Institute of Advanced Engineering and Science

A Review of Trust Aspects in Cloud Computing Security

Azeem Sarwar*, Muhammad Naeem Ahmed Khan*
*Department of Computing, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad, Pakistan

Article Info

Article history:

Received Nov 22th, 2012
Accepted Dec 30th, 2012

Keyword:

Cloud Computing
SaaS
PaaS
IaaS
Cloud Security

ABSTRACT

Cloud computing offers distributed and shared computing resources and services that belong to different service providers and websites. Before truly benefiting from cloud computing, there are several issues associated to it which need to be addressed in the first place. One of the most important aspects that needs special attention pertains to the cloud security. Cloud computing has the important component as trust management. In this paper, we look at some security services practices like authentication, confidentiality and integrity as well as the trust management. A critical analysis of the trust models along with some gaps in the existing models is also reported herein.

Corresponding Author:

Muhammad Naeem Ahmed Khan,
Department of Computing,
Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad, Pakistan.
Email: mnak2010@gmail.com

1. INTRODUCTION

Cloud computing involves delivering hosted services over the Internet on demand. These services include software applications, software services, network resources, platforms, computing infrastructures and virtual servers. Cloud computing is scalable and managed infrastructure. End-users simply consume these services and pay on usage basis or subscription basis. There are three famous service models of cloud computing as described below:

- Software as a Service (SaaS). In this model, software application is hosted as service and end-users use the application on the web browser.
- Platform as a Service (PaaS): In this model, end-user creates, test and upload applications using tools and libraries hosted by the service provider.
- Infrastructure as a Service (IaaS): This model involves hosting of hardware computing services like storage, hard-drive, servers and network components. Service provider is responsible for maintenance and managing all these resources.

Security is the biggest issue in cloud computing as while utilizing storage service on a remote location, the consumers are generally unaware of what happens to their data. In fact, consumers themselves have less control to secure the data they host on the cloud. The trust mechanism has proven to be an appropriate substitute to the aforesaid security issues as it establishes entities’ relationship quickly and safely. Since trust is purely an abstract and a subjective term; therefore, it is ordinarily difficult to tangibally measure and effectively manage it.

In this paper, different security problems and trust models proposed in contemporary literature are critically reviewed and analyzed. This paper is organized into six sections. An introduction to cloud computing and its service models are described in this section. A review of the related work pertaining to the security issues, trust models and cloud computing frameworks is provided in section II. A critical evaluation of the literature review with respect to the current state of the affairs in cloud security is provided in the next section. The section IV highlights gaps in the security-related techniques discussed in the literature. An account of the challenges in cloud computing security is enunciated in section V. Some prospective dimension for further research in this area followed by the conclusion is outlined in the last section.

2. LITERATURE REVIEW

Mahmood [1] identifies that the major issues pertaining to data security in the cloud computing environment are:

- *Data Location and Data Transmission* — the customers may want that data should reside on a specific territory based on data polices and legislations within the certain country. Similarly, cross border transition of data (from one country to another) may lead to potential risks due to varying policies, regulations and legislations.
- *Data Availability* — the unavailability of data may lead to service outages.
- *Data Security* — when the data mobility is at high level, then security risks become the major concern, particularly, when data is transferred to another country with a different regulatory framework.

Behl [2] explores cloud computing security issues and highlights the key research challenges that include:

- *Availability and Performance* — this issue can be resolved through well-formed SLA (service level agreement) coined with real-time monitoring.
- *Malicious Insiders* — the cloud service providers cannot restrict their employees, contractors and other trusted people who have access to the secure data of customers through supply chain management.
- *Outside Attacks* — for example, the hackers can get access to the data; to resolve this issue, the network perimeter should be protected through firewalls.
- *Service Disruptions* — it can occur when no more resources are available for other customers and this may cause customer dissatisfaction. This issue can be resolved by ensuring that connections are coming from known IP pool and DNS (Domain Name Server).

