v18i1.12169.

Ramachandra, G., Iftikhar, M., & Khan, F. (2017). A comprehensive survey on security in cloud computing. *ScienceDirect*, *110*, 465-472. https://doi.org/10.1016/j.procs.2017.06.124.

Redda, E. (2019). Auth.Laureate.net. https://ezp.waldenulibrary.org/login?qurl=https%3A%2F%2Fsearch.proquest.com%2Fdocview%2F2316729879%3Faccou.

Roche, S. (2019, September 5). *Cloud Computing for Defense*. Amazon Web Services, Inc. https://aws.amazon.com/government-education/defense.

Rodríguez-Bravo, B., Nicholas, D., Herman, E., Boukacem-Zeghmouri, C., Watkinson, A., Xu, J., Świgoń, M. (2017). Peer review: The experience and views of early career researchers. *Learned Publishing*, *30*(4), 269-277. http://doi:10.1002/leap.1111.

Roulston, K. (2018, January 18). *Triangulation in qualitative research*. QualPage; QualPage. https://qualpage.com/2018/01/18/triangulation-in-qualitative-research/.

Ryan, S., & Carr, A. (2010). Applying the biopsychosocial model to the management of rheumatic disease. *Rheumatology*, 63-75. http://doi:10.1016/b978-0-443-06934-5.00005-x.

Saha, T. K., & Koshiba, T. (2018). Outsourcing private equality tests to the cloud. *Journal of Information Security and Applications*, *43*, 83-98. https://doi.org/10.1016/j.jisa.2018.09.002.

Salkind, N. (2010). Triangulation. *Encyclopedia of Research Design*. https://doi.org/10.4135/9781412961288.n469.

Salleh, S. (2016). Examining the influence of teachers ' beliefs towards technology integration in classroom. *International Journal of Information and Learning Technology*, *33*(1), 17-35. http://doi:10.1108/ijilt-10-2015-0032.

Sanghera, N. (2020). *Developing Military Cultural Competencyto Better Serve Those Who Have Served Us | The Journal of Optometric Education*. Opted.org. https://journal.opted.org/article/developing-military-cultural-competency-to-better-servethose-who-have-served-us/.

Sarmah, B., Kamboj, S., & Kandampully, J. (2018). Social media and Co-creative service innovation: An empirical study. *Online Information Review*, *42*(7), 1146-1179. https://doi.org/10.1108/oir-03-2017-0079.

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Jinks, C. (2017). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity*, *52*(4), 1893-1907. http://doi:10.1007/s11135-017-0574-8.

Schwarzenegger, C. (2017, November 7). *Triangulation*. Wiley Online Library. https://onlinelibrary.wiley.com/http://doi/abs/10.1002/9781118901731.iecrm0255.

Schweitzer, W. (2019, October 25). *IBM is Recognized as a 2019 Gartner Peer Insights Customers' Choice for Cloud Infrastructure as a Service, Worldwide.* IBM News Room. https://newsroom.ibm.com/2019-10-25-IBM-is-Recognized-as-a-2019-Gartner-Peer-Insights-Customers-Choice-for-Cloud-Infrastructure-as-a-Service-Worldwide.

Scientific Computing World. (2019, June/July 31). Case study: R, &D in the cloud: IDBS highlight the benefits of moving to the cloud with its SaaS solution. *Scientific Computing World*, *6*(166), 24-24.

Seffers, G. (2018, June 1). Army Accentuates Cloud Computing. *SIGNAL*, 11–12. https://www.afcea.org/content/army-accentuates-cloud-computing.

Senyo, P. K., Addae, E., & Boateng, R. (2018). Cloud computing research: A review of research themes, frameworks, methods and future research directions. *International Journal of Information Management*, *38*(1), 128-139. http://doi:10.1016/j.ijinfomgt.2017.07.007.

Shmueli, G., Bruce, P. C., Gedeck, P., & Patel, N. R. (2019). *Data mining for business analytics: Concepts, techniques and applications in Python*. John Wiley & Sons.

Simeone, A., Caggiano, A., Boun, L., & Deng, B. (2019). Intelligent cloud manufacturing platform for efficient resource sharing in smart manufacturing networks. *Procedia CIRP*, *79*, 233-238. https://doi.org/10.1016/j.procir.2019.

