International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 240-244
Published Online August 2020 in IJEAST (http://www.ijeast.com)

CLOUD COMPUTING ADOPTION FRAMEWORK FOR DATA SECURITY IN CLOUD SHARE

Ms. S. P. Gitte,
Department of CSIT, M.B.E.S. COE,
Ambajogai, Maharashtra, India.

Mrs. V. R. Chirchi
Department of CSIT, M.B.E.S. COE,
Ambajogai, Maharashtra, India.

***Abstract*— It's a major issue to deal with large capacity of data centers in the sense of security. As by nature their sizes keep growing by the cloud users and service providers also. And it's becoming a research interest nowadays to look into this large and unstructured data set. We have proposed a security system based upon a Cloud Computing Adoption Framework (CCAF) which is well structured and systematic to tackle most of the online threats. This paper exhibits working of CCAF framework, its components, multi-layered security and proposed approach. in the CCAF to protect data security.**

Keywords— **CCAF, Cloud Computing, Data center security, multi-layered**

I. INTRODUCTION

Data became a fuel in today's growing digital world as each and every service is driven by an Internet and also continuously deriving and generating a vast amount of data. As most of the things are available online it became a serious issue to preserve data privacy for a user while keeping his interest in mind. To preserve real-time security for digital services it is mandatory to provide some security framework. In general most data is stored in clouds with a secure topology and backup services and also it has been a hot topic with software as a service (SaaS) feature which provides key features as per user interests since the last few decades. Many efforts are being taken to reduce the cost of services, to improve the quality of services and also to enhance work efficiency by many researchers. As multiple cloud nodes are not cost efficient to increase the performance, this paper is a true effort to reduce the cost of service and provide trustworthy services [1-2].

According to ITU, in the upcoming decade the total data traffic on the Internet will be equal to the total global air traffic. Most organizations and firms rely on sharing data to complete their work by using shared cloud instances and in some scenarios the gaming people play games online, these all incidences may create a security threat for themselves unknowingly. In such cases service providers are creating their own security shields for their private networks, but it's not possible for all to follow this trend while providing services. In cloud computing the data is stored in data centers and it is of increasing nature with a capacity of more than 100 terabytes. A very common example is YouTube video services by Google in which daily more 300 hrs of video data is uploaded to the Google data centers. In such cases the issues related to performance like data traffic, data leakage, data security, deliverables, bandwidth arises due to the sudden increase in data [3-4].

In [8] authors have developed an algorithm to generate dynamic keys using multiple techniques in cloud share. The developed system uses coding, permutations and reorder bits with artificial intelligence by search methods which use polynomial equations to expand the original key. The system implicitly manages key generation, key-exchange, key verification, etc.

There are many new attacks and threats have been identified on cloud computing to compromise the user data in recent days. The attacks may include account or service hijacking, data scavenging, data leakage [9], DoS [10], customer data manipulation [11], VM hopping[12], etc. These attacks and threats are only possible due to improper security measures, weak API's, and insecure networks.

In this paper we have developed a well-structured framework to be followed preserving users data privacy. The framework followed is also called as Cloud Computing Adoption Framework (CCAF) and can be customized. CCAF is designed as a multi-layered security approach with desired requirements. This framework not only ensures security from internal threats while collecting terabytes of data per day but also from external threats like viruses, malwares, etc. To achieve required performance on a large set of databases as of above 10 petabytes we have used Business Process Modeling Notation (BPMN). Performance is shown in the form of simulations. The BPMN gives rights to select required security concerns according to the user's point of view [5].

The remaining paper is organized as follows. Security model adopted for cloud computing with its review is given in section II, section III describes layers and purpose of the multilayered approach in security, sections IV discusses the proposed system with screenshot. section V concludes the paper with observations and result set.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 240-244
Published Online August 2020 in IJEAST (http://www.ijeast.com)

II. SECURITY MODEL ADOPTED FOR CLOUD COMPUTING

There are a number of threats registered till date and becoming the serious threat for the expansion of cloud computing technology in the industries. To tackle these issues we have to build an algorithm which can easily predict the unusual behavior of the user and also the future occurrences of attacks. The one most adopted and referenced model is Cloud Computing Adoption Framework which applies systematic and conceptual principles of security over a cloud. In our proposed work we are integrating the CCAF model for cloud security in the form of multilayer structure by which each layer will handle a specific threat like viruses, Trojans, malwares, intrusion attacks, etc.