A security strategy model is generally defined to overcome all the aforesaid security challenges. However, a generic security model is equally implementable for complex and ever dynamic cloud infrastructure. Chen et al. [3] discuss cloud computing data security and data privacy protection issues. The security architecture is defined at three levels: *software security* (identity authentication, identity management, access control), *platform security* (framework security, component security, interface security) and *infrastructure security* (virtual environment security, shared storage security). Data privacy protection issues of the data lifecycle in cloud computing include transfer, use, share, storage, archival and destruction.

Popovic et al. [4] indicate security issues of cloud computing systems by highlighting the problems of cloud computing, particularly, the security management models based on security standards and the security issues pertaining to security standards — such as the information technology infrastructure library (ITIL), ISO/IEC 27001/27002 and open virtualization format (OVF). The service providers can follow these guidelines to secure their cloud services. It is imperative to address the security issues aptly, as otherwise they could possibly result in unauthorized access to the systems that ultimately lead towards potential data corruption and compromising the confidential data.

Siani et al. [5] highlight that the major hurdles in large-scale acceptance of cloud computing, mostly due to service security and privacy issues. Based on the discussed scenarios, it is recommended that sensitive information should be minimized when data is processed on cloud and privacy to the end-user must be assured. A client based generic privacy manager tool has been proposed for this purpose that not only reduces security issues but also provides added privacy features.

Harauz et al. [6] highlight the regulatory and legal concerns associated with security issues. To avoid unauthorized access and to ensure data integrity, confidentiality and availability, the storage provider should offer encryption schema, strict access control mechanism and scheduled data backups. Adoptation of a universal standard is also recommended to ensure interoperability among service providers.

Shen et al. [7] analyze the security component of the trusted cloud computing systems through role-based access control model. It is stressed that the trusted cloud not only comprises of data security elements but also entails availability, reliability, integrity and safety. Security aspects have further been described as data confidentiality, the trust among the participant and dynamically building trust domains. For this purpose, a software middleware has been designed named as the Trusted Platform Software Stack (TSS) which makes use of security functions of Trusted Platform Model (TPM). TSS has two layers namely, the TSS service provider (TSP) and TSS core services (TCS). Application calls TSP function which sends a call to TCS and, in response, TCS authenticates the request in TPM order and returns the results to the upper layer. The proposed middleware provides hardware level authentication with the help of TPM, which makes the solution more secure from unauthorized access.

Gaurangkumar et al. [8] identify the potential barriers for cloud usage as the lack of consumer trust and complexity of compliance to make the cloud trustworthy. They ascertain the components of trust as security, privacy, accountability and auditability. To achieve the trust components in the cloud, the system controls are identified as preventive, detective and corrective. Further, a model is proposed to achieve trust in the cloud by applying preventive control on data requests. If the *request* is faulty, as ascertained through detective control, then the model makes a vulnerability log and generates the report accordingly; and if the *request* is not faulty then it is forwarded to service provider through the corrective control. Response is also validated through this model. However, the proposed model is not capable to support security and privacy components of trust.

According to Zou et al. [9], trusted cloud can be obtained through system security and trusted environment. Trusted Cloud Group (TCG), a group of cloud computing professionals, proposed an authenticated boot and platform attestation function which is implemented by TPM. A caveat to this model is that the security component of the proposed solution is only meant for service users and not for service providers.

Malluhi et al. [10] focus on building customers' trust for safety and security of their sensitive data. The identified trust factors include control, ownership, prevention and security. Further, the challenges for trust are identified as:

- *Diminishing Control* — it pertains to the lack of control over data stored and processed by third parties over the remote site.
- *Lack of Transparency* — the physical location of storage and security profiles of the site are major issues involved in it.

According to Li et al. [11], security is the biggest barrier in large-scale deployment and usages of cloud computing; therefore, traditional security mechanisms are not suitable for cloud. Rather trust mechanism is quick and safe mechanism for establishing entity relationship in distributed environment. A novel domain-based trust model is proposed for the security framework to ensure security of cloud computing. The proposed trust model is verified by using a simulation experiment. The experiments set up two evaluation factors: trust accuracy and transaction success rate. The disadvantage of proposed model is that it does not support the cross-cloud and large-scale environments.

