Software as a Service (SaaS) as Cloud Computing: Security and Risk vs. Technological Complexity

Sandesh Achar*

Application Management Advisor, Dell Technologies, Round Rock, Texas, **USA**

*Corresponding Contact: sandeshachar26@gmail.com

ABSTRACT

The software delivery model known as Software as a service (SaaS) has evolved from cutting-edge innovation to an essential technology for many companies. However, due to the extensive range of cloud services that companies offer as part of their SaaS offerings, it is indispensable to thoroughly comprehend the dangers associated with using these services. This article describes those dangers and recommendations for the most effective methods of control that are open to managers. This study's objective is to investigate the factors of Technological Complexity, Security and Risk, and Technical Support within an organization to determine how these factors can influence an organization's end-use intention regarding cloud technology. The availability of technical support, the complexity of use, and the organization's training have been highlighted as the most crucial factors of this aim. The findings suggest that complexity negatively influences intention to use, although training and assistance are vital, with a similar weight. Shared or collective knowledge is essential in the adoption of cloud computing technologies.

Key words

Technological Complexity, Cloud Computing, SaaS, Security Issues

12/31/2016 **Source of Support:** None, **No Conflict of Interest:** Declared

INTRODUCTION

The expression "cloud computing" derives from the combination of the words "cloud" and "computing" (Torres, 2011). The word "cloud" is short for "cloud," which is the most commonly used symbol to represent the internet. It is determined that an abstract concept exists (unspecified physical systems, data storage in unknown locations, ubiquitous user access, and outsourced administrations). And computing, also known as computation, is the process of bringing together information technology ideas, coordination logic, and storage.

The use of the metaphorical term "cloud" refers, in general, to a sizable collection of resources, both hardware and Software, that are readily available and can be reached through the utilization of the internet as a means of access (Sá & Rocha, 2012; Vouk, 2008; Vaquero et al., 2009). The National Institute of Standards and Technology of the USA has stated that cloud computing is a model that enables access to a set of computing services

(networks, servers, storage, applications, and services) in a convenient and on-demand manner. These computing services can be rapidly provisioned and released with minimal administrative effort and interaction from service providers (Buyya et al., 2009).

The term "software as a service," or SaaS, refers to a model for delivering Software in which applications are made available to users on demand over the internet after being remotely hosted by the application or service provider. Customers are afforded significant advantages by adopting the SaaS model, including improvements in the effectiveness of their operations and cost reductions. The use of Software as a service (SaaS) is swiftly becoming the most popular delivery model for satisfying the requirements of enterprise IT services. On the other hand, most businesses are not yet on board with the SaaS model because they do not have sufficient visibility into how their data is secured and stored.

Numerous researchers offer a variety of security models and contribute their efforts to resolve the security issues and problems in the SaaS model; however, a significant number of challenges need to be surmounted to raise the security level. For example, data security, data breaches, network security, backup, authentication and authorization, web application security, availability, and data integrity are some security issues that need to be addressed. This research focuses on data security, and our study is based on concerns regarding the security of SaaS. Since it has been established that SaaS floats on top of PaaS and PaaS sits on top of IaaS, the security concerns associated with SaaS are connected to those of the two layers below it. Consequently, more responsible security will eventually constitute SaaS security. The SaaS model provides a high degree of integrated functionality but offers little customer control or extensibility. However, it does offer a high degree of integration. For example, PaaS offers somewhat greater customer control and extensibility on a lower level because it has a relatively lower degree of abstraction than IaaS. Finally, IaaS, the softest bed in the cloud computing hierarchy, provides customers with more power and control over the security of their data than either PaaS or SaaS.

