AN ANALYSIS OF CLOUD COMPUTING SECURITY CHALLENGES - A CONCEPTUAL FRAMEWORK FOR CLOUD COMPUTING EARLY ADOPTERS AS A TECHNOLOGY MODEL

T. Vinodh Kannan and M. Arvindhan

Department of Computer Science and Engineering, Mookambigai College of Engineering, India

Abstract

Distributed computing has become predominant nowadays, and with most of the populace reliant on it, its security issues have become a significant concern. The Cloud Security System can be assessed based on three key parts namely Privacy, Integrity, and Availability (CIA). These components continue as before independent of the system or design of the Data Security utilized. Henceforth the arrangements can be resolved based on the CIA. This paper shows an audit on the essentials of Cloud Security and spotlights on the significance of the CIA for giving better arrangements.

Keywords:

Cloud Computing, Privacy, Authentication, Trust and Transparency, Data Recovery and Backup

1. INTRODUCTION

Security in cloud computing is a much discussed theme and this article focusses on the security challenges related with cloud computing. With the current patterns and progresses in cloud computing, there appears to be an agreement within the writing that security in cloud computing is genuine and it must be tended to. This paper proposes a reasonable instrument to play down the effect of security challenges in cloud computing. While the technological know-how model of cloud computing is praised for the super edges it offers, it also poses the decision-makers with unpleasant challenges that reduce the effects of protection aspects in [2] cloud computing. Studies conducted in this regard indicate that users and organizations are considering adopting cloud computing science so as to reap their enterprise goals. Contrary to the wish and excitement among users and corporations to adopt cloud computing, there is also the need for the effective adoption of practicable mechanisms for countering the protection challenges.

The Service Level Agreement (SLA) is an agreement between the specialist organization and its client. Be that as it may, numerous issues still stay impending. This is on the grounds that the CSP should bolster all periods of the data lifecycle, in particular generation, storage, usage, distribution and destruction, for ideal security [3].

The classification, integrity and availability is capable of arranging their data and virtualization partners. Classification can commonly be characterized as the circumstance of maintaining information mystery or private. It is a method for giving accepted control. Uprightness is the mix of exactness and consistency of information. This ensures the records are bona fide. Accessibility is the potential of a customer to get data from a precise region in the proper configuration. This is assured by the proper maintenance of all equipment.

Cloud computing as a technology gives a real chance for the enlargement through its splendid benefits that are proven among its Users and companies. The terrific scope for innovation and development that cloud computing provides has rendered it to be the much sought after and practicable technology solution.

The advantages of cloud computing have enabled the users of the premise-based environments to save on the massive costs associated with hardware and software maintenance. While distributed computing offers various advantages, security difficulties and concerns are not immaterial in the selection of the innovation model. This paper gives a specific consideration to the security concerns related with the reception of the innovation model by early adopters. The examination attempts to propose an applied structure to address these difficulties [5].

2. LITERATURE REVIEW

Cloud computing is characterized as a virtual pool of assets conveyed over the Web, advertising on-demand frameworks computer program over negligible human interaction [1]. In expansion, [5] gives a more specialized and orderly definition to cloud computing as a compilation of existing methods and advances bundled inside a modern framework worldview that gives progressive adaptability, versatility, commerce nimbleness, quicker start-up time, decreased administration fetched, and just-in time accessibility of resources. The following are the characteristics of cloud computing:

- On-demand self-service whereby the user has the ability to manage and perform computing tasks with minimal interaction from the service providers.
- Measured service whereby the user only pays for the service used.
- Resource pooling whereby the resources are made available through the network.
- Rapid elasticity and scalability whereby computing resources are delivered in a flexible manner and scaled based on users’ requirements.

Services in cloud computing are presented at three levels, namely, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS). In addition to these three delivery models, other services generally referred to as the XaaS develop on regular basis [8]. The deployment models in cloud computing as follows:

- Public cloud whereby services are made available through the Internet;
- Private cloud whereby services are exclusively managed by one organization;

- Community cloud whereby computing resources are shared by organizations with similar policies or requirements; and
- Hybrid cloud whereby one, two or three of the above models are combined then deployed as a standard and single unit or entity.

