International Conference on Advances in Engineering Management & Sciences - ICEMS -2017

A Study of Data Security and Security Mechanisms of Cloud Service Providers

K.K. Nikhil[1] S.A.Poojitha[2]
Assistant Professor, Department of CSE, MLRITM, India
Email ID : krishnakishore.kk@gmail.com

Abstract – **Cloud computing is one of the expanding innovation that is associated with Grid Computing, Utility Computing, Distributed Computing. In today's world, securing of information assumes an indispensable part. In the processing condition, information protection and information security is prevalent in fields like government, industry, education organizations and business for the future advancement. These are inter-related to both hardware and software. Consequently, this paper analyses the information security solutions and security mechanisms of cloud service providers in Cloud Computing.**

Keywords – **HaaS, DaaS, SaaS, IaaS.**

I. Introduction

Cloud computing provides a new way of services by organizing various resources and providing them to users based on their demands. Cloud computing and storage solutions provide users and enterprises with various strengths to store and process their data in third-party data centers that may be situated far from the user–ranging in distance from across a city to across the world. There are two basic types of functions in Cloud computing. They are computing and data storage. Storing data in the cloud greatly decreases storage load of users and brings them access comfort, thus it has become one of the most important cloud services.

The cloud models are infrastructure as a Hardware as a service (HaaS), users could buy IT hardware - or even an entire data center/computer center - as a pay-as-you-go subscription service. The HaaS could be flexible, scalable and manageable to meet your needs. Software as a service (SaaS) which completes all the application are on the internet. Data as a service (DaaS) Data in various formats, from various sources, could be accessed via services to users on the network.

Data security is more muddled than data security in the conventional data frameworks. Cloud computing security is one that is more essential to be tended to these days. In the event that security measures are not given appropriately, then Data operations and transmissions will be at high risk [1]. To deal with these difficulties, most grounded security measures are to be made and it must be executed by distinguishing security test and its solutions [2]. The trust issues, security issues and privacy were given by sun et al [3]. A data security framework for cloud computing networks is proposed [4]. Younis and Kifayat give a survey on secure cloud computing for critical infrastructure [5]. The privacy will be used to study about the tangible threats and also the intangible threats, some of the issues in data security were privacy of data, protecting the data, availability of data, etc. The various challenges in the security were loss of data, data threats and malicious attacks from outsiders [6]. By using the cloud security techniques and the data segregation Chen and Zhao [7] analysed and presented the issues in the cloud computing environment through the data privacy and security. The most challenging issue in cloud computing is data sharing.

II. Cloud Security Controls

The different types of cloud security controls will fall under any one of the following category:

1. Deterrent Controls: These controls are intended to reduce attacks on a cloud system. deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed
2. Preventive Controls: The system strength can be given by the preventive controls which can be against like any of the incidents like eliminating the vulnerabilities.
3. Detective Controls: Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue
4. Corrective Controls: By limiting the damage this Corrective controls reduce the consequences of any incident.

III. Data Integrity

Data integrity is one of the most critical element in most of the information system. This will protects the data from modification, fabrication or from deletion. Through database constraints and transactions, data integrity is done by the database management system which is maintained in the standalone systems. Data integrity acts as the basis to provide services in cloud computing such as IaaS, SaaS, and PaaS. RAID-like strategies can be used to obtain Data integrity easily. Bowers et al. an author proposed a theoretical framework known as "Proofs of Retrievability" to be aware of the remote data integrity checking by combining spot checking and error correction code [8].

IV. Data Confidentiality

In cloud, for the users to store the confidential data, data confidentiality is very essential. It can be ensured that data confidentiality and data authentication strategies are used as shown in Table1 & Table2. The access control, data confidentiality and data authentication can be addressed by increasing the trustworthiness and the reliability of cloud. The problem of Key management can be faced with the Simple encryption, it does not support complex requirements like query, parallel modification, and fine-grained authorization.

(i) *Homomorphic Encryption*

Confidentiality of data can be ensured by using encryption. Rivest et al [9] proposed this system of encryption. There is a consistent algebraic operation with cipher text with the clear operation. Very high complicated calculation are included in this encryption system. The cost of computing and the storage is very high.

(ii) *Encrypted Search and Database*

The most inefficient encryption is homomorphic encryption. So in the cloud environment researchers started to learn the limited homomorphic encryption application algorithm. Encrypted search is the one of the most common operation. A lightweight mechanism for database encryption which was proposed by Manivannan and Sujarani have and it is known as transposition, substitution, folding, and shifting (TSFS) algorithm. An asymmetric encryption mechanism for databases was proposed by Huang and Tso in the cloud. When more than once the commutative encryption is applied on to the data, the private/public key order is very useful for decryption/encryption which does not matter.