Cloud computing is a step forward, but its implementation must take place within a modular framework that provides extensive reconfiguration capabilities and in which resources and services can be flexibly accumulated to accommodate the ever-shifting requirements of the market (Achar, 2015). Despite this, the idea is still in its earliest stages of implementation, both in Spain in particular and across the world in general. As a result, it is unevenly impacting the two primary components of the commercial landscape, namely large businesses and small and medium-sized businesses (SMEs). Understanding the factors that can influence the rate of adoption of cloud computing by organizations, particularly businesses, is essential if cloud computing is to continue its rapid growth. The goal of this work is to gain an understanding of the influence that complexity has, to provide personnel within the organization with training in cloud systems, and to receive support and support from the organization during the adoption process. This work is organized into the first section, referred to as the theoretical framework, which justifies the selection of these three variables. It is then followed by an area that provides an analysis of the structural model through the use of structural equations.

THEORETICAL FRAMEWORK

Based on the goals of this article, the research that is the most pertinent to cloud systems and the adoption models for those systems has been identified. According to Burda and Teuteberg (2014), most research published in the field of technology focuses on proposing new architectures and methods to solve problems such as cloud infrastructure security

(see, for example, Wang et al., 2013). In other instances, the primary focus of research is on issues concerning the opportunities, costs, and risks associated with cloud computing, service quality measurement criteria, or factors related to SaaS adoption, such as service availability, accessibility, performance, the lack of interoperability standards, and its difficulty of integration and customization (Fortes et al., 2016). It is also possible to locate some works highlighting the significance of trust, not only in the implementation of cloud technology but also in the privacy conditions present in data storage. Other investigations conclude that factors such as uncertainty, compatibility, support from senior management, perceived usefulness, ease of use of technology, previous experience, geographical restrictions, company size, market, vendor efforts, security, trust, social influence, and pressure from business partners all play a significant role in the adoption of cloud computing (Gangwar et al., 2015).

It is common practice to include a final variable labeled "intention to use" (UI), as many previous studies have held the belief that an intention always comes before an action, which boosts the reliability of the model's ability to predict future behavior (Fishbein & Ajzen, 1975). Therefore, user interface refers to the amount of previously acquired behavior when utilizing the technology mentioned above. We will refer to the degree to which a technology is perceived as relatively difficult to understand and use as the technological complexity (CT). Some research works that can be found in the literature and are related to complexity are those that investigate the degree of difficulty that employees have in using the skills necessary to use the technologies or the problem of integrating these technologies at work (Premkumar & Roberts, 1999).

Based on these ideas, we can assert a negative relationship between the perceived complexity and the utilization of the cloud. We will make an effort to find evidence that confirms this relationship. Since technological sophistication is perceived in the proliferation of standards and protocols for correctly implementing hardware and Software in Information Systems, it is negatively associated to use. This is because technological complexity is perceived in the proliferation of standards and protocols. As a result, the complexity of the technology can act as a barrier to the intention to use cloud computing, which confirms the significance of the relationship between the two. As a result, the choice to use will increase in likelihood in proportion to the reduced influence of complexity (Premkumar & Roberts, 1999).

It has been determined that the level of support and support within the organization (SA) is a relevant factor in adopting information systems. Aid and support are essential, whether from within the organization or from the outside; they provide synergy, ensure the safety of users, and assist in living up to expectations. When we talk about support and assistance provided within a company, we refer to that provided between the various departments that make up the business. On the other hand, when we talk about help and support from the outside, we're referring to the connections that our company keeps with the cloud provider. Following the logic presented above, the goal we have set for ourselves is to collect evidence that cooperation is positively related to the perceived usefulness of the cloud. In this sense, we presume that the support and support, as well as the common treatment of the issues derived from the cloud, make it easier for users to have the intention to use them. The model that is being suggested is depicted in figure 1, which is as follows:

