Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.11, No.2, 2021

Security Limitations with Cloud Computing: Well-defined Security Measures Using Cloud Computing

Alberta Pratt-Sensie[1*] and Gail Miles[2]

1. College of Management and Technology, Walden University, Minneapolis, MN
alberta.pratt-sensie@cms.hhs.gov
2. College of Management and Technology, Walden University, Minneapolis, MN
gail.miles@mail.waldenu.edu

Abstract

Due to the ever-growing threat of security breaches that information technology (IT) organizations continually face, protecting customer information stored in the cloud is critical to ensure data integrity. Research shows that new categories of data breaches frequently emerge; thus, security strategies that build trust in consumers and improve system performance are crucial. The purpose of this qualitative multiple case study was to explore and analyze the strategies used by database administrators (DBAs) to secure data in a private infrastructure as a service (IaaS) cloud environment. The participants comprised of six DBAs from two IT companies in Baltimore, Maryland, with experience and knowledge of security strategies to secure data in private IaaS clouds. The disruptive innovation theory was the foundational framework for this study. Data were collected using semistructured interviews and a review of seven organizational documents. A thematic analysis was used to analyze the data. Two key themes are addressed in this article: importance of well-defined security measures in cloud computing and limitations of existing security controls in cloud computing. The findings of well-defined security strategies may benefit DBAs and IT organizations by providing strategies that may prevent future data breaches. Well-defined security strategies may protect an individual's data which, in turn, may promote individual well-being and build strong communities.

Keywords: cloud computing, security strategies, data breaches

DOI: 10.7176/JIEA/11-2-05
Publication date: June 30th 2021

1. Introduction

In recent years, the general public has become gravely concerned about securing personal identifiable data in the cloud. During the Covid-19 pandemic lockdown, leveraging the Internet has become one of cloud computing greatest strengths, when numerous businesses and schools were ordered to continue operations using the Zoom platform for meetings, schoolwork, or even social activities (Wagenseil, 2020). Serious concerns have been expressed by information security personnel about the security and privacy of the Zoom platform because hackers have taken advantage of vulnerabilities within the Zoom platform by participating in meetings, which they were not invited (Wagenseil, 2020). In this paper, the authors identified the importance of well-defined security measures in private infrastructure as a service (IaaS) cloud environments. Many organizations are now conducting business transactions and meetings online and are faced with numerous challenges of preventing hackers from accessing their customers' proprietary data. This paper focuses on using data to address the well-defined security strategies which can be used by organizations to secure data in cloud computing. The primary objective of this study is to inform Information Technology (IT) security professionals, of the well-defined successful security measures in cloud computing associated with data security policies.

This new trend of leveraging the Internet via cloud computing such as Zoom meetings has changed the IT work environment. Many organizations that were reluctant to adopt cloud computing have now embraced the use on their varied platforms, which, in turn, has improved productivity and efficiency, and decreased administrative costs. The use of cloud computing has supported disruptive innovation technology in IT organizations. This shift in how organizations currently conduct business is explained by King and Batartogtokh (2015), who opined that, despite cloud computing being a disruptive innovation technology, it has improved along a performance trajectory of sustaining innovation. Cloud computing emergence, though slow, confirmed Christensen's (1997) argument that this new IT technology disrupted the IT market. This process shift has enabled organizations to get their work done internally and externally (Baskerville, 2011). The emergence of increased use of cloud computing platforms has posed security and privacy challenges. The impact of increased use of cloud computing has changed the existing core business logic in organizations and created new business units that

performed diverse value activities (Christensen, 2011).

Securing data should be a priority for DBAs to prevent fraudulent access of customers personal identifiable information (PII). Authentication is a strategy used to verify the user's identity, which prevents unauthorized access to data confidentiality, security, and availability (CIA) (Yesilyurt and Yalman, 2016). A common authentication strategy now used by DBAs to prevent data breaches in IaaS cloud computing is multifactor authentication. Multifactor authentication is used to safeguard data in IaaS cloud computing by ensuring the data CIA. Multifactor authentication is more reliable than complex passwords because it uses two forms of verification (a password and something the user possesses) to prevent data breaches in IaaS cloud computing (Simon, 2019). Safeguarding data CIA to prevent data breaches in IaaS cloud computing, the use of multifactor authentication has been proposed (Heatherly, 2016). Multifactor validation of users password is now the emerging strategy which uses not only a fixed password, but also demands two or more proof of the three types of verification factor types: knowledge of what you know (password), what you possess (personal identification verification (PIV) card), and what you are (Jim, 2013). Another form of securing data in cloud computing is through authorization. Authorization is granting access rights to users based on their roles in their IT organizations. Cusack and Ghazizadeh (2016) recommended that authorization should be based on the user's access control to the data stored in the IaaS cloud computing. DBAs provide users access controls to the data stored in the IaaS cloud. Foresti et al. (2018) noted that regulatory rights are given to the users to different parts of the data to maintain data confidentiality. Authorization can be permitted using the user's role in the IT organization (Ramachandran and Chang, 2016). Granting authorization to users is using access controls such as a unique user ID and password (Ramachandran and Chang, 2016). DBAs can track the assigned user IDs to specific users to monitor any suspicious network activity to prevent data breaches. Only a few security methodologies are effective in ensuring information security within the cloud; data encryption is suggested as one of the topmost solutions to safeguarding data in IaaS cloud computing (Rao and Selvamani, 2015). DBAs can utilize encryption strategies such as scrambling data before storing it in the cloud server (Rao & Selvamani, 2015) to better secure information. Employing this strategy helps prevent access to data from various clients and makes the information unusable (Rao and Selvamani, 2015). For the successful implementation of cloud computing services within an organization, DBAs must identify adequate strategies to implement and prevent data breaches in private IaaS cloud computing.