Song, H. H. (2020). Testing and evaluation system for cloud computing information security products. *Procedia Computer Science*, *166*, 84-87. https://doi.org/10.1016/j.procs.2020.02.023.

Srinivasan, A., Quadir, M. A., & Vijayakumar, V. (2015). Era of cloud computing: A new insight to hybrid cloud. *Procedia Computer Science*, *50*, 42-51. http://doi:10.1016/j.procs.2015.04.059.

Srivastava, P., & Khan, R. (2018). A Review Paper on Cloud Computing. *International Journal of Advanced Research in Computer Science and Software Engineering*, *8*(6), 17. https://doi.org/10.23956/ijarcsse.v8i6.711.

Stugocki, W., & Walkowiak, M. (2021). The Importance of Military Information Security. Scientific and Technical Journal, 7(1), 1–13. https://doi.org/https://doi.org/10.37105/sd.93.

Suh, M., & Hsieh, G. (2016). *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. Living Healthy.

Sun, S., Law, R., & Schuckert, M. (2020). Mediating effects of attitude, subjective norms and perceived behavioural control for mobile payment-based hotel reservations. *International Journal of Hospitality Management*, *84*, 102331. https://doi.org/10.1016/j.ijhm.2019.102331.

Sussman, R., & Gifford, R. (2018). Causality in the theory of planned behavior. *Personality and Social Psychology Bulletin*, *45*(6), 920-933. https://doi.org/10.1177/0146167218801363.

Szolnoki, G., & Hoffmann, D. (2013). Online, face-to-face and telephone surveys—Comparing different sampling methods in wine consumer research. *Wine Economics and Policy*, *2*(2), 57-66. http://doi:10.1016/j.wep.2013.10.001.

Teo, T., Zhou, M., & Noyes, J. (2016). Teachers and technology: Development of an extended theory of planned behavior. *Educational Technology Research and Development*, *64*(6), 1033-1052. http://doi:10.1007/s11423-016-9446-5.

Theofanidis, D., & Fountouki, A. (2018). Limitations and delimitations in the research process. *GORNA*, *7*(3), 155-162. https://doi:10.5281/zenodo.2552022.

The Theory of Planned Behavior [Behavioral Change Models]. (2019, September 9). Boston University School of Public Health. http://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories3.html.

Tornikoski, E., & Maalaoui, A. (2019). Critical reflections – The Theory of Planned Behaviour: An interview with Icek Ajzen with implications for entrepreneurship research. *International Small Business Journal*, *37*(5), 536–550. https://doi.org/10.1177/0266242619829681.

Tran, K., Nguyen, P., Dang, T., & Ton, T. (2018). The Impacts of the High-Quality Workplace Relationships on Job Performance: A Perspective on Staff Nurses in Vietnam. Behavioral Sciences, 8(12), 109. https://doi.org/10.3390/bs8120109.

Trapero, R., Luna, J., & Suri, N. (2016). Quantifiably trusting the cloud: Putting metrics to work. *IEEE Security & Privacy*, *14*(3), 73-77. https://doi.org/10.1109/msp.2016.65.

Tripathy, M. (2018). Building Quality Teamwork to Achieve Excellence in Business Organizations. International Research Journal of Management, IT and Social Sciences, 5(3), 1–7. https://doi.org/10.21744/irjmis.v5i3.662.

Trochim, W. M. K. (2020, March 10). *The Research Methods Knowledge Base*. Conjointly.com; Conjoint.ly. https://conjointly.com/kb/qualitative-validity.

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A cybercrime incident architecture with adaptive response policy. *Computers & Security*, *83*, 22–37. https://doi.org/10.1016/j.cose.2019.01.011.

Turner, P., & Turner, S. (2009). Triangulation in practice. *Virtual Reality*, *13*(3), 171–181. https://doi.org/10.1007/s10055-009-0117-2.

United States: Cohesity introduces comprehensive data management capabilities for AWS GovCloud. (2019). *Mena Report*.

Varghese, B., & Buyya, R. (2018). Next generation cloud computing: New trends and research directions. *Future Generation Computer Systems*, *79*, 849–861. https://doi.org/10.1016/j.future.2017.09.020.

