Journal of Artificial Intelligence and Capsule Networks (2019)
Vol.01/ No. 01
Pages: 45-53
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2019.1.006

AN EFFICIENT SECURITY FRAMEWORK FOR DATA MIGRATION IN A CLOUD COMPUTING ENVIRONMENT

Dr. Subarna Shakya,
Professor, Department of Electronics and Computer Engineering,
Central Campus, Institute of Engineering, Pulchowk, Tribhuvan University,
Pulchowk, Lalitpur Nepal - 44600.
Email: drss@ioe.edu.np.

Abstract: Cloud computing is advantageous in several applications. Data migration is constantly carried out to hybrid or public cloud. Certain large enterprises will not move their business-critical data and applications to the cloud. This is due to the concerns regarding data security and privacy protection. In this paper, we provide a data security analysis and solution for privacy protection framework during data migration. A Secure Socket Layer (SSL) is established and migration tickets with minimum privilege is introduced. Further, data encryption is done using Prediction Based Encryption (PBE). This system will be of use for healthcare systems and e-commerce systems that can store data regarding credit card details. We provide a strict separation between sensitive and non-sensitive data and provide encryption for the sensitive data.

Keywords: Cloud Computing, data security, encryption, data migration, virtual machines

1. INTRODUCTION

Cloud acts as a virtual interface for data access in a virtual environment. For smooth functioning of cloud migration, the presentability and knowlegability of the cloud provider are to be taken care of. Problems regarding data and cloud security of the company's data assets will arise if data migration is not done systematically [1]. Cloud providers with thorough experience may face issues like unauthorised access by third party or data crash while transferring data to the cloud. This causes reputation as well as monetary losses.

In cloud computing environment, data migration is an exercise in risk management [2]. Quantitative as well as qualitative factors are to be considered during analysis. Careful balancing of risk must be done against the available security and predicted benefits. Security accountability should remain within the organization. Adding excessive controls may make the system unproductive and incompetent. Hence, it is necessary to make sure that the benefits does not outweigh the risks involved. The strength of control and the relative risks involved in a program should be appropriately balanced. Data security is a significant factor in cloud computing [3]. Service providers are dependent on infrastructure providers to access the physical security system for complete data security. In case of virtual private cloud, security settings can be remotely specified by the service provider without the knowledge of implementation status.

ISSN: 2582-2012 (online)

Journal of Artificial Intelligence and Capsule Networks (2019)
Vol.01/ No. 01
Pages: 45-53
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2019.1.006

Confidentiality and auditability are two major infrastructural objectives that has to be monitored during data transfer. Confidentiality involves secure transfer and access of data and is achieved by cryptographic protocols. Auditability is to attest that the security settings of the application has not been tampered. It can be done with remote attestation procedures. For remote attestation, a trusted platform module (TPM) [4] is required to generate a system summary that acts as a proof of the system security. Virtual Machines (VM) can vigorously transfer from one location to another in virtual environments like cloud. Hence building a trust mechanism at each architectural layer of the cloud is also essential.

2. CLOUD COMPUTING SECURITY ISSUES

2.1 Data breaches and data loss: Data is said to be breached if any unauthorised person gets access to view the data. Data breaches in cloud computing [5] can occur in the form of malware injection, hijacking and other means. Data loss may occur due to malicious attacks, data wipe by service provider or natural disaster. Amazon suffered permanent loss of its client data. Similarly, Google lost its client data when its power grid was hit by lightning on multiple occasions.

2.2 Insider threat and cloud services abuse: Sensitive information including financial data, customer accounts and so on can be misused by people who have authorised access to the cloud services of an organization. Secure strategies, access control and implementation technologies can be used to control this type of security attack. Hackers as well as authorised users can host malware [6], digital properties and illegal software as vast storage capacity is available.

2.3 Insecure Application Programming Interfaces (APIs): API allows user to customize their cloud experience by interaction, management and data extraction. It gives the ability to customise cloud service features as per business requirements as well as authenticate, offer access and influence encryption. APIs [7] are used for interaction of mobile apps with website and back end services. API permits the programmer to build programs and integrate applications with other essential software.

