International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 05, 2020
ISSN: 1475-7192

A Meta-analysis on the Security Control Measures in Cloud Migration

S.P. Sreeja and Dr.B. Meenakshi Sundaram

Abstract--- *The data need to be shared on cloud platform with high security and maintained in the cloud in a secured manner for any customer storing the information. There are various cloud providers who provides separate datacenter and are present in different location. This enables to act as a backup for the customer and it should be secured. This paper discusses about the cloud computing security measures.*

Keywords--- *Security, Public Cloud, Insurance, Network, Users, Encryption, Descryption*.

I. INTRODUCTION

Now the PCs on our desks, are having complete control over the computer system used by various customers or users. They are also enabled with complete responsibility for them as well. Cloud computing changes all that. It comes in two basic flavors, public and private, which are the cloud equivalents of the Internet and Intranets. Web-based email and free services like the ones Google provides are the most familiar examples of public clouds. The world's biggest online retailer, Amazon, became the world's largest provider of public cloud computing in early 2006.

To rent the computing power and infrastructure facilities from the distributed cloud, Amazon Web Services (AWS) is the technology adopted. There are private, public and hybrid clouds available, the private cloud works in personalized resources with required secured connections. Amazon provides VPN and VPC as a virtual private networks and clouds for providing highly secured private network for any crucial business application migrations onto cloud environments. There are many advantages while shifting on to cloud, but there are some cons also. Among that privacy and security risks of putting valuable data on someone else‟s system in an unknown location is a major problem.

The public cloud data and applications are accessed by every stakeholders of the business solutions. More open is more vulnerable. The insider attack is a kind of risk, which is higher in the public cloud scenarios. Research analyst on cloud security and alliance report says, public cloud environments are having one of the biggest threats due to its wide openness. Thereby the service providers must conduct many levels of check while accessing the data from massive data centers. The data centers are under surveillance for any kind of suspicious activities.

The scalable cloud infrastructure helps to perform the cost cutting, efficient utilization of resources and process efficiency, since the data is stored within a single server. All sensitive information of various customers is encapsulated within the single server. This ensures the data isolation and logical segregation of storage data.

S.P. Sreeja, Sr. Asst. Professor, Department of MCA, New Horizon College of Engineering, Bangalore. E-mail: sreeja.anil71@gmail.com
Dr.B. Meenakshi Sundaram, Assoc. Professor, Department of MCA, New Horizon College of Engineering, Bangalore. E-mail: bmsundaram@gmail.com

DOI: 10.37200/IJPR/V24I5/PR2020693
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020

II. SECURITY CONTROL PARADIGM

A. Disincentive Controls

This control enables to reduce the threats on a cloud system which act as threatening sign for the intruders trying to cross a defence area or highly secured proximities. It generates an alert similar while crossing the limits. The alerts are kind of message dialogues or an alarm. This is quite similar to burglar alarm techniques in bank security systems.

B. Preventive Controls

It is a superset of the disincentive controls, i.e. it tries to protect from various accessibilities. It supports the system by strengthening as well as by reducing the incidents from malicious attacks even though the vulnerabilities are not eradicated completely. The access rights given to the users provide strong authentication, in such a way that intruders are identified and secured. The log information is stored for any references.

C. Detective Controls

This is a form of control which helps to detect malicious attacks and ensure the appropriate actions. Depends on the type of attacks, the issue is addressed by passing an indication to the preventive or corrective control. This avoidance procedure is detected in the cloud system and its backbone infrastructure with the help of the network security and detection systems.

D. Corrective Controls

The consequences of an attack are reduced with the help of corrective control. Their existence will be action either during the occurrence of intrusion or immediately after the occurrence. These controls are the immediate solutions to recover from such attacks. For an example, building a compromised system to restore or taking the periodical backups or maintaining the mirrored copies on data centers.

