Volume 8, No. 2, March 2017 (Special Issue)
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW ARTICLE
Available Online at www.ijarcs.info

Security Enhancement in Cloud Networks By Neoteric Techniques

Tayibia Bazaz
Department of CSE, SEST
Jamia Hamdard, New Delhi, India
ttb.bbz@gmail.com

Abstract: Cloud computing paradigm is a platform that helps the geographically distributed users to access outsourced data without much hardware and software requirements.With the tremendous growth and popularity of cloud, its security aspect is getting more priority and importance than ever before. Unfortunately, a lot of malicious activities have been identified with the growth of cloud users. This paper provides a comprehensive review and analysis of security enhancement in cloud networks using some security algorithms.

Keywords: cloud security; security algorithms; metaheuristic algorithm; threats; Quality of service (QOS); Application Delivery Network.

I. INTRODUCTION

Cloud computing has become a slogan in distributed computing due to its distinctively marked feature of providing on-demand access to resources from a shared pool ubiquitously. The access is provided via Internet following a "pay as you go" trend [1]. Cloud computing, now used as a synonym for Internet, has paved a better path to increase capacity as well as capability without much infrastructure investment or software licensing. Thus, it has verily made its landmark in the field of technology [2]. The cloud users are increasing substantially due to the growing popularity of cloud networks. This has imposed various challenges for the cloud service providers as they need to adequately satisfy the thirst of their users. They not only need to provide their users a secure access to resources, but also have to maintain a proper Quality of service (QOS) balance. QOS is a requirement of clients to connect smoothly with the servers of these service providers and is sometimes mentioned in Service Level Agreements (SLA).

Thus, there is an alarming need of optimization of QOS parameters like throughput, response time, end to end delay, etc as well as security enhancement. Security concern becomes more pressing issue for customers when they have to store confidential data on cloud. Thus, users cannot compromise on security of their data anyway [3]. Besides data security, other types of security problems in cloud are like Network security, Data locality, Data integrity etc. Based on the nature of the cloud used, the cloud provider's responsibilities could include operating system and network security, infrastructure security, physical security of premises, etc [4]. There are various techniques available to implement and prolong security in cloud environment like AES, Hash-key algorithm, DES, RSA, etc.

Figure 1 shows a simple cloud computing environment where different corporate users, clients, employees are accessing cloud services. In the scenario, different data centers are used and placed at different locations. These data centers consist of a collection of networked computers and storage devices. Various organizations and companies use these data centers to store, process, organize etc their immense data. Also, besides storage, data centers offer other functionalities like power backups, communication connections, etc. On the side of data center, there is an Application Delivery Network (ADN), a suite of topologies which when deployed together, provides visibility, availability, security, etc. Application Delivery Controller (ADC) also called as web switch, is used for advance traffic management and distributes the load to various servers and hence, performs load balancing.

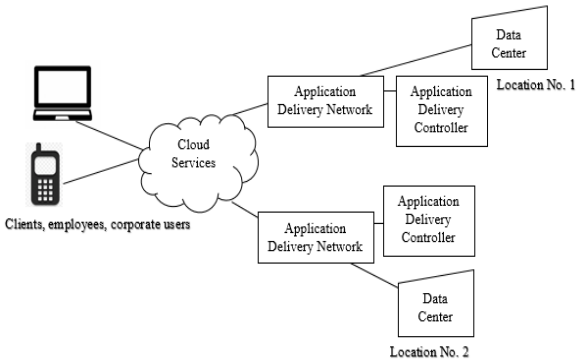

Figure 1: Cloud Computing Environment

Followed in this paper, a literature survey is given in Section II followed bysecurity threatsof cloud in Section III. A brief description of security algorithms is given in Section IV. Later sections include conclusions followed by references.