2.4 Denial of Service Attacks: DoS attacks [8] block the legitimate users from gaining access to website and server by flooding the network with traffic. It can also be used as a camouflage to perform malicious activities and affect firewalls and other security applications. It may also cause the server to crash. Using load balancers or rerouting malicious traffic can moderate DoS. Intrusion detection system (IDS) can prevent and fight back DoS attacks.

2.5 Shared vulnerability: Security is a shared responsibility among the cloud service provider and the client. Omitting any of the responsibility may lead to compromise of data security. Cloud also offers multi-tenanted

ISSN: 2582-2012 (online)

Journal of Artificial Intelligence and Capsule Networks (2019)
Vol.01/ No. 01
Pages: 45-53
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2019.1.006

features by means of virtual machines (VM) [9]. Proper testing before installation ensures proper implementation of VM.

3. CURRENT DATA SECURITY SOLUTIONS

Virendra et al. [10] proposed a system for secure cloud migration process by understanding the distributed file system over cloud such as Google File System (GFS) based on Hadoop Distributed File System (HDFS) by allowing data replication and Prediction Based Encryption (PBE) that allows asymmetric encryption of selective fine-grained access control in cryptographic operation. Decryption keys are created and encryption is done using attributes of the data. David G. Rosado et al. [11], provide an analysis of various approaches that provide security during cloud migration process and insist on the importance of security during migration in legacy systems.

Bjorn Johnson et al. [12] proposed a cloud migration decision making model covering several major genres of cloud computing risk. Antonis et al. [13] presents a novel cloud infrastructure facilitating confidentiality of data and mechanism for protecting integrity.

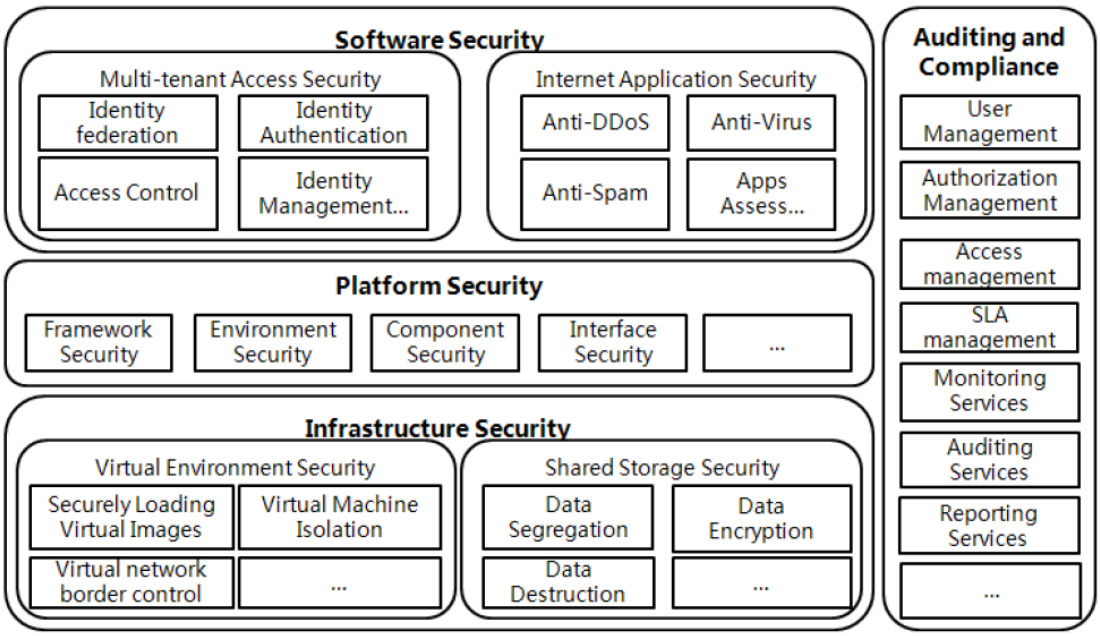

Figure 1. Cloud Security Architecture [14]

Prasad et al. [15] proposed a cloud computing based scheduling algorithm that is energy efficient and works on the basis of prediction model. It offers better efficiency compared to minimum migration time, round

ISSN: 2582-2012 (online)

Journal of Artificial Intelligence and Capsule Networks (2019)
Vol.01/ No. 01
Pages: 45-53
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2019.1.006

robin and first fit algorithms. The paper presented an iterative fractal model based prediction system with advanced heuristic algorithm.

