End-User Cloud Data Storage Experiences, Challenges, and Security Perceptions of the Emerging Technologies Security Tools among Small Businesses

Juanita Carson-Irvin Stewart
Capella University, Minneapolis, Minnesota, USA

[Abstract] The purpose of this qualitative study was to explore small business end-users' experiences and challenges with cloud data storage and security perceptions of cloud emerging technologies security tools. Cloud data storage security is critical to business success, as more small businesses are moving to cloud data storage. The gap identified in the literature was the perceptions and experiences of end-users' trust in cloud data storage. The central research question was: How do the perceptions and experiences of challenges with cloud data storage and security perceptions of cloud emerging technologies security tools affect the trust of small business end-users in cloud data storage? An exploratory generic qualitative study design was utilized to explore the cloud data storage experiences, challenges, and security perceptions of the emerging technologies' security tools among end-users of small businesses. The target population was 20 small business end-users from four different types of small businesses with at least one year of cloud experience within a South Atlantic state. The study findings addressed the experiences and challenges of small business end-users with cloud data storage and security perceptions of cloud emerging technologies security tools. The results found that all 20 end-users reported a lack of trust in data storage cloud security. The conclusion is that end-users questioned the protection of cloud storage data.

[Keywords] big data, data storage, cloud data security, cloud service provider, emerging technology security tools

Introduction

The security of data is a challenge for many organizations. New security concerns emerge weekly because of the rapid pace of change in the development and use of hardware and software. Cloud data storage security is critical to business success, as more small businesses move to cloud data storage. The purpose of this qualitative research was to explore the small business end-user experiences and challenges with cloud data storage and security perceptions of cloud emerging technologies security tools. The gap identified in the literature was the perceptions and experiences of end-user trust in cloud data storage.

The cloud is a collection of computers and servers that are accessible via the Internet (Bhandayker, 2019), which provides businesses a definite advantage, as end-users can access the data anywhere and at any time (Abeykoon, Kamburugamuve, Govindrarajan, Wickramasinghe, Widanage, Perera, ... & Von Laszewski, 2019). Businesses that are moving data to the cloud must adjust to security policies and privacy requirements (Jaatun, Tondel, Moe, Cruzes, Bernsmed & Haugset, 2018; Topper, 2018) while attempting to achieve proper security with a mixture of technology, process, and people (Aljawarneh, 2020). The lack of security creates serious security issues and subsequent data exposure. Previous researchers found and addressed different cloud security issues, such as knowledge management security concerns in cloud computing (Bhise & Latif, 2020; Gunadham & Kuacharoen, 2019), cloud computing security issues (Benjelloun & Lahcen, n.d.), and cloud systematic identification threats (Hong, Nhlabatsi, Kim, Hussein, Fetais, & Khan, 2019).

The problem is that the protection of data in the cloud is questionable (Bhardwaj et al., 2016; Bhise & Latif, 2020), which has created distrust among end-users (Oliveira, 2018). End-users are identified as system operators and system administrators for this study. End-users are one of the highest security risks, and yet, when end-users lose confidence in providers, the likelihood of changing providers increases, thereby decreasing the business of the provider while increasing the security risks for the end-user as the data is transferred. The views of end-users around cloud data security are essential both from a data security and a business perspective (Mahalle, Yong, Tao & Shen, 2018). There are end-user vulnerabilities and insider attack risks with the cloud. End-user pre-employment screening and enhancing internal security are two preventable measures that prevent employee insider attacks if followed (Hosseinzadeh, Ghafour, Hama, & Khoshnevis, 2020).

Business Technical Problem

Up until 2018, the cloud emerging technologies' security tools were not sufficiently safeguarding data in the cloud data storage (Jaatun et al., 2018). For example, once data is moved to the cloud for storage, a malicious tool can be installed to intercept, monitor, and interfere with online transactions in a credible organization. The software security tools are inadequate and function as ad-hoc tools that protect the network and host levels (Aljawarneh, 2020).