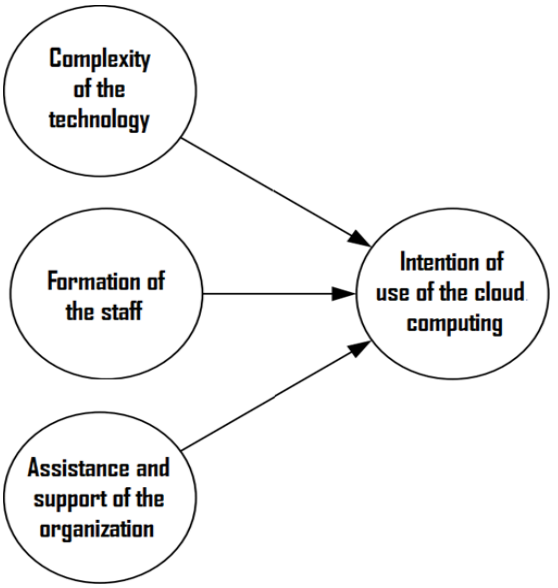

Figure 1: A proposed theoretical model

RISK IMPACTS OF SAAS CLOUD COMPUTING

Cloud computing is quickly becoming an essential service for many businesses, and it is no longer considered a novel or good form of technology. This alternative technology offers users of Software as a Service (SaaS) the flexibility to adapt to rapidly shifting demand while also providing managers with alternative financial solutions that facilitate the introduction of or improvement to service delivery strategies. For example, the user of the SaaS may have to make concessions in how technological risks are managed if they want to reap these benefits. Cloud computing fundamentals and general risk management strategies for evaluating cloud environments have been presented to readers in previous articles (for a list of these articles, see the sidebar titled Background Reading on Cloud Computing). This article provides readers with a more direct understanding of the SaaS-related cloud computing activities that they may engage in and the resultant risks that require management's attention to achieve the desired benefits and enterprise goals.

Users who are not part of the technology department are the ones who are most likely to interact directly with a SaaS solution. These users are sometimes referred to as "end" or "business" users because the SaaS solution frequently represents an application or data processing activity that falls directly under the business user's purview. E-mail and other office tools are included in SaaS services (e.g., Office 365 or Google Workspace). In the enterprise market, accounting and financial management software providers such as SAP, NetSuite, and Oracle Financials offer a SaaS delivery model. In the small and midsize business market, accounting and financial management Software providers such as Intacct, Xero, and Quickbooks also provide this model. Other well-known software companies, such as Salesforce, Slack, ServiceNow, Github, and Workday, offer SaaS business models that have evolved to become essential components of corporations. According to the author's personal experience, larger SaaS user organizations with the financial resources to make the most effective use of these solutions also offer risk management oversight of the vendors that provide them.

However, a significant advantage of SaaS contributes to increased risk management concerns. This is mainly the case when the solution's use falls outside the entire enterprise's purview. SaaS solutions don't require the upfront money and oversight of traditional Software. In a decentralized firm, an executive can pick what to acquire and which technology tools to utilize, especially in decentralized organizations. If the subscription fee is manageable, the CEO can implement the system with minimal intervention from risk management and compliance officers. Unfortunately, the risk is not limited to the amount of money spent; the storage and processing of data by an unvented or unmanaged SaaS vendor or service organization is the higher vulnerability. This is because the acts of this vendor or service organization could severely affect the reputation of the SaaS customer and, in certain situations, its survival.

TECHNOLOGY ACCEPTANCE MODEL

As previously mentioned, the theory of reasoned action (TRA) (Ajzen & Fishbein, 1980) served as the foundation for the development of the technology acceptance model (TAM), which was first presented by Davis (1989) to explain system use and to determine the level of technology acceptance. When deciding whether or not to adopt new technology, the perceived usefulness of that technology is essential to a company (Venkatesh, 2000). The individual will not find the latest helpful technology enough to adopt if it is not believed that using the technology will improve job performance (Workman, 2007). There are, of course, exceptions to this rule; however, this is generally the case with the majority of people and the majority of businesses. It is also essential to consider how simple it is to use the new technology. People do not want to switch from using something they are accustomed to working with to something difficult to deal with because it is more complicated, complex or complex (Venkatesh, 2000). The vast majority of people do not or are unable to see a benefit if they have to learn a lot of new information and spend a lot of time determining how to work on new technology. There would be no real point in doing that unless there was a significant benefit, and there would have to be a substantial benefit for it to be worthwhile. If the new technology has any chance of being adopted, it needs to make their lives (and their jobs) easier from the beginning of their use (Workman, 2007). However, it provides links to explain how external variables influence beliefs, attitudes, behavioral intention to use, and actual usage using the TAM. The TAM theory also suggests that exogenous factors influence the actual application of a technological system via mediated effects on the perceived usefulness and ease of application. For example, the first version of the TAM was created by Davis, as shown in Figure 2.