Hassan et al. [12] discussed the following security challenges in cloud computing:

- *Authentication and Identity Management* — the data is made available to various services through Internet; therefore, an identity management is required to accommodate concerns related to protection of private data.
- *Access Control* — a role-based authentication is required to provide access in accordance with the privileges assigned to the user.
- *Policy Integration* — the different service providers offer different policies; however, these policies should be integrated when a user requires them together.
- *Service Management* — since different service providers offer different services, therefore, there should be a mechanism to integrate all these services to form a new composite service desired by the customer.
- *Trust Management* — the trust level is evaluated and updated periodically between users and service providers.

However, the proposed framework is only for service providers and not for service users. A security framework comprising the following components is required to be designed to fulfill aforesaid challenges:

- *Services Integrator* — it facilitates composing a new service through collaboration among different service providers.
- *Security Management* — it esupports authentication of users and services based on credentials.
- *Service Management* — it is responsible for secure service discovery.
- *Trust Management* — it pertains to establishing, negotiation and evolution of trust.

Habib et al. [13] argue that traditional methods to establish trust for service providers include SLAs, auditing, and self-assessment questionnaires. According to the research trends, trust management (TM) system are very useful for decision making for the selection of a cloud service provider that best suits the client's specific requirements. To incorporate attributes for trust establishment in the cloud world, a TM system requires specific properties like multi-faceted trust computation, trust customization, trust evaluation, trust representation, trust presentation and attack resistance. A TM system is designed in such a way that it usually has multiple components such as registration manager, consensus assessment initiative questionnaire engine, trust manager, trust semantics engine, trust computation engine and trust update engine. However, a caveat to such a model is that the proposed solution is only meant for service users to identify trustworthy service providers.

Sato et al. [14] focus on matters related to social insecurity of cloud and propose a model to overcome the insecurity issues. The proposed model is capable of creating the trust factor for both service provider and service users. For instance, the hosting of private data, which is ordinarily protected within an organization's embients, on a public cloud gives rise to the speculations and suspicions that third parties may get indirect or covert access to the data. Social insecurity is classified into the following three categories:

- *Multiple Stakeholder Problem* — since the data is delegated to different service providers operating under the umbrella of different organizations and each following different standards and policies.
- *Open Space Security* — as the client's data is stored on unknown places and above it, he/she is not offered any access control mechanism to put in place his/her policies for data security.
- *Mission Critical Data Handling* — the absence of secure handling of mission critical data could lead to serious issues. Therefore, to resolve these problems, the data security model should ensure *internal trust* and *contracted trust*. The *internal trust* is maintained through ID provision and key management. It could solve the multiple stakeholder and open space security problems. The *contracted trust* is established through a documentary contract between the organization and service provider. It solves the mission critical data handling because security enhancement is the only solution in this regard.

Nivetha [15] states that cloud computing have the potential for revolutionizing the traditional computing yet there is a considerable inadequacy in the area of security and risk assessment. One of the most severe limitations corresponds to the lack of consistency and adoption of standards in the areas of Information Security Management Systems (ISMS) which entail delineating a set of policies corresponding to the information security management. The ISMS are scalable and secure, which can be helpful for an organization to respond quickly to the market opportunities. In this regard, the CIA (confidentiality, integrity and availability) model is used to analyze how cloud computing needs to be more secure to scale across the diverse needs of the organizations.

3. CRITICAL ANALYSIS

The critical review of the surveyed literature on cloud computing security is provided in Table I.

Table I. Summary of Trust in Cloud Computing Security.

Author	Proposed Approach/Technique	Key Points
Mahmood [1]	Identification of major issues in cloud computing.	Various security aspects in cloud computing are discussed that can serve as a quick reference guide.
Behl [2]	Cloud computing security issues are discussed. A security strategy model is proposed to overcome the security challenges like availability of data, performance, malicious insiders, outside attacks and service disruptions.	The same security model is equally implementable for complex and dynamic cloud infrastructure.
Chen and Zhao [3]	Data protection and data privacy issues in the cloud computing are discussed.	Data security and protection issues covers all the data lifecycle components i.e., transfer, use, share, storage, archival and destruction of data.