End-users who have an extended relationship with cloud providers tend to trust those services that allows for less distrust (Jaatun et al., 2018; Ou & Beckers, Van Doorn, & Verhoef, 2018). Cloud data security depends on the cloud data storage provider (Benjelloun & Lahcen, n.d.). The cloud provider sharing protection, advantage, and disadvantage can increase end-user cloud services' trust and confidence. End-users need to trust cloud providers to ensure the security of the data in the cloud (Jaatun et al., 2018).

The purpose of this qualitative study was to explore small business end-users’ experiences and challenges with cloud data storage and security perceptions of cloud emerging technologies security tools. Cloud data storage security is critical to business success, as more small businesses move to cloud data storage.

Assumptions, Limitations, and Delimitations

Assumptions

The primary assumption in using an exploratory generic qualitative study is that the participants volunteer for the research, have previous exposure to business data in the cloud, and are familiar with business data. Additionally, an assumption is that participants answered all questions truthfully and honestly. Also, the researcher assumed that the research question might be answered using the exploratory generic qualitative study research method to identify themes related to challenges faced by businesses adopting cloud data storage for big data (Ghauri, Gronhaug, & Strange, 2020).

Limitations

The primary limitation of this study was relying on participants’ experiences with data in cloud data storage, challenges, and emerging technologies security tools. Ghauri et al. (2020) stated that all analysis contains limitations. The research question used in this study was designed for IT end-users because they are the best source of information for the study.

Delimitations

There were some delimitations of the study. The researcher acknowledges that the small sample size might not have been generalizable to the broader population. The study was delimited within a South Atlantic state, a geographic region of the United States. Areas outside a South Atlantic state were not included due to time and distance considerations.

An additional delimitation was the literature review, which identified studies on data and cloud storage; however, cloud data storage and components were not explored in this study. Finally, the experiences of supervisors and leaders of IT end-users were not included in the study. The theory of planned behavior (TPB) was the theoretical orientation of the current research, as it has emerged as one of the most popular theories for understanding human behavior in IT since it predicts an individual’s intention to engage in activities at a specific time and place (Roos & Hahn, 2019). Since the participants were IT end-users only, TPB was not used to explore the behavior of supervisors and leaders in the current study.

Literature Review

The research question guided the parameters of the literature review. The researcher used a keyword search approach to identify related articles, utilizing a multisource search strategy. The literature revealed a large quantity of research conducted on data and the cloud; however, there was very little knowledge of small business end-users cloud data storage experiences, challenges, and perceptions of emerging technologies security tools (Mohapatra et al., 2015).

Abeykoon et al. (2019) found the use of data in the cloud has increased significantly since 2015. Big data is the volume of collected knowledge that continues to increase as business end-users establish ways to manage and manipulate data in the cloud (Abeykoon et al., 2019). Organizations have obtained large amounts of data, and the cloud has become a critical storage location that has caused the cloud to expand. The increase in data volume in the cloud changes the data's characteristics and how data is collected, stored, and retrieved (Abeykoon et al., 2019). Once data is in the cloud, IT end-users can access the data during all times of the day, regardless of the business end-user location (Abeykoon et al., 2019).

Cloud data storage is a collection of thousands of digital data storage tools grouped by a network, distributed file systems, and other storage middleware to provide cloud data storage service for IT end-users. The conventional structure of cloud data storage contains a digital data storage resource collection, distributed file system, service level agreements, and data service interfaces. Universally, the stored data can be divided into logical and physical functions, boundaries, and connections to provide additional interactions and compatibilities. Cloud data storage is inclined to combine with cloud data security to produce extra protection (Atan et al., 2018).

Breaches, leaks, and hacked data are all security risks that can threaten businesses and undermine a business's confidence in using the cloud for data storage. Jaatun et al. (2018) addressed participants' experience regarding developing a connection between accountability, security, trust, and participants' views and procedures regarding faith and risk by evaluating the cloud service framework's expected services. Jaatun et al. (2018) found that additional research is required to address the cloud data storage provider's complete cloud process, which includes accountability and consequences.