4. PROPOSED METHOD

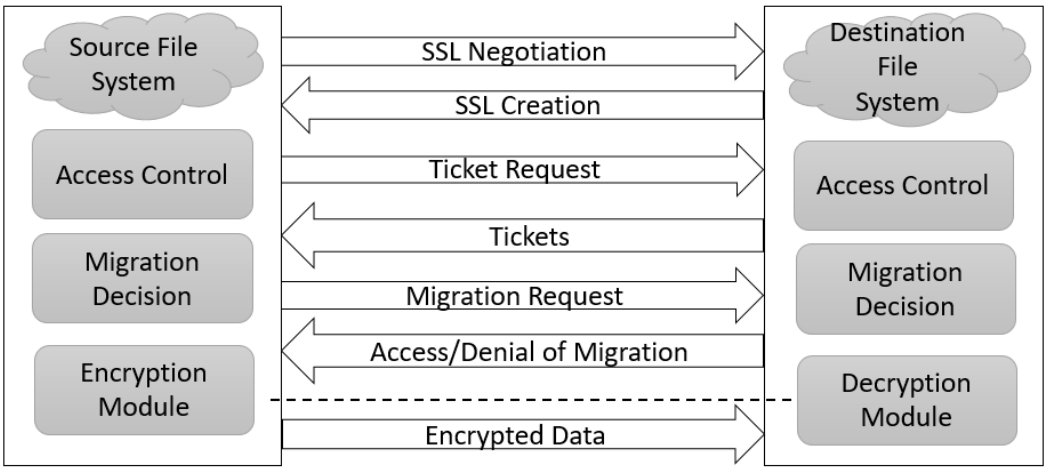

Figure 2 Secure Cloud Migration Framework

A. Pre-migration Security

Before conducting the migration process, it is essential to perform a thorough examination on the access rights and user accounts. This ensures that there is no insecure access protocol or outdated credentials. The entire system security can be made vulnerable with a single stray user account. Hence this step is the essential and foremost in secure data migration.

B. Security Socket Layer (SSL) establishment

Before beginning the migration process, the SSL protocol is used by the source and destination nodes and a secure channel is established. This security channel acts as a foundation for migration related security parameters. Data encryption key, random key, message authentication code and so on are temporarily used in this security channel. The temporary tickets that can authenticate data node in source and destination nodes can also be secured at this level. The data migration may happen between two different cloud servers or from premise to cloud server. Establishing secure connectivity for migration between the cloud clusters is essential and has a commercial significance. During initial communication between the two nodes in SSL, the major

ISSN: 2582-2012 (online)

Journal of Artificial Intelligence and Capsule Networks (2019)
Vol.01/ No. 01
Pages: 45-53
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2019.1.006

security parameters to be considered include authentication of messages in code computing by initiation of a temporary session key, symmetric encryption with random key and migration tickets with minimum privilege.

C. Migration ticket with minimum privilege

In order to verify the identity of a subject and appropriate permissions, tickets are used. In the source cluster from which the transmission is initiated, the data nodes holds the tickets. The destination node accepts the ticket when the SSL connection is established. Intrusion at this level is possible where attackers may interlope the ticket and obtain the permissions that are directed to the destination cloud and may retransmit the ticket causing damage of data. The software security improvisation can help reduce the impact of stolen tickets, but cannot completely restrict the occurrence of such delinquency. Hence one plausible solution to such events is the minimization of permission given by one ticket that enables normal migration without any hitches. If the trespasser acquires the tickets, the operations that can be performed with it would be very restricted. In this paper, we present a prototype that provides minimal cluster migration privilege ticket. Such tickets encompasses the identification of data node and the output file and has a single usage feature. It also sets an expiry data for every ticket. Hence, on existence of duplicate tickets, existence of intruders can be identified. The migration administrator gets notified on such situations.