3. SECURITY IN CLOUD COMPUTING

This section addresses the issues related to security in cloud computing after examining the context [6] to the analysis. Security is one of the most important concerns reported in the adoption of cloud computing.

In many cases, the responsibility for maintaining privacy, data protection from misuse, malicious attacks and access remains with the service provider [7]. One of the key issues to be discussed in this analysis is how security problems impact cloud computing adoption.

3.1 SECURITY CONCERNS

Security is considered as one of the significant worries in the usage and reception of any innovation, and distributed computing is no exemption. Security turns into a significant factor since information utilized and shared by associations ought to be ensured, and unapproved specialists must not be permitted to approach. The nearness of security issues in the cloud are prompted by privacy, validation, encryption and unscrambling, and information assurance, just to give some examples [8].

With information in the cloud and server farms being constrained by an outsider, there is no genuine assurance for information security. This leaves the client with no power since the client is not responsible for his information. The security concern influences both the client and the specialist co-op. This establishes a test in guaranteeing appropriate reinforcement and recuperation systems for information and verification of clients, just as information openness

Given the present security dangers in distributed computing, unmistakable measures are being taken to manage security challenges in the cloud. Regardless of these unmistakable measures, security challenges stay a major threat in cloud reception and usage, with no place for clients to settle on a decision other than to depend on the specialist organization [13]. There is a need in this examination to build up the degree of security worries as to the reception of distributed computing.

3.2 ORGANISATIONAL RISKS

Cloud computing security has a direct impact on how users handle their privacy and data security. Often, if affected by security threats and how the customer choose to act in order to protect his / her data, there are direct consequences. The study [11] reiterates that data security and personal information of users remain a major concern in the cloud, and it remains a major challenge for service providers to secure these elements [12].

An effective information security governance should be in place to protect organisation data as agreed upon in the service level agreement [13].

3.3 PROTECTION OF DATA FROM THEFT

One of the most perplexing difficulties recognized in the writing is the assurance of information in distributed computing [14]. Distributed computing specialist co-ops and clients have no full command over application organizations and administration conveyance in the cloud, along these lines making information progressively powerless in different ways. The study in [13] reviews the two circles of information assurance in distributed computing giving no geographic limits, where information security can be given when contrasted with in-house conditions.

With cloud computing, information becomes the topic of breach and unauthorized access from internal or external quarters. The employment of accessible strategies like cryptography, draft of policies or security assurance mechanisms to manage breaches will reinforce information protection. Protection of knowledge in cloud computing can go an extended means as long as there’s a full commitment from each the service suppliers and users. This study is regarding providing viable mechanisms to guard information from felony within the cloud [15].

3.4 DATA ACCESS AND CONTROL

While distributed computing gives information openness anyplace and whenever, there are different security dangers to information once it is gets out of the control of the association in charge of its administration. The study in [9] claims that in spite of the degree of authoritative security, for example, giving firewalls and other security controls, security stays an incredible test to manage.

The complexness of organisational security is exacerbated by the actual fact that a lot of insiders have access to organisational network systems on one hand and on the other hand, third parties units have the access to manage knowledge operations. Knowledge access and management in cloud computing appear to be tough to administer [12]. The best challenge within the administration of knowledge of information is exacerbated by the actual fact that even confidential data is lawlessly accessed due to the lenient access controls within the cloud.

The study in [12] explains that the period of knowledge within the cloud will increase the high risk of risks for intruders to access data. At a similar time, a number of the exaggerated risks related to knowledge access and management within the cloud emanate from each internal and external environments. Thus, knowledge access poses a significant challenge to cloud computing adoption. The amplification of the accessibility risks within the cloud has become crucial as a result of IT services and users converge on one management domain with very little transparency into the method and procedure.

The strategy of consistence and giving access to clients probably won’t be completely clarified or featured in the administration level concurrence with specialist organizations, which can add to an alluring open door going for side interest programmers, composed wrongdoing to state-supported interruption. The study in [15] claims that trust of information in distributed computing is basic to guarantee a degree of security in the arrangement of the administration. The absence of trust regularly prompts issues of believability, affectability and notoriety, which have negative results.