III. ANALYSIS ON CLOUD SECURITY

A. Data Encryption Standard (DES)

The Federal Register in the year 1977 published Data Encryption Standard (DES) [2]. It is a symmetric key block cipher. DES is used for encryption as well as decryption. It takes 64-bit plain text in the encyption and a cipher text of size 64 bits is created at the decryption. The key is genearated with the help of plain and cipher text for both encryption and decryption. Sixteen Feistel rounds along with initial and final permutations text for encryption is generated[10]. According to an algorithm shown in Figure below, each of the Feistel rounds generates a cipher key in each round of 48-bit each.

Feistel Rounds are performed by receiving two 32-bit blocks as L0 and R0 from the initial permutation of DES which has a 64- bit block of data. Each of the rounds are identical and the effects of increasing their number is twofold - the algorithms security is increased and its temporal efficiency decreased.

DOI: 10.37200/IJPR/V24I5/PR2020693
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020

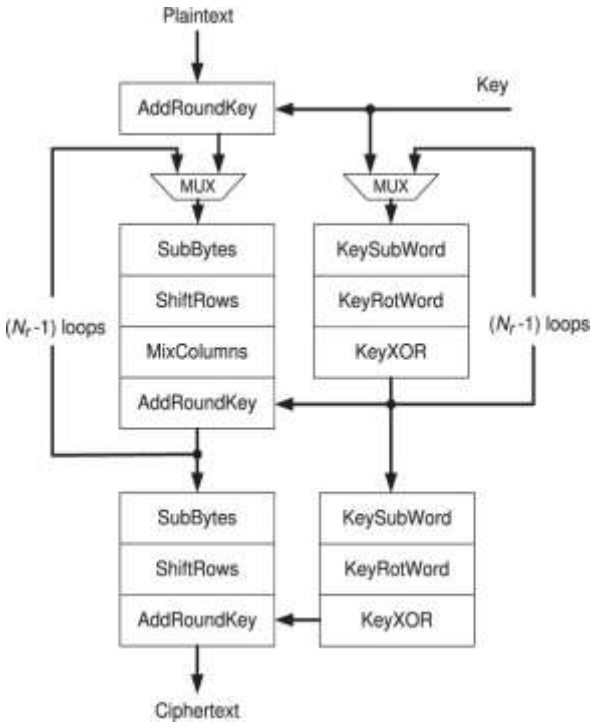

Figure 1: DES Model

B. RSA Algorithm

A public-key algorithm, RSA is used to encrypt the data which is accessed by the concerned user to provide security that prohibits from unauthorized user access. RSA stands for three author names first letter of last name, namely Ron Rivest, Adi Shamir and Len Adleman. Data stored in cloud is first encrypted, when data is needed, a request is sent to the cloud provider and the cloud provider delivers the data after authenticating the user permissions. Every message sent by the user is mapped to an integer by the block cipher, RSA. RSA mainly consist of two keys, i.e., public-key and private-key. In the cloud environment the two keys basically the private key is secured and known only by the user who owns the original data, whereas, the public key is transparent. Encryption and decryption are respectively dealt by the Cloud service provider and Cloud user or consumer. When the data is encrypted using a public- key and the same can be decrypted using the private key. RSA algorithm involves Key Generation, Encryption, Decryption.

C. Homomorphic Encryption

Homomorphic encryption uses asymmetric key algorithm in which two different keys are used for encryption and decryption i.e. public key and private key [10]. In mathematics homomorphic means conversion of one data set to another, without losing its relation between them. In homomorphic complex mathematics functions are applied to encrypt the data and similar but reverse operation is applied to decrypt the data.

D. Blowfish Algorthim

Blowfish Algorithm is a symmetric key algorithm which was developed in 1993 by Bruce Schneier. Its working is almost like DES but in DES key size is small and can be decrypted easily but in Blowfish algorithm the size of key

DOI: 10.37200/IJPR/V24I5/PR2020693
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020

is large [4] and it can vary from 32 to 448 bits. Blowfish also consists of 16 rounds like DES [11]. Blowfish algorithm can encrypt data having size multiple of eight and if the size of the message is not multiple of eight than bits are padded. In Blowfish algorithm also 64 bits of plain text is divided into two parts of size 32 bits. One part taken as the left part of message and other is right part of message. The left part is XOR with the elements of P-array which creates some value, then that value is passed through transformation function F. The value originated from the transformation function is again XOR with the other half of the message i.e. with right bits, then (F) function is called which replace the left half of the message and (P) replace the right-side message.