(iii) *Distributive Storage*

Distributive storage of data is one of the promising approach in the cloud environment. AlZain et al [10] discussed the security issues which is relating to data privacy in the cloud computing including integrity of data and availability of service in the cloud environment. Internal or external data are divided into chunks to protect them from unauthorized access. Ram and Sreenivaasan [11] have proposed a technique known as security-as-aservice (saas) which is for securing data in cloud. The maximum security can be achieved by dividing the user's data into pieces.

(iv) *Hybrid Technique*

For data confidentiality and data integrity hybrid technique is used. This uses both the authentication and key sharing techniques. By making process more secure, powerful key sharing and authentication process are used, and also the user and the cloud service provider can also be connected. The data security technique is proposed in three-layered structure [12]: the first layer is used for authenticity of the cloud user. It can be either by one factor authentication or by two factor authentications; the second layer is for ensuring protection and privacy by encrypting the user's data; and the third layer will do the fast recovery of data by a speedy process of decryption.

(v) *Data Concealment*

Data concealment is also be used to keep the data confidentiality in the cloud environment. Delettre et al [13] introduced this data concealment concept for database security. This technique will combine the real data with the visual fake data to make real data as the negative (false) one. The overall volume of real data can be increased by b Data concealment but it provide enhanced security for the private data. The main objective is that to secure the real data from other malicious attackers or other users.

(vi) *Deletion Confirmation*

Deletion confirmation means after the deletion confirmation when users delete their data that data cannot be recovered. When data gets deleted by the users, the data of all the copies should get deleted at the same time. This should be ensured by the cloud storage providers.

V. Data Privacy

The ability of an individual or a group of persons to seclude the information about themselves and reveal them in a selectively. Oblivious RAM technology (ORAM) was mostly focused by the researchers. ORAM technology have been used in protection of software and protecting the privacy in the cloud computing as a promising technology. Stefanov et al. stated that a path ORAM algorithm is state-of-the-art implementation [14].

(i) *Service Abuse*

Service abuse means that attackers may abuse the cloud service and acquire the extra data available or destroy the interest of other users. User data may be abused by other users. In the cloud storage the most used technology is De-duplication. It means that data which is often are stored, can be shared by multiple users.

(ii) *Averting Attack*

Cloud systems should be efficient of averting Denial of Service (DoS) attacks. in cloud computing requirement of security services was analyzed by Shen et al [15]. Trusted platform support services (TSS) and trusted computing platform (TCP) for integrating cloud services. The trusted model should bear characteristics of dynamically building trust domains and dynamic of the services and with confidentiality. Yeluri et al. focused on the cloud services from security and explored security challenges in cloud when deploying the services [16].

VI. Conclusion

Everyone wants to use the cloud for cost savings and also for new business models. But for cloud security, it is very important to understand the different threats that comes into play, **sa**ys Derek Tumulak. Cloud is a promising technology for the future IT applications. The main requirement of an organization were reducing data storage and processing cost. The analysis of data and information is the most important tasks in all organizations to make the decisions. So, the will not be transferred by an organizations to the cloud till there is a trust between the cloud service providers and consumers.

References

[1] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable and fine-grained data access control in cloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9.

[2] R. Velumadhava Raoa, K. Selvamanib, "Data Security Challenges and Its Solutions in Cloud Computing" in proceedings of the International Conference on Intelligent Computing, Communication & Convergence (ICCC-2015) Conference Organized by Interscience Institute of Management and Technology, Bhubaneswar, Odisha, India

[3] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," in Proceedings of the International Conference on Advanced in Control Engineering and Information Science (CEIS '11), pp. 2852–2856, chn, August 2011

[4] A. Pandey, R. M. Tugnayat, and A. K. Tiwari, "Data Security Framework for Cloud Computing Networks," International Journal of Computer Engineering & Technology, vol. 4, no. 1, pp. 178– 181, 2013.

[5] M. Y. A. Younis and K. Kifayat, "Secure cloud computing for critical infrastructure: a survey," Tech. Rep., Liverpool John Moores University, Liverpool, UK, 2013.

[6] A. Behl, "Emerging security challenges in cloud computing: an insight to cloud security challenges and their mitigation," in Proceedings of the World Congress on Information and Communication Technologies (WICT '11), pp. 217–222, IEEE, December 2011.