CCAF is already enhanced in organizations like healthcare [6], finance [7], business clouds [8], and other types of fields also. Computer security is derived in general concepts and processes such as identification, which identifies objects, functions, and actions, authentication, authorization, privacy, integrity and durability [3]. Basic security features with identification, authentication, authorization, digital security encryption and decryption techniques are well developed in the market and industries and it can be enhanced in our system by considering technical aspects.

It has been observed that 99.95% viruses and Trojans can be detected and blocked, and also achieve >85% of blocking for 100 h of continuous attack in the penetration testing of CCAF. In a multi-layered approach each layer preserves its own security model and follows to complete the threat security. So in our proposed system we have adopted a multi-layered approach.

III. MULTI-LAYERED APPROACH

A multilayer approach adopted in CCAF shown in figure 1 maximizes the performance of the model ensuring infections reductions. Each layer is responsible for its own security task and performs accordingly its measurements and required necessary action is taken in case of threat detected.

The model includes encryption, access control techniques, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). To reach the cloud share network the users need to go through three defensive layers as follows:

- The first layer of security consists of **Access Control** and **firewall** to allow restricted members only. The layer works for protection against intruders. In this layer the data is sent over the network by encrypting it. The intrusion prevention is performed by encryption using user signature. This is done by key generation and then IPS configuration is saved [3].
- The second layer of model includes IDS and IPS which detects attacks, intrusion and penetration. It also takes care of latest technologies to serve security like DoS, anti-spoofing, port scanning, known vulnerabilities, SQL injection and cookie poisoning, etc. This layer focuses on identity management of the user. The user roles in these layers are users, CCAF server and the security manager. Users encrypt data by using key and split files into blocks and last request for cloud storage. CCAF server manages authentication during storage, access control and then encrypt/decrypt. The decryption is performed at the receiver side by verifying signature by server. Security managers store metadata like block signatures, encrypted keys, etc.
- The third layer of model focuses on policy based management, integrity management. This layer ensures the in advance prediction of abnormal behavior of the system. Convergent encryption (CoE) performs a security test using a hash of plaintext. This layer avoids deduplication of data by placing one data block at once in storage. [3]

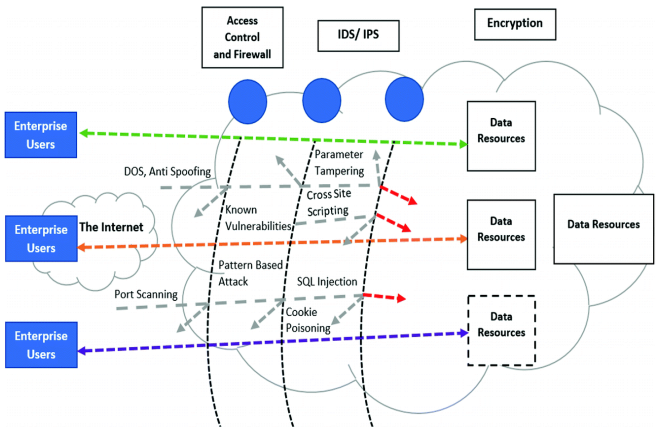

Fig. 1. CCAF multi-layered security model

The safety against Trojans and viruses is also provided in this system as sometimes the data gets affected or damaged by these attacks. In such cases it is a priority to save other data from the attack. To perform this step the CCAF security model backups the system first and then tries to quarantine the affected file. If it does not succeed then it isolates that file from the other data or keeps those files in what is called quarantine area or simply deletes those files accordingly the users interest.

IV. PROPOSED SYSTEM

In our proposed system we are strictly following the CCAF multi-layered approach. User needs to store the data in a cloud store so he will create a secure account on a cloud. So at the time of transmitting the data on a cloud the system follows the RSA public-key cryptography. so according to the algorithm the user first generates the private key and also obtains the public key of the receiver to encrypt the data as shown in the fig. 2.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 240-244
Published Online August 2020 in IJEAST (http://www.ijeast.com)

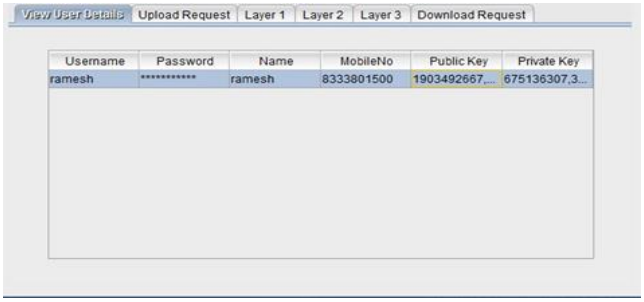

Fig. 2 Public key and private key for encryption

Now the file is converted in some unreadable numeric form by applying the encryption. Then at the time of uploading the file is further segmented into the more secure blocks as shown in fig. 3.

