Conference Proceeding Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Cloud Computing Security Challenges, Approaches and Solutions: A Review

Menangsosang Pongen
Student, M.Sc Computer Science, Indian Academy Degree College, Bangalore, India

Abstract: Cloud computing have been widely adopted into the mainstream than any other technology in the domain. According to Cloud Security Alliance (CSA), over 70 percent of the world's businesses now operate – at least in part – on the cloud. This adoption has been fueled mainly by the ever-increasing number of smartphones and mobile devices that can access the internet. Cloud computing is not just for organizations and businesses; it's also useful for the average person as well. It enables us to run software programs without installing them on our computers; it enables us to store and access our multimedia content via the internet, it enables us to develop and test programs without necessarily having servers and so on. As such, security has been one of the most challenging issues for the IT executives particularly in cloud implementation. In fact, numerous security challenges face the cloud as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. In this paper, I have surveyed several research work on the security issues of cloud computing. The goal of this paper is to provide a better understanding of the security challenges currently facing cloud computing and determine different approaches and solutions which have been adopted by the cloud service industry.

Keywords: *Cloud Computing, Cloud Service.*

I. INTRODUCTION

1.1 Cloud Computing is the next generation internet based computing system which provides easy and customizable services to the users for accessing or to work with various cloud applications. Cloud Computing provides a way to store and access cloud data from anywhere by connecting the cloud application using internet [1].

Buyya et al.,[2], have defined it as follows: "Cloud is a parallel and distributed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements (SLA) established through negotiation between the service provider and consumers."

1.2 Despite the tremendous business and technical advantages of the cloud, the security and privacy concern has been one of the major hurdles preventing its widespread adoption. Especially for outsourced data services, the owners exclusive control over their data is ultimately relinquished to the CSPs [3]. For example, Google's recent privacy policy implies that they essentially own the right to arbitrarily handle the uploaded user data [4]. As a result, from the data owners point of view, whenever their outsourced data contain sensitive personal information, such as financial and medical records, and social network profiles, it can no longer be considered as private as before. On the other hand, although in reality CSPs usually enforce data security through mechanisms like firewalls and virtualization, these measures do not fully guard against threats of unauthorized data access from insiders, outsiders, or other cloud tenants due to the non-bug-free deployment and low degree of transparency. Infamous data breach incidents occur from time to time, such as the recent Sony PlayStation data breach and DropBox privacy leakage.

II. REVIEW OF LITERATURE

Dimitrios Zissis et al.,[5], proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust[5]. In this paper they have identified generic design principles of a cloud environment which stem from the necessity to control relevant vulnerabilities and threats. To do so, software engineering and information systems design approaches were adopted. Security in a cloud environment requires a systemic point of view, from which security will be constructed on trust, mitigating protection to a trusted third party. A combination of PKI, LDAP and SSO can address most of the identified threats in cloud computing dealing with the integrity, confidentiality, authenticity and availability of data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh through federations, within which essential trust is maintained.

Farrukh Shahzada [6], has surveyed several research work on cloud computing related to security challenges and privacy issues. The primary goal of the paper was to provide a better understanding of the security challenges of cloud computing and identify approaches and solutions which have been proposed and adopted by the cloud service industry [6]. The revolution of cloud computing has provided opportunities for research in all aspects of cloud computing. He presented the five essential characteristics of cloud computing, three cloud service models, and four cloud deployment models. The paper also states that research in the secure cloud storage is compounded by the fact that users' data maybe kept at several locations for either redundancy/ fault tolerance or because the service is provided through a chain of service providers. They have also explored the security measures adopted by the largest cloud service provider(Amazon web services or AWS) including their infrastructure security and security best practices followed by AWS.

R. Velumadhava Rao et al.,[7], has highlighted data related security challenges in cloud based environment and solutions to overcome. It addresses the requirement for great emphasis on Data Security and Privacy as we are moving into internet based cloud model as Data loss or Data leakage can have severe impact on business, brand and trust of an organization. It also states that Data leak prevention is considered as most

important factor with 88% of Critical and Very important challenges. Similarly, Data Segregation and Protection has 92% impact on security challenges. This paper addresses data security challenges and solutions are provided for these challenges to overcome the risk involved in cloud computing [7].

B. Hari Krishna et al.,[8], has addressed security issues in service model of cloud computing environment are highlighted such as the threats facing cloud computing, cloud computation implementation guidelines, issues of security to clarify before adopting cloud computing. In their future work, they will include the different cryptographic-algorithms to solve the security problems in cloud computing [8].

Naresh Vurukonda et al., [9], identifies the issues related to the cloud data storage such as data breaches, data theft, and unavailability of cloud data. And also provides possible solutions to respective issues in cloud. In this study we focused on data storage security issues in cloud computing and we first provided service models of cloud, deployment models and variety of security issues in data storage in cloud environment. In the final section, we addressed possible solutions for the data storage issues that provide privacy and confidentiality in cloud environment[9].