3.5 AVAILABILITY ISSUES

Availability of cloud computing, flexibility is considered an important feature [3]. The study in [16] describes availability as a method to maximize production system readiness by accurately measuring and assessing the production system outages.

The significant objective of information accessibility in distributed computing is to guarantee that clients can get to information whenever and anyplace [13]. With no space for question, the three primary cloud administrations do a similar capacity of giving the administrations anyplace when required [12]. Specialist organizations are said to do everything available to them to give repetition to make information open to various clients.

The challenge in spite of the fact that remains on the benefit suppliers to guarantee accessibility of information anyplace and anytime [13]. When major operations or overhauls are embraced by the benefit suppliers, genuine dangers of information inaccessibility and intrusion are experienced by the client on one hand and on the other hand, the issue may indeed be exacerbated by the wastefulness in organizing the capacity of transmission or the capacity to support upgrades.

Addressing all the issues related to the accessibility of information in cloud computing is one among the other dangers posed by cloud computing appropriation. Very little is done to guarantee that information is accessible twenty-four hours a day, seven days a week, and three hundred and sixty five days a year. Clients have small to do to ensure their information; in this manner, they are influenced by the impact of accessibility of their information within the cloud.

3.6 DATA RECOVERY AND BACKUP

Clients have the commitment to guarantee that they are mindful of essential reinforcement and recuperation instruments to secure their information within the cloud. The method in [17] claims that fundamental recuperation and reinforcement techniques are now and then ignored by users. The study in [17] clarifies in advance that ignoring these viewpoints can bring an unrepairable damage to information put away within the cloud. The length and time outline it ought to take to recuperate from blackout and control disappointment within the cloud ought to be highlighted and accounted for within the service level understanding. Clear confirmation mechanisms should also be given to benefit the supplier (SP) within the intrigued of recuperating information within the cloud.

Failure to recover information on time has enormous financial and organizational consequences for the consumer who has invested in the technology [17]. As the literature points out, the consequences of failing to ensure data recovery and backup pose enforcement and governance concerns.

One of the major concerns posed in the implementation of cloud computing is the issue of data recovery and backup in cloud computing. In the literature, little has been done to raise visibility for users of data recovery and backup in the cloud. To address these concerns, this paper would like to suggest feasible methods.

3.7 STANDARD-BASED SECURITY ISSUES

The problem of data recovery and backup in cloud computing has been one of the major concerns raised in cloud computing adoption. In the literature, little has been done to raise visibility for users of data recovery and backup in the cloud. To address these concerns, this paper would like to suggest feasible methods.

This study noted that while customizing security requirements appears to be a significant development in cloud computing, users remain largely concerned about the consequences of security issues, especially when they have little or no adequate understanding of the security standards provided by the software model [18].

3.8 DATA PRIVACY

The idea of information protection in security has been reliably formed by various variables relying upon societies and ward; in this manner making it difficult to characterize. The study in [9] refers to security similar to the responsibility of the association to information, just as its straightforwardness as to individual data. The idea of protection goes further and covers parts of the utilization, maintenance and revelation of individual data.

Cloud computing makes it even more difficult for users to have full control of their personal information as data are stored in data centers and databases around the world. While protections may be offered by service providers, when it comes to the protection of personal information, data privacy transcends issues of confidentiality and trust from the user perspective.

Cloud data is either secured or not protected at all because software insecurity makes all aspects of privacy very complex. It further argues that a valuable amount of information can be accessed by hackers and even made available to third parties without the users' consent [14]. Cloud computing software design appears to be vulnerable to potential user usability threats

3.9 TRUST AND TRANSPARENCY

In the wake of talking about the protection of information in distributed computing, trust and straightforwardness are other two ideas especially lined up with security as coming about elements for the absence of security. Trust alludes to when a person or thing is dependable, genuine, and compelling [18].

A risk management system is crucial with uncontrollable levels of security violations in the cloud. In various decision-making situations and environments such as intrusion detection, encryption, access control, key management and other similar purposes, trust management is useful [18]. The study in claims the cloud computing trust management system

3.10 AUTHENTICATION AND VALIDATION

Authentication within the cloud provides authorization to users with credentials through varied context-aware info to access cloud services. With key concerns to authentication, authorization and validation services offer a medium and platform to regulate and manage what the user must access from the perspective of the profile and role of the user.