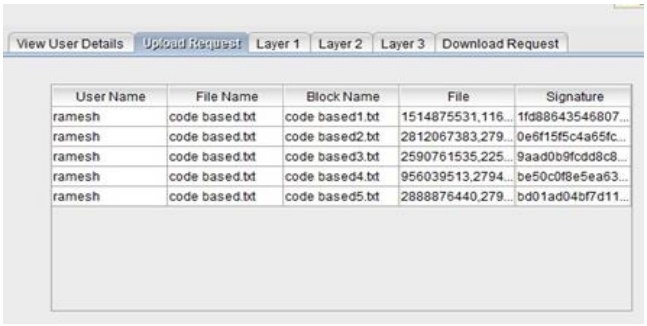

Fig. 3 File Segmentation into the blocks

As discussed in the above section III the layer 1 will be responsible for the access control over the network level like firewall, private network securities, etc. In the second layer we are taking care of the outside attacks like hackers, intruders, vulnerabilities, spoofing, etc., by introducing an intrusion detection system as shown in fig. 4

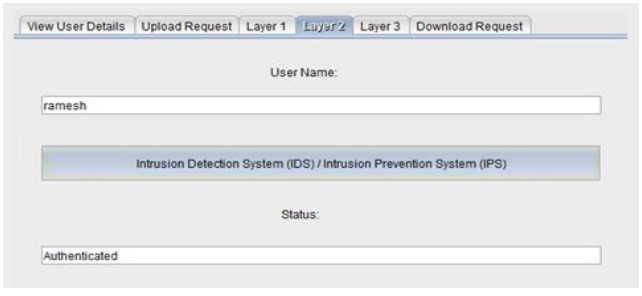

Fig. 4 Intrusion Detection System

.
This layer keeps track of the successful and unsuccessful attempts towards the system and automatically predicts the behaviour of the unknown user. Most of the threats are prevented in this layer only.

Atlast in layer 3 a security test is performed to make sure of the security of the data using the Convergent Encryption. This encryption also ensures the file deduplication and integrity of the data in the cloud share. The users of the system allocated the cloud space for their storage by providing an cloud account, virtual machines and sometimes with hardwares as per their business requirements. The users in the system are the potential cloud customers, cloud administrators, cloud providers, service providers, etc.

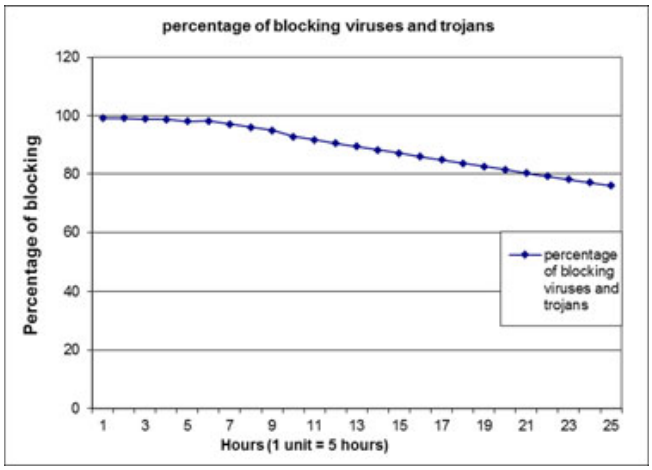

Fig. 5 Blocked Percentage (viruses and trojans)

To demonstrate the threat scenario we have created fake users in the system and tried to access the cloud data using random keys and also by using viruses. Also the system must withstand the increasing nature of cloud size with numerous possibilities of attacks. We have tried to penetrate in the system by creating the real time set up using virtual machines with CCAF multi-layered security turning on. Fig. 5 describes the percentage of viruses and trojans are blocked [3]. This penetration testing with its outcomes shows that multi-layered security gives better results in filtering of malicious attacks. To perform this penetration test we have recorded the following observations:

- The number of viruses and trojans detected and blocked by each layer.
- The total numbers of viruses and trojans detected and blocked the system.
- The number of viruses and trojans detected but unable to be blocked and sent to quarantine.
- In the quarantine, the number of viruses and trojans that can be destroyed.
- In the quarantine, the number of viruses and trojans that cannot be destroyed. [3]

Two types of penetration tests are performed in the experiment as continuous virus and trojan attack on the system and the second one by using fake accounts and trying to hack the system by using the different permutations and combinations of keys and passwords. As the RSA makes the system more secure to crack into. the results are shown in the percentage format rather than in numbers.