The lack of accountability for monitoring and managing data is an essential concern, which impacts the end user's trust (Jaatun et al., 2018). The cloud providers' clouds distribute the data workload in a self-aggregating way to reconfigure the data load balancing. The data distribution in the cloud moves between several clouds across different cloud data storage providers to supply end-users with quality cloud storage service. The data movement prioritization takes place based on the time required from the shortest to the most extended task. After the achievement of the data movement task, redistribution takes place (Cusack & Ghazizadeh, 2018).

Analysis of Research Question

The research question for this study is: How do the perceptions and experiences of challenges with cloud data storage and security perceptions of cloud emerging technologies security tools affect the trust of small business end-users in cloud data storage? Protection of data in the cloud is questionable, which has created distrust among end-users who are identified as system operators and system administrators (Bhardwaj et al., 2016). The following researcher-designed structured interview questions (IQ) were developed from the initial question to ask each participant:

IQ1: Please elaborate on the cloud data storage used by the organization
IQ1(a): Please talk about any challenges with cloud data storage.
IQ2: Please elaborate on experiences with cloud data storage?
IQ3: What are the perceptions of the small business process for cloud data storage security?
IQ3(a): Please describe the organization's cloud data storage security technologies.
IQ3(b): Please explain the role in the decision-making process of the cloud data storage.
IQ4: Talk about the concerns and experiences with data security in the cloud.
IQ5: Please share the perceptions of cloud security.
IQ6: What are some security perceptions of the emerging technologies' security tools?

IQ7: Please explain cloud data storage experiences and how the trust process is affected?

Participant Recruitment

Participants were recruited using social media. A recruiting advertisement was distributed via Linkedin, and word-of-mouth to locate people who use the cloud. The advertisement included a short description of the purpose of the research, and the activities participants were engaged in. Based on the study criteria, the *inclusion criteria* to participate in the study were small business IT end-users who (a) were cloud data storage IT end-users, (b) had a minimum of 1 year of experience working with cloud data storage, (c) worked in a South Atlantic state, and (d) worked for a small business that did not employ more than 100 employees.

Results

The results and insights in this study serve as relevant indicators of perceptions and experiences of end-users using the cloud working for a small business with no more than 100 employees with at least one year of work experience with the cloud. The research exposed that 20 out of 20 end-users lacked the trust of the data storage cloud security and questioned the protection of the data in the data storage cloud. End-users' experiences are shown in Table 1.

Table 1
Challenges with the Cloud

Security challenges	Challenges when using different applications	Not aware of merging tools
20 out of 20	12 out of 20	16 out of 20

End-users were only aware of one emerging technology security tool, which was two-factor authentication. Small businesses were hesitant to trust that their data was protected in the cloud. Companies have a responsibility to make sure that the data is protected or access to the data is locked down. End-users thought Apple, Microsoft, and Google had sound security practices. The study provides end-user perspectives and experiences regarding challenges with cloud data storage. Security perceptions of cloud-emerging technologies security tools affect the small business end-users trust in cloud data storage. End-users were only aware of one emerging technology security tool, which was two-factor authentication. The majority of the interviewed end-users thought there was a privacy concern. Small businesses are hesitant to trust that their data is protected in the cloud. The company has a responsibility to make sure that the data is protected or access to the data is locked down. End-users' experiences are shown in Table 2.

Table 2
Understanding Security Practices

No concerns since security was outsourced	Used commercial security products	Did not know much about security	Two-factor authentication improved security
16 out of 20	16 out of 20	19 out of 20	20 out of 20
Checked data remotely	Unaware of mobile security tools	Complicated emerging technologies tools	Knowledge of security tools to manage data
16 out of 20	12 out of 20	6 out of 20	20 out of 20

Conclusion and Recommendations

The target population was 20 small business end-users within a South Atlantic state, who contributed to the collection of the data needed to address the research question. While the participants of this qualitative study were limited, the data was consistent. The study findings addressed the experiences and challenges of small business end-users with cloud data storage and security perceptions of cloud emerging technologies security tools. The researcher recommends further research, including expanding the locations of participants, an extensive quantitative study, and a participants group study.