Verification is respected as an awesome concern in cloud computing [20]. Clients have a critical obligation to guarantee that they confirm themselves on hierarchical gadgets to get through the cloud administrations facilitated exterior/peripheries with controlled firewalls. The study in contends that the concern is indeed more prominent since confirmation puts a colossal sum of weight on clients to oversee dynamic catalogs of databases, as well as their claim qualifications put away within the cloud. In expansion, contends that verification and approval of users' qualifications have put an awesome sum of overhead on both IT administration and clients alike to self-manage and precisely evaluate the effect of not being in control of their possess credentials.

3.11 RISKS IN CLOUD COMPUTING

This sub-section explains that user's threats in embracing cloud computing, even unknown risks, should be made known to them. Some of the dangers of cloud computing technology outlined in the literature include long-term sticker shock, long-term competitiveness, organizational hazards, to list but a few that are shielded from users in nature [14].

As cloud computing is no longer a new concept, it is necessary to raise awareness among users of the risks and related impacts of the software model. Cloud computing technology's threat debate is still far from over, and a great deal of knowledge needs to be generated particularly for users willing to adopt the template as their preferred [25].

3.12 REGULATORY AND LEGAL ISSUES

Regulatory and legal uncertainties in cloud computing have raised several considerations within the adoption of cloud computing as a technology model [24]. These considerations rose as a result of the processes involved in managing, storing, accessing, and controlling the knowledge within the cloud. Knowledge on cloud is stored across various locations on the globe. The rules and regulations for accessing and processing the knowledge varies from place to place. Therefore, handling the laws that regulate breaches and complaints create an even more troublesome scenario when it comes to safeguarding the users' rights.

The Business software system Alliance indicates that a well-balanced policy and involvement of foreign governments can play a big role in addressing the users' considerations. Moreover, there are many different aspects like privacy, info security, and crime that are connected to the holding of cloud computing. This mandates the careful designing of a restrictive and legal framework that aligns with the users' considerations to deal with the challenges and considerations related to cloud computing adoption. A binding agreement is indispensable for a triple-crown adoption method [15].

3.13 CONTRASTING PARADIGMS OF SECURITY

With huge implications that security includes in the implementation of cloud computing, the service provider is obligated to provide customers with a number of security protection mechanisms, which in effect are also responsible for improving security controls, on the one hand, shows that the treatment of protection deals by service providers in many cases takes away a great deal.

On the other hand, it describes the difficulty of security mechanisms in cloud computing. The study in [24] further states that, given the complexities of protection in cloud computing, multi-domain security interfaces give users a number of benefits.

Although security is still considered one of cloud computing's most daunting factors, many organizations are working to reduce its complexities backed by service-level agreements [24]. A security solution backed by a robust service level agreement is a good way to give companies and consumers peace of mind in order to focus on other areas of improvement.

4. CONCEPTUAL FRAMEWORK

The study uses the conceptual framework of the Technology Acceptance Model (TAM). The proposed TAM model suggests that a system or software use is a reaction that can be clarified or predicted by a consumer incentive that can be directly influenced by an external stimulus consisting of the features, capabilities and characteristics of the actual system or technology [12].

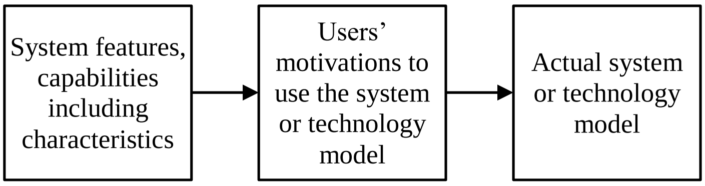
System features, capabilities including characteristics
Users' motivations to use the system or technology model
Actual system or technology model