According to the research and our results in experiments from the proposed system it is observed that the time to take control of security breach can take between 60 and 150 hours. So we will require additional security to be assured with our data safety during this period. The proposed system follows the CCAF multi-layered security approach to protect data in real-time and by its three layers of security: 1) firewall and access control; 2) identity management and intrusion prevention and 3) convergent encryption.

The results show that even if the system blocks the viruses and trojans the blockage percentage can be degraded by continuous attacks of viruses and trojans. Around 90 percent of them can be quarantined and isolated by the system.
The authors in [13-16] presented an theoretical-based approach and addressed similar approaches with their rationale
and theories in place without performing large scale experiments to check the robustness of their models. We compared CCAF multi-layered security with a single-layered approach by performing experiments.

V. CONCLUSION

We have proposed and experimented multi-layered security for the Cloud share's data security by following CCAF principles according to different industry demands and requirements. The proposed system gives a wide security protection against multiple threats like viruses, Trojans, intruders, etc. using a layered approach for petabytes of memory in cloud share. We have simulated all the aspects of data like its uses, either data at rest, in use, or in motion using Business Process Modeling Notation which is one of the well known practices in the sense of security and results discussed in the thesis are achieved in 5 seconds. These results can be viewed and observed by increase in the amount of data in real practice and can be stated as it will take up to 30 hours to protect all the 1 PB data and up to 125 hours to notify in case of a threat detected and resolve ULCC Data Center. The potential threats and attacks are predicted by analyzing the behavior of data and the user sessions while using the cloud in the real systems. So we can conclude that we can increase the performance by selecting an appropriate algorithm for the security system in the sense of execution time, blocking viruses/Trojans in real-time.

VI. REFERENCE

[1] Y. Yu, (2015) "The Cost-Efficient Awareness for Cloud MapReduce," 2015 3rd International Conference on Future Internet of Things and Cloud, Rome, pp. 573-578.

[2] D. Kapil, P. Tyagi, S. Kumar and V. P. Tamta, (2017) "Cloud Computing: Overview and Research Issues," 2017 International Conference on Green Informatics (ICGI), Fuzhou, pp. 71-76.

[3] V. Chang and M. Ramachandran, "Towards Achieving Data Security with the Cloud Computing Adoption Framework," in IEEE Transactions on Services Computing, vol. 9, no. 1, pp. 138-151, 1 Jan.-Feb. 2016.

[4] Q. Zhang, L. Cheng, and R. Boutaba, (2010) "Cloud computing: state-ofthe-art and research challenges," J. Internet Services Appl., vol. 1, no. 1, pp. 7–18.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia,(2010) "Above the clouds: A Berkeley view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58.

[6] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A Berkeley view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

[7] L. Liu, E. Yu, and J. Mylopoulos, "Security and privacy requirements analysis within a social setting," in Proc. 11th IEEE Int. Requirements Eng. Conf., Sep. 2003, pp. 151–161.

[8] Chang, Victor & Kuo, Yen-Hung & Ramachandran, Muthu. (2015). Cloud Computing Adoption Framework–a security framework for business clouds. Future Generation Computer Systems.

[9] Cloud Security Alliance, *Top Threats to Cloud Computing V1.0*., 2010.

[10] Dawoud W, Takouna I, Meinel C, *Infrastructure as a service security: Challenges and solutions*. The 7th International Conference onInformatics and Systems (INFOS), Potsdam, Germany. IEEE Computer Society, Washington, DC, USA, 2010, pp 1–8.

[11] Grobauer B, Walloschek T, Stocker E, *Understanding Cloud Computing vulnerabilities*, IEEE Security Privacy, 2011, 9(2):50–57.

[12] Winkler V, *Securing the Cloud: Cloud computer Security techniques and tactics*, Elsevier Inc, Waltham, MA, 2011.

[13] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE INFOCOM, Mar. 14–19, 2010, pp. 1–9.

[14] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc. 17th ACM Conf. Comput. Commun. Security, Oct. 2010, pp. 735–737.

[15] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of

encrypted data," in Proc. 13th ACM Conf. Comput. Commun. Security, Oct., 2006, pp. 89–98.

[16] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Gener. Comput. Syst., vol. 28, no. 3, pp. 583–592, 2012.