Varia, J. (2013). New Whitepaper: AWS Cloud Security Best Practices. Compliance Security, 4(19), 4–7. Permalink. https://aws.amazon.com/security/new-whitepaper-aws-cloud-security-best-practices/.

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

Vesely, S., & Klöckner, C. A. (2018). Global social norms and environmental Behavior. *Environment and Behavior*, *50*(3), 247–272. https://doi.org/10.1177/0013916517702190.

Violino, B. (2019, August 15). *What is IaaS? Your data center in the cloud*. InfoWorld. https://www.infoworld.com/article/3220669/what-is-iaas-your-data-center-in-the-cloud.html.

Waller, V., Farquharson, K., & Dempsey, D. (2015). *Qualitative social research: Contemporary methods for the digital age* (1st ed.). London, England: SAGE.

Watkins, D. C. (2017). Rapid and rigorous qualitative data analysis. *International Journal of Qualitative Methods*, *16*(1), 160940691771213. http://doi:10.1177/1609406917712131

Weber, J., & Gillespie, J. (2001). Differences in ethical beliefs, intentions, and behaviors: The role of beliefs and intentions in ethics research revisited. *Research in Ethical Issues in Organizations*, 265-283. https://doi.org/10.1016/s1529-2096(01)03016-4.

Whitehead, M. (2020, September 28). Cybersecurity testing essentials for mergers and acquisitions. TechTarget. https://searchsecurity.techtarget.com/post/Cybersecurity-testing-essentials-for-mergers-and-acquisitions.

Williams, D. (2011, August 14). *About*. Qualitative Inquiry in Daily Life; Qualitative Inquiry in Daily Life. https://qualitativeinquirydailylife.wordpress.com/about/.

Wilson, V. (2014). Research methods: triangulation. *Evidence based library and information practice*, *9*(1), 74-75.

Wootton, B. (2018, March 5). How and why to leverage AWS GovCloud for compliance and regulation. *Contino*. https://www.contino.io/insights/how-and-why-to-leverage-aws-govcloud-for-compliance-and-regulation.

Wu, D. (2020). Empirical study of knowledge withholding in cyberspace: Integrating protection motivation theory and theory of reasoned behavior. *Computers in Human Behavior*, *105*, 106229. http://doi:10.1016/j.chb.2019.106229.

Yang, H., Lee, H., & Zo, H. (2017). User acceptance of smart home services: An extension of the theory of planned behavior. *Industrial Management & Data Systems*, *117*(1), 68-89. http://doi:10.1108/imds-01-2016-0017.

Yang, S., Su, Y., Wang, W., & Kaicheng, H. (2019). Research on developers' green procurement behavior based on the theory of planned behavior. *Sustainability*, *11*(10), 2949. http://doi:10.3390/su11102949.

Yirdew, G. N., Mnoj, S. K., & Bhaskari, D. L. (2017). Privacy enhancement in cloud environment through trusted third party approach. *International Journal of Advanced Research in Computer Science*, *8*(8), 273-277. http://doi:10.26483/ijarcs.v8i8.4700.

Yom, S. (2014). From Methodology to Practice. *Comparative Political Studies*, *48*(5), 616–644. https://doi.org/10.1177/0010414014554685.

Yuriev, A., Dahmen, M., Paillé, P., Boiral, O., & Guillaumie, L. (2020). Pro-environmental behaviors through the lens of the theory of planned behavior: A scoping review. *Resources, Conservation and Recycling*, *155*, 104660. http://doi:10.1016/j.resconrec.2019.104660.

Zaerens, K. (2011). Enabling the benefits of cloud computing in a military context. *2011 IEEE Asia-Pacific Services Computing Conference*. http://doi:10.1109/apscc.2011.42.

Zarzuela, P., & Antón, C. (2015). Determinants of social commitment in the young. Applying the theory of reasoned action. *Revista Española de Investigación de Marketing ESIC*, *19*(2), 83-94. http://doi:10.1016/j.reimke.2015.05.001.

Zhang, K. (2018). *Theory of Planned Behavior: Origins, development and future direction* (Unpublished doctoral dissertation). Hong Kong Baptist University, Kowloon, Hong Kong.

Zhao, K., Yang, Q., & Ma, X. (2017). Exploration of an open online learning platform based on Google cloud computing. *International Journal of Emerging Technologies in Learning (iJET)*, *12*(07), 17. https://doi.org/10.3991/ijet.v12i07.7249.