[7] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12), vol. 1, pp. 647–651, Hangzhou, China, March 2012.

[8] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: theory and implementation," in Proceedings of the ACM Workshop on Cloud Computing Security (CCSW '09), pp. 43–53, November 2009.

[9] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms,"Foundations of Secure Computation, vol. 4, no. 11, pp. 169–180, 1978.

[10] M. A. AlZain, B. Soh, and E. Pardede, "Mcdb: using multi-clouds to ensure security in cloud computing," in Proceedings of the IEEE 9th International Conference on Dependable, Autonomic and Secure Computing (DASC '11), pp. 784–791, 2011.

[11] C. P. Ram and G. Sreenivaasan, "Security as a service (sass): securing user data by coprocessor and distributing the data," in Proceedings of the 2nd International Conference on Trendz in Information Sciences and Computing, (TISC '10), pp. 152–155, IEEE, December 2010.

[12] S. Kardaş, S. Çelik, M. A. Bingöl, and A. Levi, "A new security and privacy framework for RFID in cloud computing," in Proceedings of the 5th IEEE International Conference on Cloud Computing Technology and Science (CloudCom '13), Bristol, UK, 2013.

[13] C. Delettre, K. Boudaoud, and M. Riveill, "Cloud computing, security and data concealment," in Proceedings of the 16th IEEE Symposium on Computers and Communications (ISCC '11), pp. 424–431, Kerkyra, Greece, July 2011.

[14] E. Stefanov, M. van Dijk, E. Shi et al., "Path oram: an extremely simple oblivious ram protocol," in Proceedings of the ACM SIGSAC Conference on Computer & Communications Security, pp. 299– 310, ACM, 2013.

[15] Z. Shen, L. Li, F. Yan, and X. Wu, "Cloud computing system based on trusted computing platform," in Proceedings of the International Conference on Intelligent Computation Technology and Automation (ICICTA '10), vol. 1, pp. 942–945, IEEE, May 2010.

[16] R. Yeluri, E. Castro-Leon, R. R. Harmon, and J. Greene, "Building trust and compliance in the cloud for services," in Proceedings of the Annual SRII Global Conference (SRII '12), pp. 379–390, San Jose, Calif, USA, July 2012.

[17] A. Squicciarini, S. Sundareswaran, and D. Lin, "Preventing information leakage from indexing in the cloud," in Proceedings of the 3rd IEEE International Conference on

[18] K. Hwang and D. Li, "Trusted cloud computing with secure resources and data coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14–22, 2010.

[19] Alex Pucher, Stratos Dimopoulos, A Survey on Cloud Provider Security Measures.

[20] Products & Services, Amazon Web Services. At: https://aws.amazon.com/products/

[21] JR Raphael, InfoWorld, July 1, 2013. The worst cloud outages of 2013. JR Raphael (July 1, 2013) The worst cloud outages of 2013- slide4. InfoWorld.

[22] Top Threats Working Group (Feb, 2013). The Notorious Nine, Cloud Computing Top Threats in 2013. Cloud Security Alliance.

[23] Carl Bagh (May16, 2014). Sony PlayStation Network attack shows Amazon EC2 a hackers' paradise. Ibtimes.com

[24] By Pavel Alpeyev, Joseph Galante and Mariko Yasu (May 15, 2011). Amazon.com Server Said to Have Been Used in Sony Attack, Bloomberg.com.

[25] Google Cloud Platform, At: https://cloud.google.com/

[26] JR Raphael (July 1, 2013) The worst cloud outages of 2013-slide12. InfoWorld.

[27] Twitter breach revives security issues with cloud computing, Cloud Center News Article, Clear Center Corp

[28] Microsoft Azure. At: http://azure.microsoft.com/enus/services/

[29] Charles Babcock (May 14, 2014). Social Science Site Using Azure Loses Data. Informationweek.com

[30] JR Raphael (July 1, 2013), The worst cloud outages of 2013-Slide 8, InfoWorld.

[31] Smart Cloud, Infrastructure and platform services. IBM Inc.

[32] Smart Cloud, Cloud Applications (SaaS, PaaS). IBM Inc.

[33] Rackspace. At: http://www.rackspace.com/

[34] Ben Greiner (December 23, 2013), Rackspace Email Security Breach. Source: forgetcomputers.zendesk.com

[35] Information Age (21 May 2012), Exposing the cracks in cloud security, Information-age.com.