A Literature Review on Security Issues in Cloud Computing

T. Sainath, Prof Dr.B.Indira Reddy

CNIS, M.Tech Sreenidhi Institute of Science & Technology, Hyderabad, Telangana, India

ABSTRACT

The use of Cloud Computing has increased rapidly in many organization .Cloud Computing provides many benefits in terms of low cost and accessibility of data. In addition Cloud Computing was predicted to transform the computing world from using local applications and storage into centralized services provided by organization. Ensuring the security of Cloud Computing is major factor in the Cloud Computing environment. Security and privacy are the key issues for Cloud Computing and still face some huge challenges. This article contains a review of technical literatures relating security challenges and security issues of Cloud Computing. I review the methodology and consequently solution, analysis, finding and other main points in these lectures. So the purpose of this paper is to search out various issues in cloud computing where all computing is done on the server side and both data & tasks are stored on the data centers.

Keywords : Cloud Computing, Service Level Agreement (SLA), IaaS, PaaS, SaaS, Cloud computing, data threats, information security, data security, threats in security, Security service, FPGA

I. INTRODUCTION

Cloud Computing is using internet as a communication media. The dealer has to provide some assurance in service level agreements (SLA) to convince the customer on security issues. They provide different services like Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a service (IaaS). The SLA has to describe different levels of security and their complexity based on the services to make the customer understand the security policies that are being implemented.

II. RELATED WORK

Writers put forward some security issues that have to be included in SLA. But they only discussed about the services provided and the waivers given if the services not met the agreement, but this waivers don't really help the customers fulfilling their losses.

The waivers have to be made according to the type of business done by the patrons. Besides the waivers the SLA has to discuss about many other issues like security policies, methods and their implementations. [1]

They have introduced a new cloud security management framework based on aligning the FISMA standard to fit with the cloud computing model. They have developed a proof of concept of their framework using .NET and have deployed it on a tested cloud platform. They have evaluated the framework by managing the security of a multitenant SaaS application paradigm. They have utilized the existing security automation efforts such as CPE, CWE, CVE and CAPEC to facilitate the cloud services Security Management Process (SMP).At the whole, The framework can be used by cloud providers to manage their cloud platforms security, by cloud consumers to manage their cloud hosted assets security, and as a security as a service

tool to help cloud consumers in outsourcing their internal SMP to the cloud platform.[2]

New strategy toward delivering cloud computing protection by using reconfigurable computing. It has been extrapolated components of the cloud from software based solution to hardware .Four different types of solutions are being proposed to ensure user data security. These four solutions are: (i)Trusted Platform, (ii)User Enabled Collaboration Mechanism using Security Groups (iii)Data Security, (iv)CSU and CSV confirmation. All four of these solutions ensure that the security is enabled by the Client. [13]

"Cloud SSDLC", a cloud security self-governance deployment framework is proposed from the system development life cycle perspective (Cloud SSDLC), and especially from government and industry perspectives. The cloud SSDLC incorporates the secure system development life cycle (SSDLC), cloud security critical domain guidelines, and risk considerations.

According to the SSDLC, there are five main phases in

Cloud SSDLC:

Initiation, development, implementation, operation, and destruction. From the industry and government perspective, different cases are used to demonstrate practical usage and legal issues in the proposed Cloud SSDLC. The main contributions are:

✓ To provide a framework to connect the SSDLC and cloud computing paradigm for enhancing cloud application security.

✓ To specify the significant security concern in each cloud service development phase.

✓ To leverage the proposed framework in order to analyze a real case in government cloud services migrations. [17]

✓ There are two detailed analyses of the cloud security problem in two essay (art05, art06). Both of them have investigated the problem from the cloud architecture perspective, the cloud offered characteristics perspec-tive, the cloud stakeholders' perspective, and the cloud service delivery models perspective.

✓ Base on the fifth essay's analysis the main cloud security problems are summarized as follows:

✓ Some of the security problems are inherited from the used technologies such as virtualization and SOA.

✓ Multi-tenancy and isolation is a major dimension in the cloud security problem that requires a vertical solution from the SaaS layer down to physical.

✓ Security management is very critical to control and manage this number of requirements and controls.

✓ The cloud model should have a holistic security wrapper.

✓ But they believe, currently security has lot of loose ends which scares away a lot of potential users. Until a proper security model is not in place, potential users will not be able to leverage the advantages of this technology. They will focus on:

o Propose the security model that should be adopted in each part of the cloud computing stake.

o Standardizing Cloud computing security protocols.

o Propose an agreement document model (SLA) that discusses the security policies and methods of their implementations.