Data security is not prioritized by IT organizations. IT leaders do not completely comprehend the importance of security controls and are less inclined to enforce them, which places data integrity at risk (Noguerol and Branch, 2018). Data confidentiality and integrity risks pose management issues for IT leaders. IT organizations are faced with increased pressure to secure the confidentiality of data for their customers, but after the Facebook privacy scandal in 2018, organizations are now receptive to mitigate data breaches (Gale, 2018). Managing data security is challenging, and IT leaders must ensure that their data are secured by implementing security controls to minimize data breaches in IaaS cloud computing. The general IT problem is that increased use of cloud computing platforms increases organizations exposure to security and privacy risks with challenges of how to secure customers personal identifiable data. The specific IT problem is that some DBAs lack organizational strategies to secure personable identifiable data in order to increase the use of cloud computing platforms.

2. Foundational Theory

We adopted the Disruptive Innovation Theory (DIT) as the conceptual framework for this study. Christensen first coined the term *disruptive innovation theory* in 1995 and published it in his book titled *An Innovator's Dilemma* (Christensen, 1997). A series of case studies in the book gained notoriety because it showed how incumbent organizations become incapacitated when a new technology with low performance and low costs disrupts the existing market and traditional firms. Christensen (1997) emphasized that in the initial stages of disruption, the lower-performing innovation meets the necessities of a little portion of the current client base but as the innovation advances, its execution enhances and the development addresses the issues of more clients in the business. Christensen proposes that organizations can be successful when their leadership supports new technology instead of evading it or refusing to acknowledge it. DIT was the basis of a series of mature technological innovation studies, the focus of which was on identifying radical innovation (Bohnsack and Pinkse, 2017, Christensen, 2011). Christensen (1997) stated that the DIT supports innovations and spawns evolution, which enhances performance in the current IT environment. Therefore, the DIT was a good choice to support this qualitative case study because the research emphasis was on the opinions of IT professionals regarding well defined security strategies on cloud computing used to prevent data breaches. The results of the study may help IT leaders improve the process of organizations implementing cloud computing and making use of the cost-saving benefits of this technology. The increased use of Zoom meetings by organizations during the pandemic aligns with the suggestion of Yu et al. (2017), that cloud computing is a disruptive innovation due to its frequent use by organizations. The increased use of cloud computing has made organizational leaders change the way they conducted business, such as accessing software anywhere and anytime as long as there is access to the Internet. Disruptive Innovation Theory was

adopted as our theoretical foundation to study well defined security strategies associated with securing data in a private IaaS cloud computing.

3. Methodology

A multiple case-study design was used for this research study. We independently interviewed 6 individuals from two IT organizations. Gentles et al. (2015) stated that a case study consisted of independent individuals and other organizational documents. A case study is also exploratory and explanatory which helped the researchers answer the how and why questions. The phenomenon explored in this study was the strategies DBAs used to secure data in private IaaS cloud computing. Using a multiple case study helped improve the credibility of the study's findings The multiple case study allowed us to collect data from research participants to compare and contrast the strategies DBAs used in the two IT organizations to secure data in private IaaS cloud computing. Methodological triangulation was adopted in this study by recording interviews from the research participants, as well as analyzing the organizational documents related to security strategies used to prevent data breaches in private IaaS cloud computing. Methodological triangulation is the use of two or more data sources that minimized biases and limitations resulting from using a single method (Joslin and Müller, 2016). Therefore, the use of methodological triangulation was beneficial to ensure validity and reliability of this study.

3.1 Data Collection

The data collection technique used for this research is focused on using multiple data sources: semi-structured interviews, organizational documents, and observations. Interview has been the most common data collection technique used for qualitative studies (Jamshed, 2014). The semi-structured interview for this study was completed by each participant through audio recordings and transcribed. The interview protocol consisted of open-ended questions that generated rich and thick data from the participants. Document analysis was used for a review of organizational documents related to security strategies to prevent data breaches in private IaaS cloud computing, field notes, and a personal diary (reflective journal). Carter et al. (2014) stated that the use of multiple resources in a qualitative case study provided in-depth and thick data to understand the phenomena better. Additionally, this data collection was focused on locating peer-reviewed articles from a variety of sources. The databases provided access to a large number of peer-reviewed articles and journals on cloud computing. The procedures used to locate these articles included the use of keywords related to the topic of study. These included *cloud computing definition*, *data security*, *cloud computing and regulations*, *cloud computing and cost*, *cloud computing and benefits*, and *cloud computing and risks*. A summary of these sources is given in Table 1.

Table 1
Summary of Research Articles Consulted in Study

Sources from review of the professional and academic literature	Number
Total references in study:	**70**
Total peer-reviewed references in study:	**65**
Total peer-reviewed in lit. w/in 5 years:	**64**
% Peer-reviewed references in study:	**93%**
% Peer-reviewed references in % w/in 5 years:	**77%**

4. Results

4.1 Importance of well-defined security measures in cloud computing

The importance of well-defined security measures in cloud computing emerged as the primary theme for this study. The DBA interviewees all emphasized how important it was to use authentication, encryption, authorization, data integrity, and confidentiality to secure data stored in private cloud computing. This theme was

consistent with the trends revealed in the open literature review (Cusack and Ghazizadeh, 2016, Flores et al., 2014, Schniederjans and Hales, 2016, Sindhu and Mushtaque, 2014, Sookhak et al., 2018). The results from the study support the use of the DIT (Christensen, 2006, Goldstein, 2015) as the conceptual framework. Well-defined security measures, when used in cloud computing, are associated with the protection of the database. This theme consisted of four pivotal subthemes: authentication; encryption; authorization; and data integrity and confidentiality.

Based on participant data, these four subthemes were required for DBAs to secure data in cloud computing. Figure 1 shows the participants responses to the use of the four subcategories of well-defined security strategies.