LITERATURE SURVEY

While switching to cloud environment, many hurdles are being faced by organizations and enterprises in which security is one of the highlighting aspect. Some of the related work done in the enhancement of cloud storage security is discussed below:

Deyan Chen et al[6] have provided a brief analysis on privacy and security issues related to cloud

environment. Also, here some current security enhancement solutions are being discussed and some new and improved techniques are proposed in their future scope. **Ashutosh Kumar Dubey et al [7]** proposed a new cloud computing environment where control is in hands of both the client as well as the cloud environment admin. They have divided the approach in two parts. In the first part, user takes permission from the cloud environment to perform operations and to load their data. While in the second part, admin has to take permission from the cloud environment to read and update data. Thereby, creating trusted secure cloud computing scenario. **Bohar Singh et al [8]** have put some effort to deal with privacy and security issues by proposing an approach including use of RSA and image sequencing password. Also, the proposed approach is integrated with authentication. The overall approach enhances security of cloud. **Saurabh Singh et al [9]** worked on the security concerns of some public and private cloud authorities. Also, the requirements for better security management are also included in the paper. They also discussed about 3-tier security architecture with some discussions on new security concepts.

SECURITY THREATS

In a distributed and multi- tenant environment, the most complex challenge nowadays is cyber warfare. During the data transfer in a client-server architecture, the requirement of security should be most important. This section discusses about some of the threats in security of cloud environment.

- ***Failure in Security of Service Provider [7]:*** The security of the service provider of cloud is paramount as it controls all the hardware and the hypervisors on which data is stored and applications run. Hence, cloud provider security must top-of-the-line.
- ***Cloud environment is shared among its users [7]:*** One user might try to access other user's data or try to interfere with his/her applications if the barrier separating the users is interrupted.
- ***Storage Security:*** In cloud environment, users store their data on cloud and afterwards have no knowledge or learning of their data. The storage security always has been an important aspect of Quality of Service (QOS). It uses homomorphic token with distributed verification of erasure-coded data in order to ensure the correctness of user's data in the cloud. Cryptography, data leakage, data sanitization, cryptography, data-Remanence, data leakage, snooping of data availability, malware, etc. are the major concerns of storage security [10,9].
- ***Network Security:*** Communication in Cloud computing is possible via Internet which is a backbone for cloud computing environment. Hence, the security of network is essential. Network security includes both internal and external attacks that can occur either in a physical or virtual network [11,9].
- ***Infrastructure Security:*** The demonstration of whether the physical and virtual infrastructures of cloud can be trusted or not is one of the most common and vital challenges. For critical business processes, the verification of the third party is just not adequate. It is absolutely essential to ensure that the underlying infrastructure is secure for any business process or transaction [9].
- ***Software Security:*** It is concerned about bugs, buffer overflow, designed flaws, error handling promises etc [9].
- ***Issues of Reliability and Availability [7]:*** As cloud computing's usability depends on Internet, thus, the reliability and availability of Internet is cardinal.
- ***Integrating Provider and Customer Security Systems [7]:*** Cloud providers should integrate with systems of security architecture like automated provisioning, incident detection and response, etc. to maintain grip with customers otherwise the manual provisioning process and uncoordinated response will again come into play.

SECURITY ALGORITHMS

Many enterprises whether big or small store their important data on cloud. Thus, their data must be safe and secure and well protected from hackers and intruders. For the security of the cloud data, many algorithms are designed. Some of them are symmetric while some asymmetric. Few of them are defined below:

A. Symmetric Algorithms

Symmetric algorithms use a secret key for encryption of large amount of data. The secret key is reveled to only two entities viz., sender and receiver. These have a great processing speed. Examples include DES, AES, Blowfish, etc. Some of them are:

- ***Data Encryption Standard (DES):*** DES was developed by IBM in 1974 and is a common symmetric key algorithm. In DES, block size of plain text and cipher text is of 64 bits while key size is 56 bitsas shown in Figure 2. The initial key size is 64 bits but the 8 bits are padded resulting in a key size of 54 bits only. The encryption of the block of plain text is done by a combination of confusion and diffusion to make a cipher block. The cipher block is then made to pass through 16 rounds, but before this process, the block data is divided into two equal halves of 32 bits. A function called F-function (Fiestal function) is applied which consists of substitution, permutation, key mixing. Using XOR gate alternate crossing of data, the output of the function is combined with the other half of 32 bit followed by a crossing of data.