But they need to:

1. Capture different stakeholders' security requirements from different perspectives and different levels of de-tails;
2. Map security requirements to the cloud architecture, security patterns and security enforcement mechanisms;
3. Deliver feedback about the current security status to the cloud providers and consumers.[19]

Based on the details and facts that have explored we have summarized the cloud security issues as follows:

a. some of security implications are inherited from the technologies such as virtualization.

b. Multi-tenancy is another realm which requires maximum attention to control any attacks on victim resources from malicious users.

c. Cloud security management is very significant to control and manage the user facing data and the way provider's infrastructure functions.

d. The cloud model should have a holistic security wrap-per that any access to any object of the cloud platform should pass through multilayer security solution.

Base on their analysis they have recommended that cloud computing security solution should at least incorporate their solutions until consumer/tenant is assured of its data privacy. They are investigating the vivid cloud security issues and their objective to present a solution to various cloud security issues.[13]

The article with subject" Security Concerns in Cloud computing" is speaking about providing comprehensive study of cloud computing security that includes classification of known security threats and the state of the art practices in the endeavor to calibrate these threats. The 43 issues and 6 categories provided in this study focuses on the concept of preventive rather than proactive solutions.

Analysts believe that the cost reduction factor in cloud computing will further accelerate the adoption of cloud computing in public sectors. They have identified few areas which are still unattended in cloud computing security such as auditing, side channels and migration of data from one cloud to another. Emphasis has always been on fast performance and low cost but the quality of service has not been considered. In addition, research on mobile plat-form with respect to cloud computing is another open re-search issue. They have written Less memory, power and limited computational capability creates hurdle in order to provide best performance to mobile user.[14]

Table1. Issues Categories

Sr. #	Category
C1	Safety Standards
C2	Network
C3	Access
C4	Cloud Infrastructure
C5	Data
C6	Other

The article with subject "A New Technique of Data Integrity for Analysis of the Cloud Computing Security" is consist of a detailed analysis of the cloud security problem. Also the different problem in a cloud computing sys-tem and their effect upon cloud users, various computing system and organizations are analyzed.

They have believed, that data storage security in Cloud Computing, an area full of challenges and of paramount importance, is still in its infancy now, and

many research problems are yet to be identified. their design and development is mainly based on the usage of Public and Private key encryption system. It supports dynamic outsourcing of information make it a more realistic application of cloud computing . They have believed that work on mapping security requirement to the cloud architecture, and developing some security algorithm for cloud systems will be carried on. These security algorithms may be either Software based e.g. Encryption based or may be Hardware based e.g. Disk encryption hardware. It will help in improving the security of cloud systems and hence will lead to remove the fear of data security among users in Cloud Computing.[17]

"A Research on Cloud Computing Security" is the literature that gives an overview on cloud computing security. It presents a definition and scope of cloud computing and the security impacts of cloud security for both customers and operators are analyzed. To overcome challenges from cloud security, many state-of-the-art technical solution e.g. continuation protection mechanism, IDM, data security and virtualization security are discussed. At the end of this lecture, the best practices are proposed for operators to overcome shortcoming in cloud computing as follows:

- ✓ Operators should consider how to safely evolve to cloud platform from traditional one with keeping continuity of service.
- ✓ Operators should pay attention how to solve problem related to data security in their own clouds.
- ✓ Operators should provide customers a sophisticated virtualization security solution to keep IaaS service work-ing well.
- ✓ Operators should monitor any attacks against their cloud services, and figure out a way to incident response.

1. Operators should identify application security problems for different service models (SaaS, PaaS, and IaaS) respectively.

2. Operators should consider legal issues and customers benefit carefully when they are to deploy any security schemes in cloud. [18]

III. CONCLUSION

It is clear that although the use of Cloud Computing has rapidly increased, Cloud Computing security is still considered the major issue in the Cloud Computing environment. Yet guaranteeing the secure of corporate data in the cloud if difficult, is not impossible. In this work, I have reviewed the research about security in cloud computing and I have summarized them in my lecture.