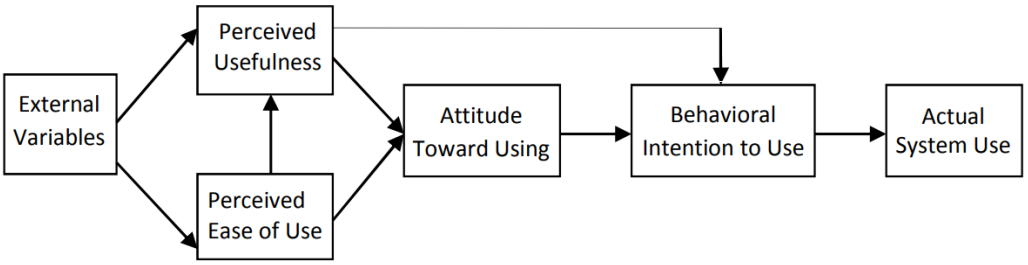

Figure 2: The first iteration of the technology acceptance model (TAM) (Davis, 1989)

A company can determine whether or not SaaS will be a good fit for their business and whether or not it is something that would be better off left alone by using the TAM (Venkatesh, 2000). However, some people should not store their data in the cloud. Because

there is no need to keep anything on the company's servers, it is difficult to argue that there is the ease of use there. This makes the argument more difficult. This takes up less space and retrieving the data when necessary is elementary.

SECURITY ISSUES OF SAAS

Hashizume et al. have published an article that provides an analysis of the work done by various authors on various aspects of cloud computing security. These aspects include vulnerabilities, warnings, procedures, security standards, data security, certainty, security requirements, and SaaS, PaaS, and IaaS security (2013). This research aims to ensure data security, and the study is based on concerns regarding the security of SaaS. It has been established that Software as a Service (SaaS) sits atop Platform as a Service (PaaS), and PaaS sits atop Infrastructure as a Service (IaaS). Because of this, the security concerns associated with SaaS are intertwined with those of the two layers below it. Ultimately, more responsible security will constitute SaaS's security. The SaaS model provides a high degree of integrated functionality but offers little in the way of customer control or extensibility. However, it does provide a high degree of functional integration. For example, PaaS, which has a relatively lower degree of abstraction than IaaS, offers greater customer control and extensibility because it is layered beneath IaaS. In comparison to PaaS and SaaS, the lowest tier of cloud computing, IaaS, gives users more power or control over the level of security they receive.

Data is the most crucial component that must be kept safe for almost all users, regardless of whether they access the Platform independently or through an organization. Because the user's data is stored in the data center near the provider, the user relies on the cloud provider for SaaS for any security concerns that may arise. There is no doubt that the data of other users are also stored there. For example, suppose a SaaS provider is also associated with a Public Cloud Service. In that case, there is a possibility that enterprise data could become contaminated with data that is not relevant to the business. In addition, the cloud service provider may replicate the data if it is necessary to achieve high availability and quick access to the data in several locations worldwide. Therefore, the lack of control that results from an unguaranteed circumstance in the SaaS model is caused by the fact that users are unaware of the locations of their data.