Popovic [4]	Security issues in cloud computing.	Absence of comprehensive security policy could lead towards compromising the confidential data, unauthorized access and potential data corruption.
Siani and Miranda [5]	A client based privacy manager tool has been proposed that not only reduces security issues but also provides added privacy features.	The proposed tool is not generic and is limited to specific scenarios.
Harauz *et al.* [6]	Highlights the regulatory and legal aspects related to the security issues.	Since, rules and regulations vary from country to county; therefore, it has limited scope.
Shen [7]	A software middleware has been designed. Analysis of the security component of trusted cloud computing system through role-based access control model is recommended.	Proposed middleware provide hardware level authentication with the help of TPM, which makes the solution more secure.
Kumar and Minubhai [8]	Identification of the potential barriers to achieve trust in the cloud by applying preventive control on request/response.	The proposed model is not capable to support security and privacy components of trust.
Zou and Zhang [9]	Strategies to establish trust in cloud are discussed.	Model is proposed to overcome the limitations in TPM (Trusted Platform Model) developed by TCG.
Khan and Malluhi[10]	Identifies trust factors and the challenges to establish trust in cloud.	The identified trust factors include control, ownership, prevention and security.
Li *et al.* [11]	A domain-based trust model is proposed for security framework to ensure security of cloud computing.	Trust is quick and safe mechanism in establishing entity relationship in distributed environment. However, the proposed model does not incorporate cross-cloud and large scale environments.
Takabi *et al.* [12]	A security framework is designed comprising multiple components that include Services integrator, Security Management, Service Management and Trust Management.	Security challenges in cloud computing are discussed. Proposed framework is only for the consumption of service providers.
Habib *et al.* [13]	Trust management systems are useful to establish trust in cloud computing. Standard trust management system is evaluated.	Proposed solution is only meant for service users to identify trustworthy service providers.
Sato *et al.* [14]	A security model is proposed to overcome social insecurity issue that can result in insecurity for cloud environment.	Proposed model creates trust factor for both service provider and service users.
Nivetha [15]	Analysis is performed with the help of CIA (confidentiality, Integrity and availability) to show how organization can minimize the insecurity factor by adopting the standards like ISMS.	Specific standards can help organizations to assess the risks and overcome them. The proposed analysis can help organizations to control the factors that limit performance of private cloud e.g., lack of collaboration and synchronization.

4. GAP ANALYSIS

A number of security and trust models are discussed in the literature. The most frequently discussed model in the literature papers is the Confidentiality, Integrity and Availability (CIA) Model. Confidentiality means that information is not disclosed to unauthorized persons. Integrity means that information held in a system is accurate and proper representation of the data is achieved. Availability means that information processing resources are immediately isolated and discontinued when a malicious attack is detected. The essence of the model is to strike a balance among all these components but the literature only emphasizes on confidentiality and availability. An integrity component has been noticed as the least focused area in the contemporary research.

5. CHALLENGES IN CLOUD COMPUTING SECURITY

A number of challenges pertaining to the security aspects of cloud computing have been observed during the survey of contemporary literature for this study. Often users are much concerned about the security of their private and confidential data. After hosting data on the cloud, users feel the deprivation of control over their data; therefore, they remain suspicious about the security and confidentiality of the data. It is primarily because of their concern that who else has access to their data. For this very reason, the major challenge in cloud computing security is to prohibit unauthorized accesses and eliminate possibilities of data corruption in order to establish trust of the users on the cloud services. Moreover, sometimes service providers opt for subcontracting certain services either to scale-up their own service or get benefited from the bargains offered by other cloud vendors. In such a scenario, the subcontracted service providers are generally bound to totally different rules and regulations that are indigenous to their country. For instance, the UK government has imposed stricter rules for data privacy and security as compare to USA. In case a UK-based organization subscribes to a service provider in USA then the USA-based service provider is not obligated for any sort of data corruption compensation due to variations in rules and regulations in both the countries.

Cloud infrastructure can be complex enough as it can consist of “cloud within the cloud” architecture. It is quite impossible for service providers to claim about their servers as 100% live all the time. Sometimes, subscriber enterprises and organizations have to pay more monies because of the service provider’s superfluous claim which they cannot verify. Another major issue in cloud computing is to maintain trust between the tenant and the vendor. Trust factor is equally applicable for service providers as well as service users. Service users are mostly concerned about the security, privacy, confidentiality and availability of their data but, on the other hand, service providers are touchier about the faithfulness and integrity of the users.

