Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 7, July 2017, pg.232 – 236

Improvement in Homomorphic Encryption to Increase Cloud Security

Jasmeet Kaur, Usvir Kaur

Department of Computer Science and Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib, India
Department of Computer Science and Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib, India
panagjas195@gmail.com, usvirkaur@gmail.com

Abstract*— Cloud computing provide different services to user. But there is some issues in cloud computing, the main one is security because every user store their useful data on the network so they want their data should be protected from any unauthorized access, any changes that is not done on user's behalf. To solve the problem of Key management, Key Sharing various schemes have been proposed. The paper will work on designing new modal for key sharing and key management in fully Homomorphic Encryption scheme. In this we use the symmetric key agreement algorithm named Diffie Hellman and HMAC for the data integrity OTP(One Time Password) which provides more security. Due to this the problem of managing the key is removed and data is more secured.

***Keywords*— Cloud, Security, Encryption, Key, OTP, Homomorphic**

I. INTRODUCTION

Cloud computing is an environment which provides on demand and convenient access of the network to a computing resources like storage, servers, applications, networks and the other services which can be released minimum efficiency way. Cloud services are mainly available in the three types of cloud. In public cloud, resources allocated are publically. Applications in this cloud are on pay-per-use basis. In private cloud, resources are limited and used within an organization. It is more secure as employees in an organization can access the particular data only. In Hybrid Cloud, there is a combination of both public and private cloud [1]. The services within the organization are control by the customer and resources which need to be delivered externally are controlled by the service provider. Network security, information security and many other security types like the computer security together make the term "Cloud Security". Because it consist all of the security mechanism given above. It provides the broad set of technologies, policies and controls that are used to secure the data and applications that exists with the cloud computing environment. It is not the product of computer security like anti-viruses and anti-spam's. Security is the most concerning point to any service. External security or internal security required to each field. Only security ensures the privacy and integrity the cloud data [2]. There are many security loopholes exist in the service. There are many types of security issues exist like DDOS, Man in the middle etc. the various types of attacks within the cloud computing environment are briefly described below:

a. Denail of Service Attack (DoS): Denial of service (DOS) is very common attack. It may totally interrupt or slow down the system [3]. As cloud is used by many customers this may lead to possibility of DoS attack. In this attack attacker sends the number of zombie processes to the server that may be wrong query which may lead to eat up of resources or crash the server.

b. Cloud Malware Injection Attack: A challenger attempts to insert malicious code into a system in malware-injection attack. This attack can become visible in the form of scripts, code, active content, and other software.

c. Side channel Attack: An attacker can place the malicious virtual machine just near to actual virtual machine and pretend to be the real virtual machine and can get IDs of legitimate users [4].

d. Man-In-The-Middle Cryptographic Attacks: The man-in-the-middle attack are sometime caleed bucket brigade attack(often abbreviated MITM). This is done by any attacker when he place himself between two parties when they are communicate with each other.

Fully Homomorphic encryption: Fully Homomorphic encryption provides the better security than full disk encryption. Unlike FDE the encryption is not applied on full disk, encryption is applied on each function [5]. The cipher text and plain text is not related but the emphasis is on the algebraic operation that works on both of them. After the invention of RSA, Rivest, Adleman and Dertouzos introduce the idea of fully Homomorphic schemes. Then they asked for an encryption function that allows the encrypted data without any preliminary decryption of the operand to be operated on, and they called privacy homomorphisms. More accurately, Fully Homomorphic Encryption has the many properties.

Full Disk Encryption: The whole physical disk is encrypting with physical key for the better speed and simplicity in disk firmware in the case of fully disk encryption. In case of stolen laptop it is very effective technique to protect the etc. Therefore it cannot fulfill the requirement of data protection goals in the cloud but physical theft is not the main threat [6]. Full Disk Encryption is one of the most successful ways protect our private data on laptops, tapes etc. FDE solution comprises a number of methods for receiving admittance to the drive when a consumer can no longer authenticate. This may be a recovery key, a recovery password or an emergency log-on account. Once common with the practice, make sure that the recovery information is centrally backed up, test your recovery strategies.

Diffie Hellman key exchange: Diffie Hellman was the first public key algorithm or we can say that it is symmetric key agreement ever invented, in 1976. Diffie Hellman key agreement protocol allows exchanging a secret key between two parties [7]. It also provides exponential key agreement and also does not require any prior secrets.

II. LITERATURE REVIEW

Dian-Yuan Han, (2012) introduced in this paper [8], service interactions security module. To protect the cloud there are three layers considered: the first layer is traditional transport layer, second layer is cloud computing layer and requirements and third layer is application-driven layer. Failures are normally occurred when there is high availability; high fault tolerance and high efficiency accesses to Internet based cloud data centers. These types of issues are significant and need to be handled carefully. These issues are more important and valuable then high performance. Agents are introduced to data security module in order to provide more efficient and useful services.

Dr Nashaat el-Khameesy, (2012) suggested in this paper [9] a methodical application of "defense in depth" security technique that can help all security risks in networked storage. Most important is that the defense in the depth based networked storage security policy provides a framework towards the future attacks and the current technologies are clearly understood. The standards growing in the storage security with defense in the depth will help in making the storage much more resilient to the future threats.

Shui Han, (2011) proposed in this paper [10], trustful third party in which the user can operate and store their data securely in cloud. There is a problem of data storage security in cloud computing. For more security of the cloud new scheme is introduced i.e. novel third party auditor. The third party auditor provides techniques like RSA and Bilinear Diffie-Hellman. By using RSA algorithm encrypted data is flow from sender to the receiver and by using Bilinear Diffie-Hellman keys are exchanged for security purposes. With the exchanging of keys, data is always sent to the valid and authorized users only.