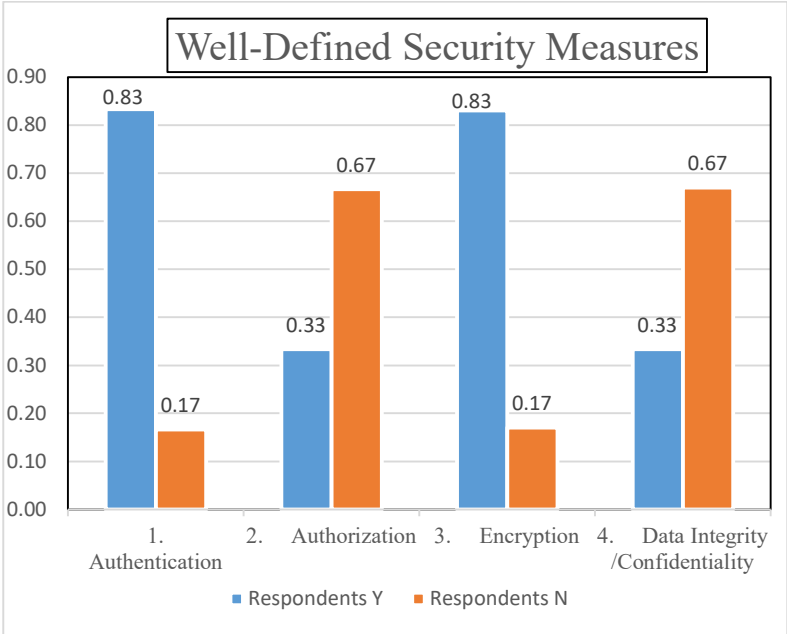

Figure 1. Importance of well-defined security measures in cloud computing subthemes

4.1.1 Authentication

The first subtheme was authentication. Five out of six of the DBAs from the two case organizations emphasized the importance of data encryption. The participants emphasized how critical authentication was in securing data in private IaaS cloud computing. Han et al. (2018) found that multifactor authentication wins the support of customers for its high-security benefits by improving the security of the user's data. Moreover, the use of multifactor authentication is more reliable than using most complex passwords, and this makes it critical to prevent database breaches. Two-factor authentication serves as an added line of protection and is a better way to protect data than the use of a stringent password (Simon, 2019) and is critical to blocking hacks and assaults to customers personal information. In comparing the two cases used, two out of the three participants from each organization agreed that multifactor authentication is the first step to prevent unauthorized access to data stored in the cloud, which would prevent data breaches in cloud computing.

The findings are consistent with how low-end disruptive technology such as cloud computing has forced organizations to change their business logic. This change in business logic is done by organizations remaining competitive by improving products and system performance in the continuously evolving technological age by exploiting the disruption. Disruptive innovation is an ordinarily substandard development that in the long run improves and spawns better products because it is less expensive, progressively advantageous, and for some customers, adequate (Goldstein, 2015). The experience of all the participants provided an understanding of using well-defined security measures like authentication in cloud computing to secure data in cloud computing and ensure that the security risks of data breaches are minimized. These findings by the authors position managers and DBAs to embrace DIT as an opportunity to position the organization for positive change. Furthermore, to establish a secure database, DBAs emphasized that authentication improves the productivity of data security in cloud computing. Once DBAs understand that authentication can prevent data breaches, they can support and assist IT organizations with securing data in IaaS cloud computing. Moreover, authentication schemes continue to evolve

to protect data in cloud computing and more research needs to be done in the future focusing on two-factor versus three-factor authentication, hash-based schemes, symmetric cryto-system-based schemes, and public key cryptosystem-based schemes (Wang et al., 2020).

4.1.2 Authorization

The second theme was authorization. Heatherly (2016) defined authorization as the permission rights provided to users to access databases. Cusack and Ghazizadeh (2016) indicated that authorization is based on users' access control. **Authorization** is critical in securing data of customers in cloud computing. Three out of six of the participants reiterated that authorization is needed based on users' access control, and it is a layered approach focused on roles and permission. This finding aligns with the research of Foresti et al. (2018). They indicated that authorization is permitted through regulatory access rights, which allows users to access varying portions of the data, as well as maintaining privacy and confidentiality. The research findings from this study support the DIT framework, in that DBAs should develop robust identity management infrastructure to ensure that the permission rights are granted or removed based on the user's roles and relationship to the organization. The participants voiced that authorization is a security strategy that works best to prevent data breaches in cloud computing infrastructure by safeguarding customer data. Organizational documents had policies and procedures focused on permission rights for enforcing authorization on data to minimize data breaches in cloud computing). Previous research supports these findings of access rights such as deletion, provisioning, and disabling of accounts should be based on the organization's approval process.

4.1.3 Encryption

The third subtheme was encryption. Encryption is a security strategy used to scramble or decode data utilizing access approaches characterized by traits (Ramu, 2018). **When participants were asked: What is your experience in securing data in cloud computing? Their topmost responses were using encryption and authentication to secure data to minimize data breaches. Pratt-Sensie (2020) findings show that five out of the six participants use encryption to secure data in cloud from unauthorized access. The participants also described how they encrypted data at rest and in transit. Literature aligns with the findings of the importance of the encryption process, which matches the description by Ramu (2018).** Encryption is a security strategy used to scramble or decode data utilizing access approaches characterized by traits (Ramu, 2018). Tankard (2017) confirmed the findings in the organizational documents that all PII data in the IaaS cloud computing should be encrypted to prevent data breaches. These findings of well-developed encryption warrant the confidentiality of the data, which was consistent with the responses from participants 1, 3, 4, and 5 of the study. Two out of the three participants in Case 1 and all three participants in Case 2 emphasized that encryption is an important security strategy to prevent data breaches in cloud computing. However, Participant 3 added that encryption uses multiple levels of protection and expressed concern about complex encryption. One of the participants from Case 2 reported that encryption is the first step to secure PII and minimize data breaches. The participants confirmed that their policies and procedures for encryption were guided by the National Institute of Standards and Technology (NIST) Cryptographic Algorithm and Module Validation Programs. These findings were corroborated by Lankford (2019), who indicated that Federal Information Processing Standards (FIPS) 140-2 is the means to certify an encryption algorithm. Tankard (2017) confirmed the findings in the organizational documents that all PII in the IaaS cloud computing should be encrypted to prevent data breaches. As a DIT, cloud computing technology as a new product has improved system performance making it appealing to large organizations that initially viewed it as a mediocre product (Crockett et al., 2013). Therefore, encryption is a pivotal security strategy.