The main purpose of the ticket is to authenticate the data transmission at source node and to reduce the use of unauthorised tickets by reducing the permission granted to the tickets. In case of multiple migrations happening simultaneously, it is easy to identify as the ticket carries the identity of the data node. This enables single usage of the ticket. Once the ticket is used, it will be destroyed automatically.

D. Data Encryption using PBE

File systems used in premise or cloud includes Hadoop, MySQL, Oracle and File Transfer Protocol (FTP)/ Network Attached Storage (NAS). The most commonly used cryptographic methods for migration of data includes Attribute Based Encryption (ABE), Identity Based Encryption (IBE) and Prediction Based Encryption (PBE). We use PBE as it offers better performance when compared to the other two schemes. An entity's identity is obtained from a set of characteristics. It can be decrypted with the required access policies.

We setup the encryption by generating a random key and encrypting the data with it in the source file system. The random key is encrypted with a shared key and data transfer is performed. At the destination cloud, decryption of random key is done with the help of the shared key and the data is decrypted with the help of random key.

ISSN: 2582-2012 (online)

Journal of Artificial Intelligence and Capsule Networks (2019)
Vol.01/ No. 01
Pages: 45-53
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2019.1.006

5. RESULT

A. Evaluation of security performance

The SSL protocol is well known for its security features and is often used in point to point networks and business environment where safety of the data is a major factor. Data can be migrated from data centre to public cloud, from one cloud to another or from cloud back to data centre. Assigning temporary tickets with limited active period and limited privileges restricts the intruder activities in the cloud. If a ticket is received twice in the system, it indicates possible attack. Minimizing the privileges restricts the intruder from reading the stolen data. Hence the data integrity is kept intact.

B. Evaluation of time cost

Evaluation of time cost can be done at three stages namely during SSL establishment, verification of ticket, PBE based encryption and decryption of data. The security framework time cost depends on establishment of SSL, Generating and transmitting encryption key, migration ticket and decryption of the keys. Encryption and decryption of data blocks with PBE using random key and shared key.

Table 1 Time cost for data migration

File Size	SSL Establishment	Migration ticket verification	PBE based encryption and decryption	Total time
64 Mb	880ms	2ms	43600ms	44.4 s
128 Mb	895ms	2ms	93700ms	1.576 min
256 Mb	900ms	2ms	187800ms	3.145 min
512 Mb	905ms	3ms	290000ms	4.848 min

Table 1 provides the individual time cost and total time taken for the complete encryption, transfer and decryption process along with the time for establishment of the SSL channel. For this purpose, we transmit sample data of different sizes from 64Mb to 512Mb. There is a progressive increase in the time taken at every level.

C. Evaluation of vulnerability to attack

Multiple levels of data security has been ensured in this system. The SSL protocol provides optimal performance and data transfer security as it enables the transfer of encryption key, random key and message

ISSN: 2582-2012 (online)

Journal of Artificial Intelligence and Capsule Networks (2019)
Vol.01/ No. 01
Pages: 45-53
http://irojournals.com/aicn/
DOI: https://doi.org/10.36548/jaicn.2019.1.006

authentication code by the establishment of security channel between the source and the destination. Further, the migration ticket with least privileges allow optimal transfer of data. Since the ticket is of single use, it is easy to identify intruders on multiple occurrences of the ticket. Lastly, PBE based encryption is also enhanced with the use of random key and shared key and thereby doubling the protection level of the data. The data can be split into blocks and stored. The individual data blocks can be encrypted separately for transmission.

6. CONCLUSION AND FUTURE WORK

Cloud migration involves moving data, applications or other business essentials into a cloud computing environment. There are three types of cloud migrations namely from data centre to public cloud, from one cloud to another, from cloud back to data centre. This paper presents an optimal solution for secure data transfer in cloud computing environment with three steps. The first step involves establishing a secure socket layer between the sender and receiver nodes. Secondly, the data migration ticket is initiated with minimum privilege. The data on the sender node is encrypted using Prediction Based Encryption with random key and shared key.