IV. Conclusion and Future Work

Cloud platform is an evolving technology for shared infrastructure, software, platform as a service. The cloud migration has become an inevitable step for every business applications. The amount of protection required is totally depends on the security mechanism employed in the data centers. The cryptographic computing practices play a vital role in security control measures in cloud platforms. The future work will be the comparison of security mechanism employed in various cloud IoT platforms. With the help of existing algorithms, we can secure our data only up to certain extent.

References

[1] Parsi Kalpana, Sudha Singaraju "Data Security in Cloud Computing using RSA Algorithm", *IJRCCT*, ISSN 2278-5841, Vol 1, Issue 4, September 2012.

[2] Neha Jain, Gurpreet Kaur, „Implementing DES Algorithm in Cloud for Data Security", *VSRD International Journal of CS and IT*, 2012.

[3] Akhil Behl "Emerging Security Challenges in Cloud Computing", *IEEE* 2011.

[4] Simarjeet Kaur "Cryptography and Encryption in Cloud Computing", *VSRD International Journal of CS and IT*, 2012.

[5] V. Sandhya, "A Study on Various Security Methods in Cloud Computing", *International Journal of Advanced Research in Computer Science,* Volume 2, No.6, Nov-Dec 2011.

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

[7] Birendra Goswani, Dr.S.N. Singh, "Enhancing Security in Cloud computing using Public Key Cryptography with Matrices", *International Journal of Engineering Research and Applications*, Vol 2, Issue 4, 339-344, July-Aug 2012.

[8] G. Jai Arul Jose, C.Sanjeev, Dr. C. Suyambulingom, "Implementation of Data Security in Cloud Computing", *International Journal of P2P Network Trends and Technology*, Vol 1, Issue 1, 2011.

[9] William Stallings, "Network Security Essentials Applications and Standards", *Third Edition, Pearson Education*, 2007.

[10] Hassan Takabi and James B.D. Joshi. Policy Management as a Service: An Approach to Manage Policy Heterogeneity in cloud Computing Environment. 2012 45th *Hawaii International Conference on System Sciences.* 2012 IEEE.

[11] Researcher Demonstrates Simple BitLocker Bypass. *By SecurityWeek News on November* 18, 2015. from http://www.securityweek.com/researcherdemonstra tes-simple-bitlockerbypass. consulted MAR 10,2016.

[12] Timothy Zhu, Alexey Tumanov, Michael A. Kozuch. Priority Meister: *Tail Latency QoS for Shared Networked Storage. ACM* 2014.

[13] Jens Myrup Pedersen, M. Tahir Riaz, BozydarDubalski, Damian Ledzinski, Joaquim Celestino Jnior and Ahmed Patel. Using latency as a QoS indicator for global cloud computing services. *John Wiley& Son* 2013.

[14] Iain Thomson. Microsoft researchers smash homomorphic encryption speed barrier. From http://www.theregister.co.uk/2016/02/09/researcher s break homomorphic encryption. *The Register* (Feb 9, 2016) consulted JUN 1, 2016.

DOI: 10.37200/IJPR/V24I5/PR2020693
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020

[15] Nathan Dowlin, Ran Gilad-Bachrach, Kim Laine, Kristin Lauter, Michael Naehrig, and John Wernsing. CryptoNets: Applying Neural Networks to Encrypted Data with High Throughput and Accuracy. Microsoft Research (February 24, 2016).
[16] MahaTebba, Saïd Haji Abdellatif Ghazi, "Homomorphic Encryption Applied to the Cloud Computing Security", World Congress on Engineering 2012
[17] Sandro Rafaeli, "Survey of key management for secure communication", ACM Computing Surveys, 2013.

DOI: 10.37200/IJPR/V24I5/PR2020693
Received: 16 Apr 2020 | Revised: 22 Apr 2020 | Accepted: 12 May 2020