4.1.4 Data Integrity and Privacy

The fourth subtheme is data integrity and privacy/confidentiality. This was the least used, well-defined security measures based on 2 out of 6 of the participants responses. The two participants who responded to the question "have you ever used security measures to prevent data breaches in cloud computing" stated that protecting data privacy in IaaS cloud computing is a key concern. Both participants emphasized use of mandates and use of Health Insurance Portability and Accountability Act (HIPAA) rules and regulations to secure PII. These findings are consistent with those in the literature reviewed by Sudha (2015). Sudha's (2015) research study supported the participants' experiences in using mandates HIPAA rules and regulations by stating that reasonable security requirements once implemented, addresses authentication, data anonymity, and user privacy, which will enhance data integrity and privacy of customers' PII. With the emergence of IT and cloud computing, data integrity and privacy of customers sensitive or PII information is now pivotal (Dhasarathan et al., 2015). Two of the six participants emphasized the importance of data integrity and privacy of PII. Participant 1 indicated that "protecting data privacy in private IaaS cloud computing is a major concern of customers". Participant 1 also added that

complying with mandates for the projects or receiving them depends on the data, whether it was either federal or healthcare data. In the experience of Participant 2, maintaining data integrity and privacy was achieved by adhering to the HIPAA rules and regulations of securing PII. Our review of three organizational documents verify that the security policies of these organizations were centered on HIPAA and NIST privacy requirements to maintain data integrity and privacy by using security measures such as multifactor authentication, encryption, and authorization. Using a multifactor authentication process such as a strong password and a PIV card will minimize the risk of hackers gaining access to PII (Goodman, 2016).

4.2 Limitations of Existing Security Controls in Cloud Computing

The second theme to emerge from the findings of Pratt-Sensie (2020) is the limitations of existing security controls in cloud computing. This theme developed from the participants' responses, the data analyzed from the organizational documents, and the findings from previous research studies and it consisted of four key subthemes: stringent passwords; human factors or errors; secure socket layers, and standardizing security approach. Figure 2 shows the participants responses to the use of the four subcategories of limitations to existing security measures.

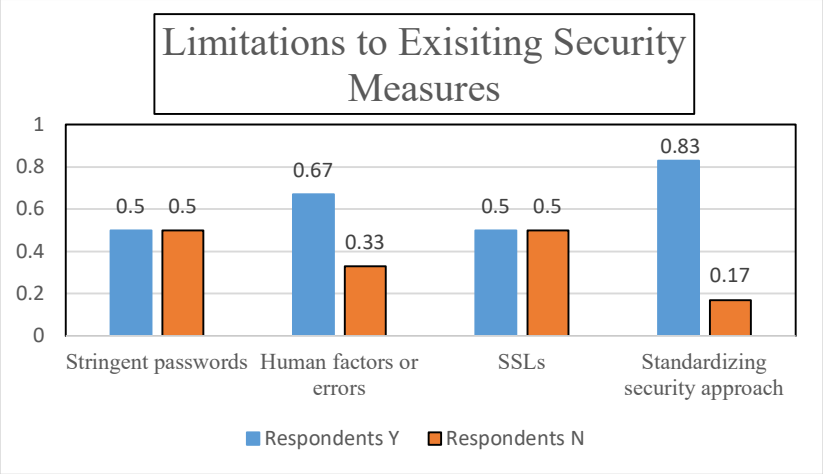

Figure 3. Limitations to existing security measures

4.2.1 Stringent Passwords

Stringent passwords have been the least effective means of protecting access by organizations, and it is also the least effective way to safeguard data from data breaches. Participant 1, when asked what the least effective security measures used in preventing cloud computing data breaches, responded that "stringent password controls used by the system are fine, those are secure. However, if you make password policy too stringent for the user, the user is just going to write it down and stick it up on their monitor". Participant 3 noted that "passwords should be changed every 60 days and the DBAs forcefully push the change". Participant 4 indicated that his organization focuses more on multifactor authentication instead of using stringent passwords. This feedback from the DBAs ties Pratt-Sensie and Miles (2020) study findings with findings from a similar study by Wei, Jiang, Zhang, and Ma (2017), who found that strong secure authentication is required to protect users' privacy. Pratt-Sensie (2020) findings also supports the works of Greengard (2015) that proposed the need of consumers wanting more robust protections instead of using stringent passwords. Further, Greengard (2015) believes that a password is a rendition of skeleton keys and organizations cannot keep on going down the path of failure. Two out of three of the participants in Case one expressed concern about the limitations of stringent passwords and this may expose data stored in the cloud to vulnerability. The two participants recommend that passwords must be changed forcefully every 60 days and the DBAs are responsible for this forceful push of the 60 days change generated from the system. However, one participant from Case two emphasized that his organization was more focused on the use of multi-factor authentication instead of the use of stringent passwords.

Methodological triangulation was achieved by reviewing the organizational documents that supported the subtheme. All the seven documents (HIPAA Security Rules, United States (US) Digital Guideline NIST SP 800-

53 Security and Privacy Controls for Federal Information Systems and Organizations, Information Security Policies: Data Breaches Response Policy, Information Security Policies: Third-Party Security Management, Information Security Policies: Security Incident Management Policy, Information Security Policies: Access Control Policy, Business Associate Agreement) addressed standards for the security of sensitive data, training of employees on the various types of security incidents that may trigger a data breach, and the process to follow when unauthorized system access is suspected or triggered. Our analysis of the organizational documents and participants' answers show that the security of data in cloud computing is pivotal in an organization, which leads to enhanced system performance and builds trust in customers.

As pivotal to the DIT theory, the research findings for this theme showed that the performance trajectory of cloud computing has changed the business logic in IT organizations. Weeks (2015) asserted that as new technology develops, it improves over time, and this meets the need of the large organizations in the business. Therefore, in the long run, the existing organizations are forced to change the way they conduct business as the disruption addressed the issues of the emerging market (Weeks, 2015). With continuous monitoring and adjustments, organizations have made strategic adjustments over time to change their business logic (Chen et al., 2016) by adopting storing data in the cloud instead of in traditional physical data centers.