Zhou, H., Zhang, J., Liu, Z., Nie, D., Wu, W., & De Albuquerque, V. H. (2020). Research on circular area search algorithm of multi-robot service based on SOA cloud platform. *Applied Soft Computing*, *88*, 105816. https://doi.org/10.1016/j.asoc.2019.105816.

Appendix A: Letter of Individual Consent for Research Study

Dear Veteran,

Greetings! My name is Marc Anthony Rangel and I am currently pursuing an advanced degree in the Doctor of Information Technology (DIT) through Walden University located in Minneapolis, MN. My doctoral study focuses on the "Military Breaking Boundaries Implementing Third Party Cloud Computing Practices for Data Storage". Specifically, I am curious as to what the opinion is for senior IT military leadership and their thoughts on this new third party cloud practice. Having previously worked at Cheyenne Mountain and Peterson AFB as a cloud architect, I am very intimate with the squadrons in and around the Colorado Springs area including the skill sets the men and women maintain in accordance with this practice.

Specifically, I am seeking veterans with previous military cloud computing experience like cloud administrators, cloud engineers, or cloud architects. I am fully aware of the military's need to know and my questions will be unclassified and will not point to any specific architecture within an enterprise infrastructure. I too am an Air Force veteran with 12 years of active duty experience and several combat tours with the 23rd Special Tactics Squadron.

I would like to identify approximately 20 to 25 members interested in partaking in this study via face-to-face, telephone, or Skype interviews. If you are a current contractor or GS worker with previous military cloud knowledge, I am very interested in chatting with you. Each individual interview should last 45 to 60 minutes depending on your responses and details. Most importantly, your protection is critical, and I will follow

Walden University's confidentiality guidelines. Each participant will be referred to as participant one, two, etc. and your organization will be also be referred to as organization one, two. No monetary incentive will be offered, and this interview possibility is available on a first-come, first-served basis. Additionally, all data will be stored under lock and key for 5 years promising identify safety. Each participant will be able to accept or decline at any point during the process. At the conclusion of my study, I will be more than happy to share my findings.

Sincerely,

Marc Anthony Rangel

Walden DIT Student

Appendix B: Interview Protocol

Hello Mr./Mrs. (populate name). My name is Marc Anthony Rangel and I'd like to start by thanking you for your consent in participating in my DIT study and taking time from your busy schedule to complete this interview. This research question interview will be stored using encryption per your previous approval and formal acceptance. And as previously noted, there is no monetary assignment or payoff for agreeing to answer questions for my study. All data will be secured and stored in a vault for 5 years according to University policy.

As previously mentioned in my email invitation and consent form, I am focusing on the military breaking boundaries implementing third party cloud computing practices for data storage. If you agree to continue with my study, then we can begin immediately. If not, there is no penalty for declining to partake in this one-on-one interview and I would like to thank you for your time.

Researcher Focus

- Allow open-ended questions to be expanded upon if possible
- Provide the opportunity for all volunteers to paraphrase
- Ensure each question is answered in its entirety
- Keep answers focused on the study and do not allow the conversation or control to be lost

Appendix C: Interview Questions

1. Within your organization, what is your specific role and are you working with a cloud-centric security team?
2. What are your thoughts in reference to the military outsourcing its cloud storage to non-military third party vendors?
3. What security challenges, if any, do you foresee the military facing with third party storage like GovCloud?
4. How is the overall security posture-maintained working alongside civilian cloud engineers storing military data?
5. What tools or security practices will the military use to enforce stringent DISA regulations and expectations from cloud spillage or leakage?
6. What is your role if a major outage or security cloud spillage occurred impacting the overall safety and infrastructure of the enterprise?
7. Do you have a specific training plan for new military members joining the cloud security storage team? If so, please expand.
8. What do you think was the deciding factor for senior military leadership to implement cloud storage methods for military data vice other storage methods?
9. Is AWS providing cloud storage training for all military and civilian engineers working with the GovCloud?
10. Do you feel this change in security storage is more beneficial or has it built barriers between the third-party vendors and the military teams managing it?

Appendix D: NIH Certificate

Certificate of Completion

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

Date of completion: 09/10/2015

Certification Number: 1845346