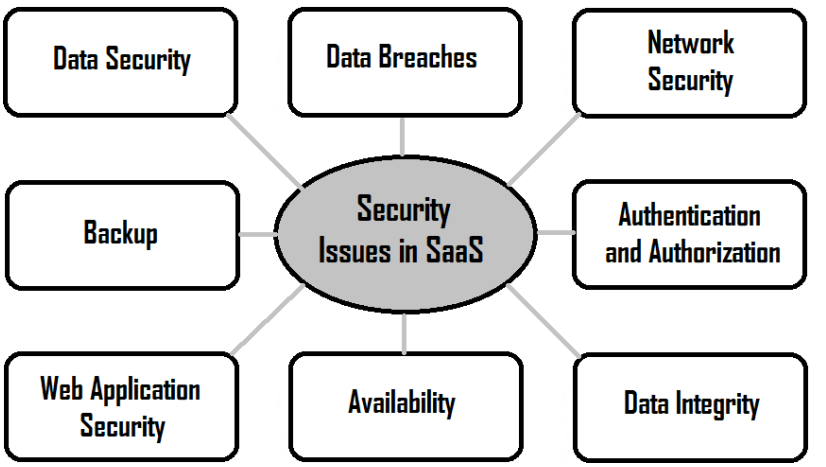

Figure 3: Security Issues in SaaS

If a user wants to remove his data, but he does not know where it is stored, and if he tries to remove it, it is removed from all of the locations where a provider duplicated it at the time it was being stored, then this case may create another problem. Cloud computing services move software applications and databases to more extensive data centers where the dependability of management services is not aspirational. These larger data centers are called "data farms." This activity gives rise to a wide variety of safety concerns and issues. It is the responsibility of the provider to protect the privacy of user data from the prying eyes of other users using a model known as SaaS. When customers use the cloud, their older software applications are periodically or sporadically replaced with newer versions of the same Software. Therefore, to accomplish a successful data migration, the provider needs to concentrate on the protection or enhancement of the security functionality issued by the legacy application, in addition to the portability of applications.

DISCUSSION OF THE FINDINGS

The findings indicate that the proposed model, based on the variables of technological complexity, staff training and support, and support from the organization, has the tendency to explain approximately 32.2% of the intention to use the cloud computing system. This result moderately explains the model's predictive power in terms of the variance presented (Chin, 1998). According to the findings of this study, an individual's intention to use a cloud-based system is impacted by its level of technical complexity. This result is consistent with Tsai et al. (2010) found regarding the cloud specifically. This suggests that although organizations consider cloud systems to be helpful and straightforward to use, implementing these systems may involve particular technological challenges that some businesses cannot overcome. These challenges may include, for example, the requirement for ICT specialists or the technical requirements for protecting processes and data. In any event, the influence of technological complexity on the intention to use is inverse, which means that there is less intention to use the cloud when there is a greater complexity in the technology. Although ease of use and usefulness have traditionally been relevant mediators in other adoption models, this paper demonstrates that technological complexity is also a mediator that needs to be considered in this new technology. This work contributes to a novel factor of influence in services because few studies support the result of training and support in information systems, also known as technological cooperation (Bueno & Salmerón, 2008). On the other hand, cloud computing has been contrasted with the complexity of technological advancements.

CONCLUSION

On the other hand, the services must be intuitive enough to be used by virtually any user with only a basic understanding of computers at the user level. For example, a decrease in the complexity of the technology and an increase in the desire to use it would result from increased usability and accessibility. For this reason, we believe it is essential to incorporate some solutions into operating systems and browsers, just as Google and Microsoft have already done. Moreover, the technological complexity has now been brought to light regarding the difficulty of comprehending it in its current state or the amount of assimilation required for learning how to use it. According to the findings of our research, the members of the 150 organizations that were polled reported that the training they had received was comprehensive, that it increased their knowledge, that it increased their confidence, that it had adequate trainers, and that it was sufficient in terms of its length and the degree of detail it included.

In conclusion, the backing and assistance provided by the organization have a positive influence on the intention to make use of it. This factor is relatively new in the cloud because, even though it has been discovered in other investigations of information systems, it is empirically demonstrated in this investigation, where we draw it within a relatively new context that is vigorously spreading on the internet: shared or collective knowledge. Although it has been found in other investigations of information systems, it is empirically demonstrated in this investigation.