4.2.2 Human Factors or Errors

The human factor is the second subtheme of the limitations of existing security controls in private IaaS cloud computing. In designing IT systems, human factors or errors should be considered as a challenge to prevent database security breaches. Participant 1 indicated that "in dealing with data security, human behavior needs to be considered by agencies or organizations in order to define policies that may prevent data breaches". Participant 1 further explained that he had one project where the password sequence had twenty-plus characters, and it involved so many symbols and weird characters that no one was going to remember it. Participant 1 made it easier for the program to figure the complex password. Participant 1 also opined that human-centered design is the key to an organization's security policy. Participant 2 noted that the human factor results in limitations of existing security controls because it is an internal threat that is ineffective to prevent cloud computing data breaches. Participant 4, when asked what your concerns are in implementing security measures and what has the organization done to rectify these concerns, responded that human errors are the leading cause of unauthorized access to data in cloud computing. Participant 5 also confirmed that human factors are the cause of most unauthorized access to PII. The results from this study supported the work by Sharma, Javadi, Si, and Sun (2016), who alluded that human errors are due to inexperience and believed that social engineering is the root cause of human errors. Previous studies by Ghafir et al. (2018) also supported the second theme reporting that, through social engineering, hackers can compromise database security through users' interactions. Safa, Solms, and Futcher (2016) further indicated that the human factor is a threat to data security. Two participants from each case concurred that human error is the leading threat to data security breaches. The findings of the researchers supported the second theme and are aligned with the DIT framework that guided this study. DIT not only enhances the performance of the database when adopted by organizations, but it also improves cost savings due to business logic change from using traditional physical storage like servers to storing data in the cloud (Ramachandran & Chang, 2016). DBAs should focus on successful security strategies such as multifactor authentication that would minimize the use of too stringent passwords that would minimize human errors.

Three documents (Information Security Policies: Data Breaches Response Policy, Information Security Policies: Security Incident Management Policy, Information Security Policies: Access Control Policy) were used in achieving methodological triangulation to enhance the reliability and validity of this theme. These documents focus on security policies and procedures when data breaches occur. In reviewing these three documents, methodological triangulation showed security strategies DBAs used. The documents guide DBAs on security awareness for effectively safeguarding data from data breaches. These documents support the theme and agree with the DIT because cloud computing has changed the business logic of how organizations now store data and protecting data in the cloud needs robust strategies to prevent data breaches. DBAs have to ensure that purposeful updates through staff training on security awareness are critical to minimize human errors.

4.2.3 Secure Socket Layer (SSL)

The secure sockets layer is the third subtheme of the limitations of existing security controls in private IaaS cloud computing of this study findings. SSL is important and aligns with DIT because it protects data in the cloud when it is transported to prevent data breaches since cloud computing data storage has security challenges that may compromise data integrity. Three out of the five participants responded that their concern in implementing security measures in cloud computing is SSL. The theme emerged from the responses of three participants and my analysis of all the seven documents provided by the organization. Methodological triangulation

was achieved with five out of the seven organizations' documents. Findings from the participants indicated that SSL certificates are required to protect sensitive data. This finding supports Shahzad (2014) who indicated that SSL certificates are pivotal in protecting sensitive data. Participant 1 noted that different levels of SSLs certificates are generated to authorize users' access to specific databases. Without this authorized SSL, data in transit may experience a middleman attack. Participant 3 specifically noted that SLS certificates are required to connect to the database and authorizing agencies need to sign the SSL certificates and provide the level of access it requires for each user. Participant 4 further emphasized that SSL is a certificate of authority that is system generated. Participant 4 also explained that his organization does not have SSL, but they can use open SSL to generate the certificates. This finding is consistent with the DIT because cloud computing as an evolving disruptive innovation brings with it many challenges such as data security that needs to be addressed to minimize data breaches. In the review of professional and academic literature, Ghazi et al. (2016) proposed that SSL is a strategy to protect encrypted data in transit so that the right person receives the data in the correct form. Singh and Chatterjee (2017) indicated that a middleman attack to the data occurs in transit due to a lack of security configuration of an SSL. Participants 1, 3, and 4 confirmed that for the overall data exchange, an SSL certificate must be in place to minimize data breaches. This finding aligned with Tipton et al. (2016). Tipton et al. (2016) noted that it is important for SSL certificates to be in place to secure data exchange. Two out of three participants from one case specified the use of SSL, while only one participant from the second case stated the use of SSL. The DBAs can use SSL to secure data when in transit to ensure it retains its correct form and prevent data loss.

4.2.4 Standardizing Security Approach

The standardizing security approach is the fourth subtheme of the limitations of existing security controls in private IaaS cloud computing. The responses from 5 participants and analysis from 3 organizational documents showed that the standardizing security approach is a limitation of existing security controls in cloud computing. Participant 1 indicated that DBAs complied with mandates provided by the organization, or they receive the mandates depending on the type of data they are working with such as PII., Participant 3 noted that in 10 years working as a DBA, he never saw standard security protocols in place to prevent data security breaches. Participant 3 added that some organizations may have their own customized standard protocol for their security system to prevent data security breaches. Participant 4 also confirmed that there is no standard security protocol in place to prevent database security breaches, and DBAs in his organization comply with laws or regulatory bodies like Health Insurance Portability and Accountability Act (HIPPA) and Information System Security Officer (ISSO) 2702 or 2701. Participant 5 also supported that there is no standard security protocol, and he added that there is "a delay in the federal posture when new technologies are adopted". Participant 6 described steps taken to prevent database security breaches such as blocking suspicious IP address and data encryption and was unable to confirm if there is a standard security protocol in place to prevent data security breaches. The literature reviewed showed that there are no standard security protocols in place. However, DBAs have to adhere to the security protocols that the organizations they work for use such as HIPPA, NIST or ISSO) 2702 or 2701.

The three organizational documents reviewed aligned with the 5 participants' responses that DBAs complied with regulatory bodies like ISO 2702/2701, HIPPA and NIST or customized security policies internal to the organizations. Recent literature supports the findings of this theme that there are no mandated standardized security policies in cloud computing to prevent data breaches (Hashem et al., 2015). These findings are aligned with Togan (2015), who noted that a lack of standardization of security solutions for cloud infrastructures has led to some organizations not implementing cloud computing. The findings of this research are consistent with those from previous studies regarding the existing security controls in cloud computing. The participants for this research mentioned the lack of national regulatory standards, however, several of the participants were using the standards of regulatory bodies such as ISSO and NIST.