References

Alenezi, A., Atlam, H. F., & Wills, G. B. (2019). Experts reviews of a cloud forensic readiness framework for organizations. *Journal of Cloud Computing*, *8*(1), 1-14. doi.org/10.1186/s13677-019-0133-z

Aljawarneh, S. A. (2020). Reviewing and exploring innovative ubiquitous learning tools in higher education. *Journal of computing in higher education*, *32*(1), 57-73. doi.org/10.1007/s10639-015-9407-3

Atan, R., Talib, A. M., & Murad, M. A. A. (2018). Formulating a security layer of cloud data storage framework based on multi agent system architecture. *GSTF Journal on Computing*, *1,* 120-124. doi:10.5176_2010-2283_1.1.20

Beckers, S. F., Van Doorn, J., & Verhoef, P. C. (2018). Good, better, engaged? The effect of company-initiated customer engagement behavior on shareholder value. *Journal of the Academy of Marketing Science*, *46*(3), 366-383. doi.org/10.1007/s11747-017-0539-4

Benjelloun, F. Z., & Lahcen, A. A. (n.d.). Big data security: Challenges, recommendations and solutions. In *Information Resources Management Association* (eds.), *Web Services: Concepts, Methodologies, Tools, and Applications* (pp. 25-38). IGI Global.

Bhandayker, Y. R. (2019). An overview: Security solutions for cloud environment. *International Journal for Scientific Research and Development*, *7*, 1596-1598. Retrieved from: https://www.researchgate.net/publication/332896632

Bhardwaj, A., Subramanyam, G., Avasthi, V., & Sastry, H. (2016). Review of solutions for securing end-user data over cloud applications. *International Journal of Advanced Computer Research, 6*, 222-229. doi:10.19101/IJACR.2016.626005

Bhise, A. S., & Latif, P. M. (2020). Secure cloud storage system by integrating trust with role based access control and cryptographic algorithm. In *Techno-Societal, 2018*, 87-97. Cham: Springer International Publishing doi:10.1007/978-3-030-16962-6_10.

Cearnau, D. (2018). Cloud computing: Emerging technology for computational services. *Informatica Economica, 22*(4*)*, 61-69. doi:10.12948/issn14531305/22.4.2018.05

Cusack, B., & Ghazizadeh, E. (2018). Satisfying secure load balancing expectations in the cloud. *Twenty-fourth Americas Conference on Information Systems, New Orleans, LA., 1-10.* Retrieved from: https://aisel.aisnet.org/amcis2018/Security/Presentations/26/

Garrison, G., Rebman, C. M., Jr., & Kim, S. H. (2018). An identification of factors motivating individuals' use of cloud-based services. *Journal of Computer Information Systems*, *58*(1), 19-29. doi:10.1080/08874417.2016.1180653

Ghauri, P., Gronhaug, K., & Strange, R. (2020). *Research methods in business studies*. Cambridge University Press.

Gunadham, T., & Kuacharoen, P. (2019). Security concerns in cloud computing for knowledge management systems. *Journal of Applied Statistics and Information Technology*, *1*, 52-60. Retrieved from https://ph02.tci-thaijo.org/index.php/asit-journal/article/view/164779/119399

Hong, J. B., Nhlabatsi, A., Kim, D. S., Hussein, A., Fetais, N., & Khan, K. M. (2019). Systematic identification of threats in the cloud: A survey. *Computer Networks*, *150*, 46-69. doi:10.1016/j.comnet.2018.12.009

Hosseinzadeh, M., Ghafour, M. Y., Hama, H. K., Vo, B., & Khoshnevis, A. (2020). Multi-objective task and workflow scheduling approaches in cloud computing: a comprehensive review. *Journal of Grid Computing*, 1-30. doi.org/10.1007/s10723-020-09533-z

Jaatun, M. G., Tondel, I. A., Moe, N. B., Cruzes, D. S., Bernsmed, K., & Haugset, B. (2018). Accountability requirements in the cloud provider chain. *Symmetry, 10*, 1-20. doi:10.3390/sym10040124