In summary, as data security measures over the Cloud continue to develop; new issues may appear which will require further up-to-date research. Future research should focus on the rapidly growing Computing do-main by studying deeply and critically the security threats and issues that users encounter in order to prescribe appropriate measures and solutions.[19]

IV. REFERENCES

1. BKandukuri, R.Paturi And R.Rakshit." Cloud Securi-ty Issues".in: IEEE International Conference on Services Computing,(pp.517&520. 2009

2. M Almorsy, J. Grundy and A. S. Ibrahim. "Collabo-ration-Based Cloud Computing Security Management Framework".in: IEEE 4th International Conference on Cloud Computing.(pp. 365&371. 2011

3. Alexa Huth and James Cebula,"The Basics of Cloud Computing" Carnegie Mellon University. Produced for US-CERT, 2011

4. Farzad Sabahi, "Cloud Computing Security Threats and Responses", 2011 IEEE 3rd International

Conference on Communication Software and Network (ICCSN, pp. 245-249, May 2011.

5. R Buyya, J. Broberg and A. Gosscinnski. 'Cloud computing.' Hoboken, N.J.: Wiley; 2011.

6. JMMondol."Cloud security Solution using FPGA". In:IEEE . (pp.747&751-752. June 15, 2011.

7. JJ Hwang, Taoyuan, Taiwan, Y.C. Hsu and C.H. Wu. 'A Business Model for Cloud Computing Based on a Separate Encryption and Decryption Service.' International Conference on Information Science and Applications (ICISA, pp 1-7, 2011.

8. TKao, Ching-Hao.Mao, Chien-Yu.Chang and Kai-Chi Chang. "Cloud SSDLC:Cloud Security Governance Deployment Framework in Secure System Development Life Cycle". In: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communi-cations.(pp.1143&1147.2012.

9. Satveer Kaur and Amanpreet Singh, "The Concept of Cloud Computing and Issues Regarding its Privacy and Security", International Journal of Engineering Research & Technology (IJERT, Vol. 1 Issue 3, May 2012.

10. A Bouayad, A.Bliliat, N.Mejhed And M.Elghazi." Cloud computing: security challenges".in:IEEE. (pp.26&31.2012.

11. JK. Wang and X. Jia. 'Data security and authentication in hybrid cloud computing model.' IEEE Global High Tech Congress on Electronics, pp 117- 120, 2012.

12. Sandip A.kale, Prof S.V Kulkarni, Department of CSE of MIT Aurangabad.Data Leakage Detection International journal of Advanced Research in Computer and Communication Engineering Vol 1, Issue 9, November 2012

13. ABehl, K.Behl. "An Analysis of Cloud Computing Se-curity Issues".in:IEEE.(pp.109&113-114.2012.

14. I M. Khali and A.Khreishah." Security Concerns in Cloud Computing".in:10th International Conference on Information Technology.(pp.411&414-415.2013.

15. Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD International Journal of Computer Science and Information Technology, Vol.2(3, 242-249, 2012

16. F Moghaddam F, Karimi O and Alrashdan M T. 'A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments.' Proceedings IEEE

2nd International Conference on Cloud Networking (CloudNet, San Francisco, USA, pp 185-189, 2013

17. RChalse, A.Selokar and A.Katara." A New Technique of Data Integrity for Analysis of the Cloud Computing Security".in: 5th International Conference on Compu-tational Intelligence and Communication Networks. (pp.469&472.2013.

18. NZhang, D.Liu and Yun-Yong Zhang."A Research on Cloud Computing Security".in: International Con-ference on Information Technology and Applications. (pp.370&373.2013.

19. L A. Maghrabi." The Threats of Data Security over the Cloud as Perceived by Experts and University Students".in:IEEE.(pp.1&5.2014.

20. N Sengupta and R. Chinnasamy. 'Contriving hybrid DESCAST algorithm for cloud security.' Elsevier, pp 47-56, 2015

21. Kang II Choi, Jung Hee Lee, Bhum Cheol Lee. Network Computing Convergence Lab, ETRI, Daejeon, Korea. ICACT Transactions on Advanced Communications Technology(TACT Vol.5, Issue 3, May 2016

22. Savitha D Torvi, Dr. K B Shivakumar, Rupam Das. AN UNIQUE DATA SECURITY USING TEXT STEGANOGRAPHY. 2016 International Conference for Sustainable for Global Development(INDIACom

23. Shweta Singh1 M. Tech Scholar, Department of CSE, Jamia Hamdrad University, Delhi, India. International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 6 (2017, pp. 1419-1429

24. Tabrez Nafis2 Assistant Professor , Department of CSE, Jamia Hamdrad University, Delhi, India. International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 6 (2017, pp. 1419-1429