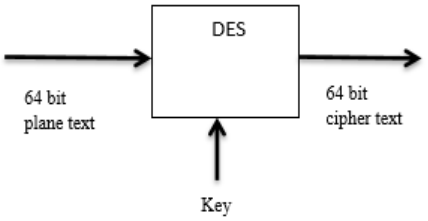

Figure 2 [12]: Basic DES

Repeating the same process for all the 16 rounds followed by inverse initial permutation, a cipher text of 64 bit is produces. The decryption of cipher text can be done easily by data reversing operation. The

SEMINAR PAPER
National Seminar on Cloud Computing and its Applications (March 9-10, 2017)
Organized by
Dept of Comp. Sci. & Eng, SEST, Jamia Hamdard, New Delhi (India)

key size of DES being small causes its security to be breached easily and it works slowly on software and faster on hardware [12].

- ***Advance Encryption Standard (AES) [12]:*** It is also known as Rijndael. In AES, the key size varies and may be used as 128, 192 or 256 bits. The key size selection depends upon the cycles it will use e.g., for 10 cycles 128-bit key is used and so on. The rounds in AES are all of same nature excluding the last one. AES consists of key expansion, initial round and final round and works on 4*4 matrices. Both initial and final round consist Add Round Key, Sub Bytes, Shift Rows with an addition of Mix Column in former oneas shown in Figure 3. Unlike DES, it works fast both on hardware and software.

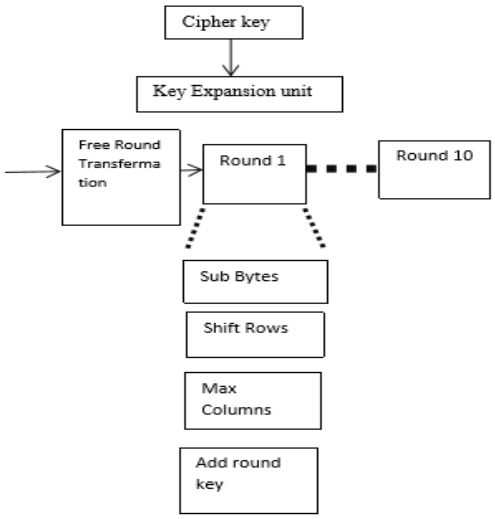

Figure 3 [12]: AES Algorithm

B. Asymmetric Algorithm

In asymmetric algorithms, a pair of keys called public key and a private key is used for encryption and decryption process. The former key is known to everyone while the later one is kept secure by its owner. It includes Diffie-Hellman, RSA, etc [13].

- **Diffie-Hellman:** Diffie-Hellman is a cryptographic algorithm where first a shared secret key is established for the intercommunication of parties followed by exchange of cryptographic keys for encryption/decryption. Here, by the process of exchanging keys between the two communicating parties, it is ensured that the two don't have any prior knowledge of each other to jointly establish a shared secret over insecure internet. After the completion of interchange of keys, both the parties end up with the similar session key that looks like a secret key. Both of the parties then calculate a third session key that is not easy for an attacker to calculate irrespective of knowing the exchanged values. This key along with a symmetric key cipher then is used for subsequent encryptions but is vulnerable to Man-in-the-Middle-Attack [13].

Besides the symmetric and asymmetric security algorithms, also some metaheuristic algorithms can be used for cloud security optimization and QOS enhancement. The term Metaheuristic was coined by Glover in 1986 and the term is a fusion of two Greek words viz. "meta meaning beyond in the sense of light" and "heuriskein which means to search". These algorithms are platform independent and do not come with a proof of finding a particular solution within finite amount of time.Some of the metaheuristic algorithms are Genetic Algorithm, Particle Swarm Optimization, Ant Colony Optimization, etc. Metaheuristic algorithms can be used for various optimization problems and help to find a solution that is "good enough" in computing time and small enough [14]. The above defined algorithms are few and list of security algorithms is not exhausting. Thereby, cloud security can be enhanced using these defined security algorithms.