Mahalle, A., Yong, J., Tao, X., & Shen, J. (2018). Data privacy and system security for banking and financial services industry based on cloud computing infrastructure. In *2018 IEEE 22nd International Conference on Computer Supported Cooperative Work in Design (CSCWD)* (pp. 407-413). IEEE. doi:10.1109/CSCWD.2018.8465318

Mohapatra, S., Paikaray, J., & Samal, N. (2015). Future trends in cloud computing and big data. *Journal of Computer Sciences and Applications, 3*, 137-142. doi:10.12691/jcsa-3-6-6

Noshy, M., Ibrahim, A., & Ali, H. A. (2018). Optimization of live virtual machine migration in cloud computing: A survey and future directions. *Journal of Network and Computer Applications*, *110*, 1-10. doi.org/10.1016/j.jnca.2018.03.002

Oliveira, A. S. (2018). Modelling trust and risk for cloud services. *Journal of Cloud Computing*, *7*(4), 1-16. doi:10.1186/s13677-018-0114-7

Philip, L., & Williams, F. (2019). Remote rural home based businesses and digital inequalities: Understanding needs and expectations in a digitally underserved community. *Journal of Rural Studies*, *68*, 306-318.doi.org/10.1016/j.jrurstud.2018.09.011

Roos, D., & Hahn, R. (2019). Understanding collaborative consumption: An extension of the theory of planned behavior with value-based personal norms. *Journal of Business Ethics*, *158*(3), 679-697. doi.org/10.1007/s10551-017-3675-3

Topper, J. (2018). Compliance is not security. *Computer Fraud & Security*, *2018*, 5-8. doi:10.1016/S1361-3723(18)30022-8

Appendix A

Definition of Terms

The use of technical and specific terms for the study are listed as follows.

Big data. Big data is the volume of collected knowledge that continues to increase as end-users establish ways to manage and manipulate the knowledge (Abeykoon et al., 2019).

Business. A business is a cloud customer that sustains a relationship with service cloud providers as an organization or individual (Jaatun et al., 2018).

Cloud. Cloud is defined as a global repository of servers for digital data that are accessed via the Internet, which enables computing as a service (Bhandayker, 2019; Bhardwaj et al., 2016).

Cloud computing. Cloud computing is data logic and infrastructure with calculating services and data on-call such as services in three categories Platform-as-a-Service (Paas), Infrastructure-as-a-Service (IaaS), and Software-as-a-Service (SaaS) (Ikram, & Hussain, 2018).

Cloud data storage provider. The cloud data storage provider is an entity responsible for making a cloud service available to cloud customers (Jaatun et al., 2018).

Cloud security. Cloud security is a set of controls, technology, and policies to safeguard stored data from deletion, exposure, and theft (Noshy, Ibrahim, & Ali, 2018).

Cloud security tools. Cloud security tools are anti-spyware, anti-virus, or an intrusion detection system, which are designed to monitor or detect intrusions in the cloud data (Alenezi, Atlam, & Wills, 2019).

Data processing. Data processing is an ordinary collection and control of data (Abeykoon et al., 2019).

Emerging technology. Emerging technology is automation or machinery that moved from the conceptual stage to the initial phase of the evolution process and most likely advances the IT community within the next decade Cearnau (2018).

End-user. An end-user is an individual that utilizes a cloud data storage provider's digital data storage service (Jaatun et al., 2018).

Hybrid cloud. The hybrid design combines aspects of the private and public cloud by proprietary technology that facilitates data maneuverability (Bhandayker, 2019; Mohapatra et al., 2015).

Private cloud. A private cloud is a restricted infrastructure managed, operated, and owned by the business, cloud data storage provider, or a mixture of both to protect multiple types data (Bhandayker, 2019; Mohapatra et al., 2015).

Public cloud. Public cloud is an open infrastructure that makes data accessible to a combination of government, academic, or business, over a public enterprise, such as the Internet at a low cost (Bhandayker, 2019; Mohapatra et al., 2015).

Small business. There are differences in how a small business is defined. Philip & Williams (2019) described a small business as a firm with fewer than 100 employees. For this exploratory generic qualitative study, a small business is one with no more than 100 employees.