As a result of this research, we have concluded that the development and advancement of such a complicated, hugely interconnected, globally distributed infrastructure has led to many security risks and vulnerabilities. To date, a significant number of researchers have helped to protect users from these problems by developing a variety of solutions, including encryption, signatures, and other mechanisms; however, the situation has become more complicated as a result of the inherent tradeoff between the various problems and functionalities that are present in this domain. In this research, we put forward a security model composed of three distinct levels, each of which possesses its own algorithm. Because the client's data comes in various formats, the client can protect the data to the appropriate degree.

Studying the factors that condition the adoption of cloud technology from the perspective of business cooperation to evaluate the effect that participation would have is one of the aspects that could be the subject of future lines of research and would be a complementary study to the research has already been carried out. This is one of the potential aspects that could be the subject of future lines of research in the context of business networks to boost the amount of organizational training and retraining of technical staff in implementing cloud systems.

REFERENCES

Achar, S. (2015). Requirement of Cloud Analytics and Distributed Cloud Computing: An Initial Overview. *International Journal of Reciprocal Symmetry and Physical Sciences*, *2*, 12–18. Retrieved from https://upright.pub/index.php/ijrsps/article/view/70

Ajzen, I. & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.

Bueno, S., & Salmerón, J. (2008). TAM-based success modeling in ERP. *Interacting with Computers, 20*(6), 515-523.

Burda, D., and Teuteberg, F. (2014). The role of trust and risk perceptions in cloud archiving. *Journal of High Technology Management Research, 25*(2), 172-187.

Buyya, R., Yeo, C., Venugopa, S., Broberg, J., and Brandic, I. (2009). Cloud computing and emerging platforms: vision, hype, and reality for delivering computing as the fifth utility. *Future Generation Computer Systems, 25*(6), 599-616.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research, 295*(2), 295–336.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *Management Information Systems Quarterly, 13*(3), 319–340. https://doi.org/10.2307/249008

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitűd, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Fortes, N., Pereira, J. H., & Costa, J. F. D. (2016). A adogão de serviços cloud computing pelas empresas portuguesas: O papel dos esforços de marketing. *RISTI - Revista Ibérica de Sistemas e Tecnologías de Informação, 18*, 33-48.

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Information Technology, Journal of Enterprise Information, 28*(1), 107-130.

Hashizume, K., Rosado, D. G., Fernández-Medina, E. & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(5), https://doi.org/10.1186/1869-0238-4-5

Martens, B. & Teuteberg, F., (2012). Decision-making in cloud computing environments: A cost and risk-based approach. *Information Systems Frontiers, 14*(4), 871-893.

Premkumar, G., & Roberts, M. (1999). Adoption of new information technologies in rural small businesses. *Omega, 27*(4), 467-484.

Sá, F., & Rocha, Á. (2012). Definiçao da arquitetura de informaçao em organismo da administraçao pública local. *RISTI - Revista Ibérica de Sistemas e Tecnologías de Informagão, 10*, 51-64.

Torres, J. (2011). *Empresas en la Nube. Ventajas y retos del Cloud Computing*. Barcelona: Libros de Cabecera.

Tsai, M., Lee, W. & Wu, H. (2010). Determinants of RFID adoption intention: evidence from Taiwanese retail chains. *Information Management, 47*, 255-261.

Vaquero, L. M., Rodero-Merino, L., Caceres, J., & Lindner, M. (2009). A break in the clouds: Towards a cloud definition. *Computer Communication Review, 39*(1), 50-55.

Venkatesh, V. (2000). Determinants of Perceived Ease of Use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information systems research, 11*(4), 342–365.

Vouk, M. (2008). Cloud computing - issues, research, and implementations. *Journal Computer Information Technology, 16*, 235- 246.

Wang, C., Chow, S., Wang, Q., Ren, K. & Lou, W., (2013). Privacy-preserving public auditing for secure cloud storage. *IEEE Transactions on Computers, 62*(2), 362-375.

Workman, M. (2007). Advancements in Technology: New Opportunities to Investigate Factors Contributing to Differential Technology and Information Use. *International Journal of Management and Decision Making, 8*(2), 318–342.

--0--

ISSN: 2409-3629

Online Archive Link: https://abc.us.org/ojs/index.php/ei/issue/archive