CONCLUSION

Cloud computing is an assured progression in the future of information technology. Nowadays, many big or small companies are switching to cloud in order to store and organize their data. Thus, security of cloud networks is the need of the hour. After performingan intensive literature survey, it can be concluded that cloud network suffers from various security breaches. These security breaches can be encountered anytime and hence, need to be addressed properly and efficiently. Various security algorithms are proposed to combat these security issues. A hybrid of these security algorithms can be used to optimize security in cloud. Also, existing algorithms can be integrated with appropriate metaheuristic algorithm, to form a neoteric approach that will further leverage the level of security and optimize QOS parameters in cloud networks and the results can be simulated on an appropriate simulator.

ACKNOWLEDGMENT

I would like to express sincere thanks to my Supervisor Prof. Moin Uddin and co-supervisor Dr. Sherin Zafar for their valuable guidance in this paper.

REFERENCES

[1] M. Kalra, S. Singh "A Review of Metaheuristic Techniques in Cloud Computing". *Egyptian Informatics Journal*, 2015.

[2] M. S. Rana, K. S. Kumar, N. Jaisankar, "Comparison of Probabilistic Optimization Algorithms for Resource Scheduling in Cloud Computing Environment". *International Journal of Information and Technology*, Vol. 5, No. 2, 2013.

[3] S. Gupta S., D. S. N. Panda, D. B. Bhushan, "Hash Key Based Effective Algorithm for Security in Cloud Infrastructure". *International Journal of Computer Science and Technology*, Vol. 6, No. 3, 2015.

[4] G. L. Prakash, D. M. Prateek, D. I. Singh, "Data Security Algorithms for Cloud Storage System using Cryptographic Method". *International Journal of Scientific & Engineering Research*, Vol. 5, No. 3, 2014.

[5] Available: www.jebas.us/cloud-computing-network-diagram.html

[6] D. Chen, H. Zhao, "Data Security and Privacy Protection Issues in Cloud Computing". *International Conference on Computer Science and Electronics Engineering*, 2012.

[7] A. Dubey, A. Dubey, M. Namdev, S. S. Shrivastava, "Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment". *CSI Sixth International Conference on Software Engineering (CONSEG)*, 2012.

[8] B. Singh, Poonam, A. Rani, "To enhance the Reliability and Security in Cloud environment using RSA algorithm and Image Sequencing Password". *International Journal of Advanced Research in Computer and Communication Engineering* Vol. 4, No. 6, 2015.

[9] S. Singh, Y. S. Jeong, J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions". *Journal of Network and Computer Applications*, 2016.

[10] T. Nguyen, W. Shen, Z. Luo, Z. Lei and W. Xu, *Novel data integrity verification schemes in cloud storage*, 1st ed. Computer and Information Science, Springer International Publishing, 2015.

[11] Wu, Hanqian, Ding, Yi, Winer, Chuck, Yao, Li, "Network security for virtual machine in cloud computing" in Proceedings of the 2010 5th International Conference on IEEE Conference in Computer Sciences and Convergence Information Technology (ICCIT), 2010.

[12] E. A. Pansotra, E. S. P. Singh, "Cloud Security Algorithms". *International Journal of Security and Its Applications*, Vol.9, No.10, 2015.

[13] A. Bhardwaj, G. Subrahmanyam, V. Avasthi, H. Sastry, "Security Algorithms for Cloud Computing". *International Conference on Computational Modeling and Security*, 2016.

[14] B. Chitra, M. Srikrishna and A. Naveenkumar, "A Survey on Optimizing the QOS during Service Level Agreement in Cloud", *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, No. 3, 2013.

[15] T. Bazaz, A. Khalique, "A Review On Single Sign On Enabling Technologies and Protocols". *International Journal Of Computer Applications*, Vol. 151, No. 11, 2016.

[16] H. Fayaz, A. Khalique, " A Review On Sociological Impacts Of Social Networking". Internation Journal of Engineering Applied Sciences and Technology, Vol. 1, 2016.

[17] B. Bashir, A. Khalique, " A Review On Security Versus Ethics". International Journal of Computer Applications, Vol. 151, No. 11, 2016.