With the increase in the levels of encryption, the time taken for the encryption, transfer and decryption of data increases. Future work involves reduction of time cost required for encryption and transfer of data. Also, the data blocks can be split into smaller units to improve the speed and security during transfer. This framework can be adopted by all cloud storage systems.

References

[1] Ogunde, Nicholas A., and Jörn Mehnen. "Factors affecting cloud technology adoption: potential user's perspective." In Cloud Manufacturing, pp. 77-98. Springer, London, 2013.

[2] Piao, Jing Tai, and Jun Yan. "A network-aware virtual machine placement and migration approach in cloud computing." In *2010 Ninth International Conference on Grid and Cloud Computing*, pp. 87-92. IEEE, 2010.

[3] Kaufman, Lori M. "Data security in the world of cloud computing." IEEE Security & Privacy 7, no. 4 (2009): 61-64.

[4] Perez, Ronald, Reiner Sailer, and Leendert van Doorn. "vTPM: virtualizing the trusted platform module." In Proc. 15th Conf. on USENIX Security Symposium, pp. 305-320. 2006.

ISSN: 2582-2012 (online)

[5] Subashini, Subashini, and Veeraruna Kavitha. "A survey on security issues in service delivery models of cloud computing." Journal of network and computer applications 34, no. 1 (2011): 1-11.

[6] Watson, Michael R., Angelos K. Marnerides, Andreas Mauthe, and David Hutchison. "Malware detection in cloud computing infrastructures." IEEE Transactions on Dependable and Secure Computing 13, no. 2 (2015): 192-205.

[7] Karnwal, Tarun, T. Sivakumar, and G. Aghila. "A comber approach to protect cloud computing against XML DDoS and HTTP DDoS attack." In 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science, pp. 1-5. IEEE, 2012.

[8] Choo, Kim-Kwang Raymond. "Cloud computing: challenges and future directions." Trends and Issues in Crime and Criminal justice 400 (2010): 1.

[9] Kazim, Muhammad, and Shao Ying Zhu. "A survey on top security threats in cloud computing." (2015).

[10] Kushwah, Virendra Singh, and Aradhana Saxena. "A security approach for data migration in cloud computing." *International Journal of Scientific and Research Publications* 3, no. 5 (2013): 1-9.

[11] Rosado, David G., Rafael Gómez, Daniel Mellado, and Eduardo Fernández-Medina. "Security analysis in the migration to cloud environments." *Future Internet* 4, no. 2 (2012): 469-487.

[12] Johnson, Bjorn, and Yanzhen Qu. "A holistic model for making cloud migration decision: A consideration of security, architecture and business economics." In *2012 IEEE 10th International Symposium on Parallel and Distributed Processing with Applications*, pp. 435-441. IEEE, 2012.

[13] Michalas, Antonis, Nicolae Paladi, and Christian Gehrmann. "Security aspects of e-health systems migration to the cloud." In *2014 IEEE 16th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 212-218. IEEE, 2014.

[14] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." In *2012 International Conference on Computer Science and Electronics Engineering*, vol. 1, pp. 647-651. IEEE, 2012.

ISSN: 2582-2012 (online)

[15] Babu, G. Prasad, and A. K. Tiwari. "Energy Efficient Scheduling Algorithm for Cloud Computing Systems Based on Prediction Model." International Journal of Advanced Networking and Applications 10, no. 5 (2019): 4013-4018.

[16] Beloglazov, Anton, and Rajkumar Buyya. "Energy efficient allocation of virtual machines in cloud data centers." In *2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing*, pp. 577-578. IEEE, 2010.

[17] Chen, Deyan, and Hong Zhao. "Data security and privacy protection issues in cloud computing." In *2012 International Conference on Computer Science and Electronics Engineering*, vol. 1, pp. 647-651. IEEE, 2012.

[18] Xiao, Zhifeng, and Yang Xiao. "Security and privacy in cloud computing." *IEEE communications surveys & tutorials* 15, no. 2 (2012): 843-859.

ISSN: 2582-2012 (online)