Fig.1. Proposed TAM model

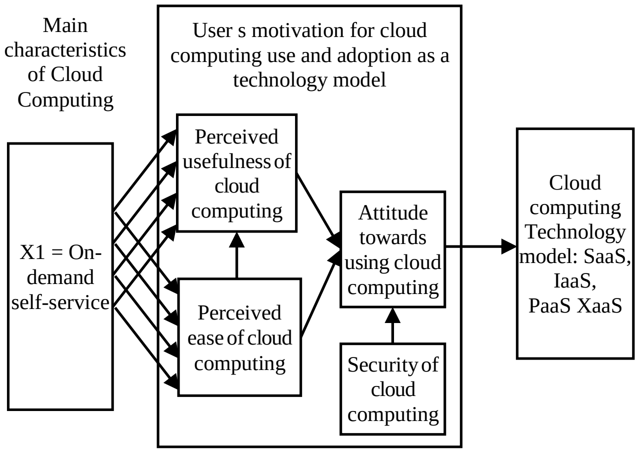
Main characteristics of Cloud Computing
X1 = On-demand self-service
User s motivation for cloud computing use and adoption as a technology model
Perceived usefulness of cloud computing
Perceived ease of cloud computing
Attitude towards using cloud computing
Security of cloud computing
Cloud computing Technology model: SaaS, IaaS, PaaS XaaS

Fig.2. Modified version of the TAM model

The concept can be applied to an information system or software model to illustrate the use of computers and factors related to acceptance and adoption of technology. The initial and proposed TAM model examines the following three constructs: perceived usefulness (PU), perceived user-friendliness (PEOU) and system user-friendliness (ATU). In relation to this report, cloud computing security has an effect and an influence on adoption and acceptance as a software model. This study focuses primarily on the security of cloud computing, as the first three buildings are not included in this analysis.

5. PERFORMANCE ANALYSIS

An approach is considered as an arrangement to decide the idea of the connection between factors. The philosophy helps the scientist to assemble members and acquire their perspectives. The examination utilized a study based technique to break down information. Normally connected with a deductive methodology, the study-based technique is generally used to answer who, what, where, how and why questions. The study in [13] contends that the technique is utilized for various reasons, to be specific:

- To enable the scientist to gather a wide scope of information from a sizeable populace;
- To enable information to be institutionalized for simple examination;
- To guarantee that produced information are effectively comprehended and translated;
- To enable the scientist to set up potential explanations behind connections among factors and build up new models for these connections; and
- To enable the scientist to produce discoveries that are illustrative of the entire populace at a lower cost.

A Wilcoxon signed ranks test was used to test the validity and significance of results in the agreement and disagreement of findings provided by the participants. The Fig.3 summarises the findings about the security challenges from the least cited to the most cited challenges by early adopters of cloud computing.

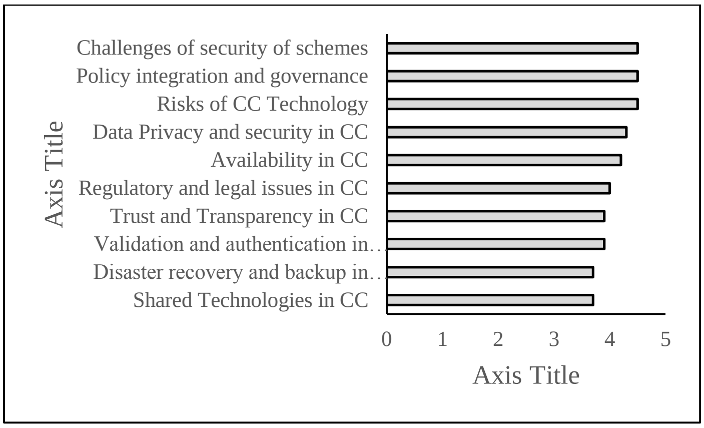

Fig.3. Level of agreement/disagreement about security challenges in cloud computing

The research adapted a reference framework [20] to support users and organizations. With the experience of users in mind, this model can be further extended across different platforms. The framework recommends the following steps to ensure that consumers and companies are prepared to address the security challenges of cloud computing adoption:

- Analysis of business objectives
- Maintain a risk management program
- Development of a security plan to support business objectives
- Development of specific corporate support
- Development of security policies, procedures and standards
- Audit and Review Strategy; and Continuous improvement of the security plan.

Since consumers are not aware of the risks associated with the use of cloud computing as a software model, they are more exposed and more vulnerable. The study in discusses the relationship between knowledge and technology adoption. It further states that the inability or failure to implement a technology can be due to a lack of awareness.