Security is a pivotal challenge when storing data in cloud computing and the responses from the participants alluded to the lack of standardized security controls in cloud computing. The framework supported the findings as DIT promoted redefining marketplace expectations by physically changing the traditional way of storing sensitive data in cloud computing (Yu et al., 2017). Despite the lack of standardization in cloud computing, the literature supports the participants responses and security remains a challenge. DBAs need to develop well-defined security strategies to prevent database breaches in cloud computing.

5. Discussion

The study findings by Pratt-Sensie (2020) show that DBAs can develop strategies to prevent data breaches in cloud computing once a security threat is identified and analyzed, which supports the disruptive innovation theory (DIT). The theory states that DBAs embrace DIT as an opportunity and position the potentials of the organization toward change (Kranz et al., 2016; Osiyevskyy & Dewald, 2015). The limitations of this study were focused primarily in one geographic location, Baltimore, Maryland. Repeating the study in different geographical regions

of the United States based on their regulations and security requirements and using a different conceptual framework and methodology will benefit organizations and IT professionals. This study added to the existing security strategies literature, but additional research is warranted due to the small sample size of qualified DBAs used in the study. Future work may consider the exploration of security strategies with larger sample sizes or larger organizations. This study has contributed to the body of literature on security strategies on cloud computing, but may also prove beneficial to the healthcare industry, academic communities, and banking sectors.

Finally, the results of this study offers recommendations on important issues that need to be addressed in the IT marketplace. Based on the literature review and the collected data of this study, recommendations for future research topics are highlighted:

- researchers should explore different encryption approaches to identify the optimal encryption approach that delivers top data security to cloud environments;
- further research needs to explore the barriers preventing leaders from taking proactive security approaches to invest in innovative security strategies that keep them relevant and prevent data breaches in organizations; and
- research should explore the key components to understanding the motivations and triggers of positive behavior change that minimizes external and internal data breaches in organizations.

6. Conclusion

There is an ongoing need for data security in cloud computing due to the increase in external threats of sensitive data. Until security issues are resolved, organizations should be cautious by weighing the security dangers against the advantages of cloud computing, by implementing well-defined controls and strategies (Tankard, 2015). Moreover, since cloud computing data security is still a challenge, future research directions should explore the efficiency of three-factor authentication versus two-factor authentication to optimally improve cloud security. Finally, fog computing should also be explored since it provides added security in public cloud by profiling the user's behavior through a decoy technique (Bhatia et al., 2020). Cloud computing may experience a great rise in its adoption if security challenges are addressed and resolved to increase customers' trust and confidence.

The limitation placed on this study was using relatively small number of experienced DBAs from two small business IT organizations in Baltimore, Maryland. The findings from this study were significant and supported by the organizational documents and recent literature on cloud computing security strategies consistent with the DIT framework of this study. As noted in the DIT framework, cloud computing is a disruptive technology and this disruptive trend is due to its security challenges, which need to be addressed and resolved. The findings of this study should have greater applicability to DBAs, as well as other IT organizations that are seeking to use effective security strategies to improve collaboration and increase customers trust in storing their sensitive data in cloud computing.

References

Alamode., & Alamode,, W. (2016). *Journal of Information Systems & Planning, 8*(19), 41-60. Retrieved from www.intellectbase.org/jounals.php

Ali, M., Khan, S. U., & Vasilios, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305, 357-383. doi:10.1016/j.ins.2015.01.025

Aminase, M. (2018). Confidentiality, integrity and availability – finding a balanced IT framework. *Network Security, 5*, 9-11. doi:10.1016/S1353-4858(18)30043-6

Ardagna, C. A., Asal, R., Damiani, E., & Quang, H. V. (2015). From security to assurance in the cloud: A survey. *ACM Computing Surveys, 48*(1), 2-2–50. doi:10.1145/2767005

Arki, O., Zitouni, A., & Dib, A. T. E. (2018). A multi-agent security framework for cloud data storage. *Multiagent & Grid Systems, 14*(4), 357–382. doi:10.3233/MGS-180296

Barrow, P., Kumari, R, & Manjula, R. (2016). Security in cloud computing for service delivery models: challenges and solutions. *Journal of Engineering Research and Applications, 6*(4), 76-85

Baskerville, R. (2011). Individual Information Systems as a Research Arena. *European Journal of Information Systems 20*(20), 251-254. doi:10.1057/ejis.2011.8

Bayramusta, M., & Nasir, V. A. (2016). A fad or future of IT?: A comprehensive literature review on the cloud computing research. *International Journal of Information Management*, *36*(4), 635-644.

Bhatia, M., Sharma, S., Bhatia, S., & Alojail, M. (2020). Fog computing mitigate limitations of cloud computing. *International Journal of Recent Technology and Engineering 8(5),* 1732-1736. doi:10.35940/ijrte.e6199.018520

Bohnsack, R., & Pinkse, J. (2017). Value propositions for disruptive technologies: Reconfiguration tactics in the case of electric. *California Management Review*, *59*(4), 79-96. doi:10.1177/0008125617717711

Carter, N., Bryant-Lukosius, D. A., Blythe, J., & Neville, A. J. (2014). The Use of Triangulation in Qualitative Research. *Oncology Nursing Forum*, *41*(5), 545-547.

Chen, C., Guo, R., & Zhang, J. (2016). The d-day, v-day, and bleak days of a disruptive technology: A new model for ex-ante evaluation of the timing of technology disruption. *European Journal of Operational Research*, *251*(2), 562-574. doi:10.1016/j.ejor.2015.11.023

Choong, P., Hutton, E., Richardson, P., & Rinaldo, V. (2016). Assessing the cost of security breach: A marketer's perspective. *Journal of Marketing Development and Competitiveness, 11*(1), 59-68. Retrieved from http://www.na-businesspress.com

Christensen, C. M. (1997). *The innovators dilemma: When new technologies cause great firms to fail.* Boston, MA: Harvard Business School Press.

Christensen, C. M. (2011). *The innovator's dilemma: The revolutionary book that will change the way you do Business.* New York, NY: HarperBusiness.