Gururaj Ramachandra et al.,[10], objective of their research was to understand the cloud components, security issues, and risks, along with emerging solutions that may potentially mitigate the vulnerabilities in the cloud. As it is a commonly accepted fact that since 2008, cloud is a viable hosting platform; however, the perception with respect to security in the cloud is that it needs significant improvements to realise higher rates of adaption in the enterprise scale. As identified by another research, many of the issues confronting the cloud computing need to be resolved urgently. The industry has made significant advances in combatting threats to cloud computing, but there is more to be done to achieve a level of maturity that currently exists with traditional/on-premise hosting. In this study they have focused on data storage security issues in cloud computing and provided service models of cloud, deployment models and variety of security issues in data storage in cloud environment. In the final section, they have addressed possible solutions for the data storage issues that provide privacy and confidentiality in cloud environment [10].

P. Ravi Kumar et al.,[11], explores the different data security issues in cloud computing in a multi-tenant environment and proposes methods to overcome the security issues. This paper also describes Cloud computing models such as the deployment models and the service delivery models. In any business or Cloud Computing data are exceptionally important, data leaking or corruption can shatter the confidence of the people and can lead to the collapse of that business. Currently cloud computing is used directly or indirectly in many businesses and if any data breaching has happened in cloud computing, that will affect the cloud computing as well as the company's business. This is one of the main reasons for cloud computing companies to give more attention to data security[11].

Dawei Sun et al.,[12] primarily focuses to highlight the major security, privacy and trust issues in current existing cloud computing environments and help users recognize the tangible and intangible threats associated with their uses, which includes: (a) surveying the most relevant security, privacy and trust issues that pose threats in current existing cloud computing environments; and (b) analyzing the way that may be addressed to eliminate these potential privacy, security and trust threats, and providing a high secure, trustworthy, and dependable cloud computing environment[12]. In the future, they will further do analysis and evaluate privacy, security and trust issues in cloud computing environment by a quantifiable approach, further develop and deploy a complete security, privacy trust evaluation, management framework on really cloud computing environments.

CONCLUSION

With so many recent breaches and technological attacks, maintaining security in Cloud service industry has become more important than ever. Companies are now becoming more and more particular about risks. Organizations are increasingly looking for Cloud service providers which are stable, secure and offer more than one layer of security for their client's data.

This paper primarily highlighted the various research work done in facing security challenges concerning Cloud Computing covering the aspects of security threats, privacy, trust issues, key encryption and vulnerabilities. Recent developments in cloud computing such as Container-as-a-Service (CaaS), Software-defined networking (a concept to design and manage networks that abstracts applications away from the underlying networks), Software-defined-storage (abstracts the logical storage services and capabilities away from the underlying hardware) and Cloud-of-Things (CoT), (a concept combining cloud computing and Internet-of-Things (IoT) for smart city applications). All these new developments bring new challenges in cloud computing and they need to be addressed.

References

[1] Foster, I., Zhao, Y., Raicu, I., Lu, S.. Cloud computing and grid computing 360-degree compared. In: Grid Computing Environments Workshop, 2008, p. 1–10.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility, Future Generation Computer Systems, 2009.

[3] Zhang, Q.,Cheng, L.,Boutaba, R.. Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 2010.

[4] Li, M., Yu, S., Ren, K., Lou, W., Hou, Y.. Toward privacy-assured and searchable cloud data storage services. Network, IEEE 2013.

[5] Dimitrios Zissis, Dimitrios Lekkas, Addressing cloud computing security issues, Future Generation Computer Systems, 2010.

[6] Farrukh Shahzada, State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions, The 6th International Symposium on Applications of Ad hoc and Sensor Networks, 2014.

[7] R. Velumadhava Rao, K. Selvamanib, Data Security Challenges and Its Solutions in Cloud Computing, International Conference on Intelligent Computing, Communication & Convergence, 2015.

[8] B. Hari Krishna, Dr.S. Kiran, G. Murali , R. Pradeep Kumar Reddy, Security Issues In Service Model Of Cloud Computing Environment , International Conference on Computational Science, 2016.

[9] Naresh Vurukonda, B.Thirumala Rao, A Study on Data Storage Security Issues in Cloud Computing, 2nd International Conference on Intelligent Computing, Communication & Convergence, 2016.

[10] Gururaj Ramachandra, Mohsin Iftikhar, Farrukh Aslam Khan, A Comprehensive Survey on Security in Cloud Computing, The 3rd International Workshop on Cyber Security and Digital Investigation, 2017.

[11] P. Ravi Kumar, P. Herbert Raj, P. Jelciana, Exploring Data Security Issues and Solutions in Cloud Computing, 6th International Conference on Smart Computing and Communications, 2017.

[12] Dawei Sun, Guiran Chang, Lina Sun and Xingwei Wang, Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments, Elsevier Ltd, 2011.