6. CONCLUSION AND FUTURE WORK

Cloud computing is the on-demand utilization of shared computing resources available from the Internet. When these services are used properly, they can reduce cost and management responsibilities in addition to increasing efficiency, agility and performance of an enterprise. On the contrary, there are several challenges to be faced by cloud computing such as data security and privacy issues. In this paper, we have discussed the issues related to data location, storage, security, availability and integrity. Establishing trust is the way to overcome these security issues as it establishes entities’ relationship quickly and safely. For this purpose, we have surveyed some of the trust management models. Since trust is an abstract and subjective term; hence, it is difficult to measure and manage the trust.

In this paper, we have conducted a review of literature on the trust management systems. Majority of the proposed systems put special emphasis on the CIA (Confidentiality, Integrity and Applicability) model. Based on the critical analysis and the gap analysis provided in section III and IV respectively, we intend to conduct research on integrity issue as a continuum to this research.

REFERENCES

[1] Z. Mahmood, “Data Location and Security Issues in Cloud Computing,” IEEE International Conference on Emerging intelligent Data and Web Technologies, 2011.

[2] A. Behl,”Emerging Security Challenges in Cloud Computing”, IEEE international Conference Information and Communication Technologies (WICT), 2011.

[3] D. Chen, H. Zhao, “Data Security and Privacy Protection Issues in Cloud Computing”, IEEE International conference on Computer Science and Electronics Engineering, 2012.

[4] K. Popovic, Z. Hocenski,”Cloud Computing security issues and challenges”, MIPRO, Proceedings of the 33rd International Convention, 2010.

[5] Siani and Miranda, “Security Threats in cloud computing”, 6th international Conference on Internet Technologies and Secure Transactions, 2011.

[6] J. Harauz, L. M. Kauifman and B. Potter. (2009). Data Security in the world of cloud computing. Security & Privacy, IEEE. 7 (4), p61-64.

[7] Z. Shen, L. Li, F. Yab, X. Wu, “Cloud Computing system based on Trusted computing platform”, International Conference on Intelligent Computation technology and Automation, 2010.

[8] K. G. Kumar and ChaudhariMinubahi, “To Achieve Trust in the Cloud”, Second International Conference on Advanced Computing & Communication Technologies, 2012.

[9] B. Zou and H. Zhang, "Toward enhancing trust in cloud computing environment", 2nd International Conference on Control, Instrumentation and Automation, 2011.

[10] K. M. Khan and Q. Malluhi. (2010). Establishing Trust in Cloud Computing. *Cloud Computing*. 12 (5), pp. 20-27.

[11] W. Li, L. Ping and X. Pan, "Use Trust management module to achieve effective security mechanisms in cloud environment", International Conference on Electronics and Information Engineering, 2010.

[12] H. Takabi, D Joshi and G. Ahn, "SecureCloud: Towards a comprehensive security framework for cloud computing environment", 34th Annual IEEE Computer Software and Applications Conference Workshops, 2010.

[13] S. M. Habib, S. Ries and M. Muhlhauser, "Towards a trust management system for cloud computing", IEEE Computer SocietyWashington, DC, USA, 2011

[14] H. Sato , A. Kanai and S. Tanimoto, "A Cloud trust model in a security aware cloud", 10th Annual International Symposium on Applications and the Internet, 2010

[15] S. Nivetha, "Assessing the Risks and Opportunities of Cloud Computing – Defining Identity Management Systems and Maturity Models", International Conference on Computing and Control Engineering, 2012.

BIOGRAPHY OF AUTHORS

Azeem Sarwar is pursuing for MS in Computing at Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad, Pakistan. His research interests include Cloud Computing and Software Architecture.

Muhammad Naeem Ahmed Khan obtained D.Phil. degree in Computer System Engineering from the University of Suusex, Brighton, England. His research interests are in the fields of software engineering, cloud computing, cyber administration, digital forensic analysis and machine learning techniques.