Cusack, B., & Ghazizadeh, E. (2016). Evaluating single sign-on security failure in cloud services. Business Horizons, 59(6), 605-614. doi:1016/jbushor.2016.08.002

Davoll, B. (2017). Do you have what it takes to be a world-class DBA? Database *Trends & Applications, 31*(5), 9-10.

Dayıo˘glu, Z. N., Kiraz, M. S., Birinci, F., & Akın, I. H. (2014). Secure database in cloud computing: CryptDB revisited. *International Journal of Information Security Science*, *3*(1), 129-148.

de Fuentes, J. M., González-Manzano, L., Tapiador, J., & Peris-Lopez, P. (2017). Pracis: Privacy-preserving and aggregatable cybersecurity information sharing. *Computers & Security*, *69*, 127-141.

Fagerholm, F., Kuhrmann, M., & Münch, J. (2017). Guidelines for using empirical studies in software engineering education. *PeerJ Computer Science*, *3*(1), 131-166. doi:10.7717/peerj-cs.

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90-110. doi:10.1016/j.cose.2014.03.004

Foresti, S., Paraboschi, S., Pelosi, G., & Samarati, P. (2018). Enforcing authorizations while protecting. *Journal of Computer Security*, *26*, 143–175. doi:10.3233/JCS-171004

Gale, S. F. (2018). Under lock and key. *PM Network*, 32(10), 54–61. Retrieved from https://pmi.org

Garg, N., & Bawa, S. (2016). Comparative analysis of cloud data integrity auditing protocols. *Journal of Network & Computer Applications, 66*, 17–32. doi:10.1016/j.jnca.2016.03.010

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *The Qualitative Report*, *20*(11), 1772. doi:10.4135/9781412950589.n885

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S.,… Jabbar, S. & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *Journal of Supercomputing*, *74*(10), 4986. doi:10.1007/s11227-018-2337-2

Ghazi, Y., Masood, R., Rauf, A., Shibli, M. A., & Hassan, O. (2016). DB-SECaaS: A cloud-based protection system for document-oriented no SQL databases. *Eurasip Journal on Information Security, 16*(1), 1-17. doi:10.1186/s13635-016-0040-5

Greengard, S. (2015). Why passwords are skeleton keys of the 21st century. *CIO Insight*, 2. Retrieved from https://www.cioinsight.com

Hashem, I., Yaqoob, I., Anuar, N., Mokhtar, S., Gani, A., & Khan, S. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems, 47*, 98-115. doi:10.1016/j.is.2014.07.006

He, L., Huang, F., Zhang, J., Liu, B., Chen, C., Zhang, Z., Yang, Y., Lu, W. (2016). Dynamic secure interconnection for security enhancement in cloud computing. *International Journal of Computers Communications & Control, 11*(3), 348-357. doi:10.15837/ijccc.2016.3.504

Heatherly, R. (2016). Privacy and security within biobanking: The role of information technology. *Journal of Law, Medicine & Ethics, 44*(1), 156–160. doi:10.1177/1073110516644206

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of basic and clinical pharmacy, 5*(4), 87. doi:10.4103/0976-0105.141942

Jian, S., Dengzhi, L., Qi, L., Debiao, H., & Xingming, S. (2017). An enhanced cloud data storage auditing protocol providing strong security and efficiency for smart city. *Journal of Information Science & Engineering, 33*(4), 923-938. doi:10.6688/JISE.2017.33.4.

Jim, R. (2013). Multifactor authentication: Its time has come. *Technology Innovation Management Review*, 51-58. . Retrieved from www.timreview.ca

Kaaniche, N., & Laurent, M. (2017). Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. *Computer Communications*, 111, 120-141. doi:10.1016/j.comcom.2017.07.006

Kaltenecker, N., Hess, T., & Huesig, S. (2015). Managing potentially disruptive innovations in software companies: Transforming from On-premises to the On-demand. *Journal of Strategic Information Systems*, 24234-250. doi:10.1016/j.jsis.2015.08.006

King, A. A., & Baatartogtokh, B. (2015). How useful is the theory of disruptive innovation? *MIT Sloan Management Review*, (1), 77. doi: 10.3138/jsp.48.1.17

Kranz, J. J., Hanelt, A., & Kolbe, L. M. (2016). Understanding the influence of absorptive capacity and ambidexterity on the process of business model change – the case of on-premise and cloud-computing software. *Information Systems Journal*, *26*(5), 477-517. doi:10.1111/isj.12102

Kumaril, K., & Mrunalini, M. (2018). A survey on big data security: Issues, challenges and techniques. *International Journal of System and Software Engineering, 6*(2), 24-36. doi:10.29042/2018-3290-3293

Maluf, D. A., Sudhaakar, R. S., & Choo, K. R. (2018). Trust errosion: Dealing with unknown-unknowns in cloud security. *IEEE Cloud Computing, 5*(4), 24-32. doi:10.1109/MCC.2018.043221011

McKendrick, J. (2018). Managing the hybrid future: From databases to clouds. *Database Trends & Applications, 32*(1), 12–14. retrieved from https://http://www.dbta.com/

Moon, Y. J., Choi, M., Armstrong, D. (2018). The impact of relational leadership and social alignment on information security system effectiveness in Korean governmental organizations. *International Journal of Information Management*, *40*, 54-66. doi:10.1016/j.ijinfomgt.2018.01.001

Noguerol, L. O., & Branch, R. (2018). Leadership and Electronic Data Security within Small Businesses: An Exploratory Case Study. *Journal of Economic Development, Management, IT, Finance & Marketing, 10*(2), 7–35.