6. CONCLUSION

This section discusses the overview and offers guidance on a security framework for the implementation of cloud computing. The literature chapter analyzes the work and discusses the need to tackle security challenges and concerns in cloud computing. Different security stages in distributed computing have been intended to give rules to associations and clients considering the reception of the innovation model. With security in distributed computing being probably the best challenge distinguished in the writing, proposed systems and components are seen to assume an indispensable job in limiting the dangers of exposing the clients to enormous misfortunes that may happen if the essential security instruments are not monitored.

REFERENCES

[1] C. Erol, S. Gulsecen, E. Karatas and Z. Ozen, "Cloud Computing and Some Scenarios for its Applications in Universities", *European Researcher*, Vol. 30, No. 9, pp. 1515-1526, 2012.

[2] A.E. Youssef, "Exploring Cloud Computing Services and Applications", *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 3, No. 6, pp. 1-12, 2012.

[3] A. Joshua and N. Ogwuelela, "Cloud Computing with Related Enabling Technologies", *International Journal of Cloud Computing and Services Sciences*, Vol. 2, No. 1, pp. 40-49, 2013.

[4] M. Mujinga, "Developing Economies and Cloud Services: A Study of Africa", *Journal of Emerging Trends in Computing and Information Sciences*, Vol. 3, No. 8, pp. 2079-8407, 2012.

[5] C. Chandravathy, V. Kumar and G. Murugaboopathi, "Study on Cloud Computing and Security Approaches", *International Journal of Soft Computing and Engineering*, Vol. 3, No. 1, pp. 2231-2307, 2013.

[6] A. Al Yasiri and N. Khan, "Identifying Cloud Security threats to Strengthen Cloud Computing Adoption Framework", *Proceedings of 2nd International Workshop on Internet of Thing: networking Applications and Technologies*, pp. 485-490, 2016.

[7] L.A. Nivedita and K. Sravani, "Effective Service Security Schemes in Cloud Computing", *International Journal of Computational Engineering Research*, Vol. 3, No. 2, pp. 2250-3005, 2012.

[8] K. Goyal and P. Supriya, Security Concerns in the World of Cloud Computing, *International Journal of Advanced Research in Computer Science*, Vol. 4, No. 4, pp. 976-997, 2013.

[9] E.S. Hajji and T. Maha, “From Single to Multi-Clouds Computing Privacy and Fault Tolerance”, *Proceedings of International Conference on Future Information Engineering*, pp. 112-118, 2014.

[10] R. Schisser, “Information Technology Systems Management”, Prentice Hall, 2010.

[11] S. Carlin and K. Curran, “Cloud Computing Technologies”, *International Journal of Cloud Computing and Services Science*, Vol. 1, No. 2, pp. 59-65, 2012.

[12] G. Sarojini, K. Selvamani and A. Vijayakumar, “Trusted and Reputed Services using Enhanced Mutual Trusted and Reputed Access Control Algorithm in Cloud”, *Proceedings of 2nd International Conference on Intelligent Computing, Communication and Convergence*, pp. 506-512, 2016.

[13] M. Ahmad, M. Chong and A. Hamid, “Enhancing Trust Management in Cloud Environment”, *Proceedings of International Conference on Innovation, Management and Technology Research*, pp. 314-321, 2014.

[14] M. Sasikumar and R. Shaikh, “Trust Model for Measuring Security Strength of Cloud Computing Service”, *Proceedings of International Conference on Advanced Computing Technologies and Applications*, pp. 380-389, 2014.

[15] L. Janczewski and A. Herrera, “Issues in the Study of Organisational Resilience in Cloud Computing Environments”, *Proceedings of International Conference on Health and Social Care Information Systems and Technologies*, pp. 32-41, 2014.

[16] F.D. Davis, “Perceived usefulness, Perceived ease of Use, and User Acceptance of Information Technology”, *MIS Quarterly*, Vol. 13, No. 3, pp. 319-340, 1989.

[17] S.L. Jackson, “*Research Methods: A Modular Approach*”, Cengage Learning, 2010.

[18] M.G. Morris, M.G. Davis and F.D. Davis, “User Acceptance of Information Technology: Toward A Unified View”, *MIS Quarterly*, Vol. 27, No. 3, pp. 425-478, 2013.