Osiyevskyy, O., & Dewald, J. (2015). Explorative versus exploitative business model change: The cognitive antecedents of firm-level responses to disruptive innovation. *Strategic Entrepreneurship Journal, 9*(1), 58-78. doi:10.1002/sej.1192

Parisha, P. K., Puneet, S., & Sheenu, R. (2017) Data partitioning technique in cloud: a survey on limitation and benefits. *International Journal of Engineering Research And Applications,* 7(7), 1-6. doi:10.9790/9622-0707100106

Pratt-Sensie, A. (2020). Security strategies to prevent data breaches in infrastructure as a service cloud computing. *Walden Dissertations and Doctoral Studies 8572*. Retrieved from https://scholarworks.walden.edu/dissertations/8572

Ramachandran, M., & Chang, V. (2016). Towards performance evaluation of cloud service providers for cloud data security. *International Journal of Information Management, 36*(4), 618-625. doi:10.1016/j.ijinfomgt.2016.03.005

Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science, 48*, 204-209. doi:10.1016/j.procs.2015.04.171

Schniederjans, D. G., & Hales, D. N. (2016). Cloud computing and its impact on economic and environmental performance: A transaction cost economics perspective. *Decision Support Systems, 86*, 73-82. doi:10.1016/j.dss.2016.03.009

Safa, N. S., Solms, R. V., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud and Security, 2*, 15-18. doi:10.1016/S1361-3723(16)30017-3

Shahzad, F. (2014). State-of-the-art survey on cloud computing security challenges, approaches and solutions. *Procedia Computer Science, 37*, 357-362. doi:10.1016/j.procs.2014.08.053

Sharma, Y., Javadi, B., Si, W., & Sun, D. (2016). Reliability and energy efficiency in cloud computing systems: Survey and taxonomy. *Journal of Network and Computer Applications, 74,* 66-85. doi:10.1016/j.jnca.2016.08.010

Silva, L., Barbosa, P., Marinho , R. & Brito, A. (2018). Security and privacy aware data aggregation on cloud computing. *Journal of Internet Services and Applications, 9*(1), 1-13. doi:10.1186/s13174-018-0078-3

Sindhu, R., & Mushtaque, M. (2014). A new innovation on user's level security for storage data in cloud computing. *International Journal of Grid & Distributed Computing, 7*, 213-219. doi:10.14257/ijgdc.2014.7.3.22

Simon, M. (2019). Two-factor authentication: How to choose the right level of security for every account. *PC World, 7*(5), 91-98. Retrieved from https://www.pcworld.com

Singh, A., & Chatterjee, K. (2017). Review: Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications, 79*, 88-115. doi:10.1016/j.jnca.2016.11.027

Sookhak, M., Gani, A., Talebian, H., Akhunzada, A., Khan, S. U., Buyya, R., & Zomaya, A. Y. (2015). Remote data auditing in cloud computing environments: a survey, taxonomy, and open issues. *ACM Computing Surveys*, (4), 65. https://doi-org.ezp.waldenulibrary.org/10.1145/2764465

Sookhak, M., Yu, F. R., & Zomaya, A. Y. (2018). Auditing big data storage in cloud computing using divide and conquer tables. *IEEE Transactions on Parallel & Distributed Systems, 29*(5), 999–1012. doi:1109/TPDS.2017.2784423

Subha, T., & Jayashri, S. (2017). Public auditing scheme for data storage security in cloud computing. *Journal of*

Information Science & Engineering, 33(3), 773–787. doi:10.6688/JISE.2017.33.3.11

Tankard, C. (2017). Encryption as the cornerstone of big data security. *Network Security*, 2017, (3), 5-7. doi:10.1016/S1353-4858(17)30025-9

Tchernykh, A., Schwiegelsohn, U., Talbi, E., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science, 36*, 1-9. doi:10.1016/j.jocs.2016.11.011

Tinkler, L., Smith, V., Yiannakou, Y, & Robinson, L. (2018). Professional identity and the clinical research nurse: Aaqualitative study exploring issues having an impact on participant recruitment in research. *Journal of Advanced Nursing, 74*(2), 318-328. doi:10.1111/jan.13409

Tipton, S. J., Forkey, S., & Choi, Y. B. (2016). Toward proper authentication methods in electronic medical record access compliant to HIPAA and C.I.A. *Triangle, 1996*, 1–9. doi:10.1007/s10916-016-0465-x

Togan, M. (2015). Aspects of security standards for cloud computing. *MTA Review, 25*(1), 31-44. Retrieved from https://www.worldcat.org/title/mta-review/oclc/882231145

Wagenseil, P. (2020). Zoom security issues: Here's everything that's gone wrong (so far). *Toms guide*, 1-3. Retrieved July 9th, 2020, from https://www.tomsguide.com/news/zoomsecurity-privacy-woes

Wang, F., Xu, G., Xu, G., Wang, Y., & Peng, J (2020). A robust IoT-based three-factor authentication scheme for cloud computing resistant to session key exposure. *Wireless Communication and Mobile Computing, 2020,* 1-15. doi:101155/2020/3805058

Weeks, M. R. (2015). Is disruption theory wearing new clothes or just naked? Analyzing recent critiques of disruptive innovation theory. *Innovation: Management, Policy & Practice*, *17*(4), 417-428. doi:10.1080/14479338.2015.1061896

Wei, F., Jiang, Q., Zhang, R., & Ma, C. (2017). A Privacy-preserving multi-factor authenticated key exchange protocol with provable security for cloud computing. *Journal of Information Science & Engineering*, *33*(4), 907–921. doi:10.6688/JISE.2017.33.4.3

Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons, 58*(6), 615-624. doi:10.1016/j.bushor.2015.06.005

Xiang, S., & Zhu, Z. (2019). Dynamic access control of encrypted data in cloud computing environment. *International Journal of Performability Engineering,* 15(3), 969-976. doi:10.23940/ijpe.19.03.p26.969976

Xu, Z., Wu, L., Khurram, M., Choo, K. R., & He, D. (2017). A secure and efficient public auditing scheme using RSA algorithm for cloud storage. *Journal of SuperComputing, 73*, 5285–5309. doi:10.1007/s11227-017-2085-8

Ye, K., & Ng, M. (2019). Intelligent encryption algorithm for cloud computing user behavior featured data. *Journal of Intelligent & Fuzzy Systems, 35*, 4309-4317. doi:103233/JIFS-169751

Yesilyurt, M., & Yalman, Y. (2016). New approach for ensuring cloud computing security: using data hiding methods. *Sadhana, 41*(11), 1289-1298. doi:10.1007/s12046-016-0558-8

Yu, Y., Cao, R. Q., & Schniederjans, D. (2017). Cloud computing and its impact on service level: A multi-agent simulation model. *International Journal of Production Research,* 55(15), 4341-4353. doi:10.1080/00207543.2016.1251624