Sean Carlin, (2011) proposed in this paper [11], that cloud computing is the distributed architecture that centralizes the resources of server on a scalable platform which provides services on demand. The main security issues and risks are discussed; sharing of resources is one of them. Customers are not satisfied with the data security on cloud. Cloud service providers must tell the customers about the deployment models. They need to use the third party auditor so that they can gain the trust of customers. For this, new techniques need to be developed and older should be removed for easy work in cloud architecture.

Deyan Chen, (2012) described in this paper [12], that data security and privacy protection issues occurred in cloud computing in all the stages of data life cycle. The paper has discussed some current solutions like fully homomorphic technique, data integrity, client-based privacy management tool, etc. No doubt cloud has many advantages but still there are many issues like security need to be solved. According to the survey of Gartner for cloud computing, Public and Hybrid cloud has a revenue of $59 billion and by the year 2014 it will reach USD 149B with a annual growth of 20.The increase in the revenue of cloud with the time shows that cloud is a trustworthy industry. But still there are some issues in cloud regarding security of data which increases the threats from hackers.

Young-Gi Min, (2012) introduced in this paper [13], three cloud computing models are i.e. SaaS, PaaS, IaaS. Security requirements of cloud computing and the solutions for the security problems are described. Different security attacks are defined which need to be overcome by applying security algorithms and another techniques. To have secured cloud deployment, areas like computing architecture, portability and interoperability, traditional security, business continuity, disaster recovery, data centre operations, Encryption and key management, identity and access management must be considered. The best way to minimize the unauthorized access is using Digital ID's for the employee; this also addresses the issue of non-repudiation.

III. RESEARCH METHODOLOGY

This study is mainly focused on to develop modal for fully homomorphism disk encryption schemes. The new scheme will provide reliable key storage and key management services. This will increase the reliability and security of the existing fully homomorphism encryption scheme. In this new model, secure channel establishment algorithm will used for the key management and key sharing. The secure channel establishment algorithms are Diffie-Hellman and RSA. The Diffie-Hellman algorithm is most secure and reliable algorithm. If the two parties that are Master and Slave wishes to exchange the data in .Diffie-Hellman algorithm. Then before starting the communication, the secure channel is established. Both the parties select random number. Secure channel and shared key is established on the basis of the selected random number.

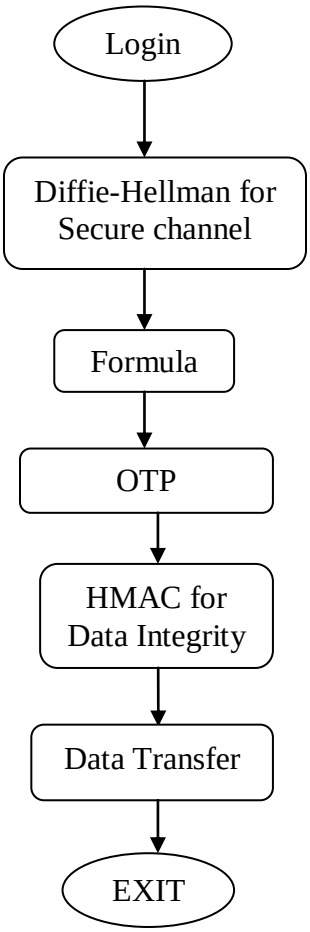

Fig 1: Proposed Flowchart

IV. EXPERIMENTAL RESULTS

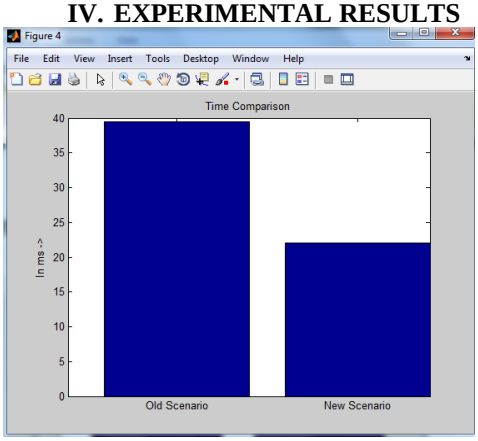

Figure 2: Comparison graph of delay

As shown in figure 2, the comparison between previous and proposed approach is shown in terms of delay. The delay in previous technique is increasing, when numbers of exchange messages are increased. In the proposed approach the delay is less due to increasing the number of message.

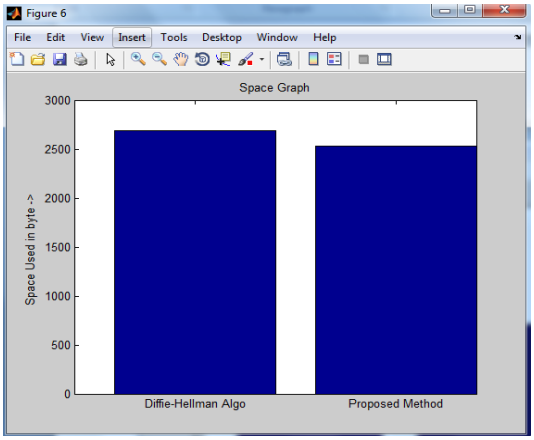

Figure 3: Comparison graph of Space

As shown in figure 3, the comparison between Deffie-Hellman and proposed approach is shown in terms of space utilized. The space utilized in Deffie-Hellman technique is more. However, in the proposed approach there is reduction in the space utilization which shows its effectiveness in comparison to the existing technique.

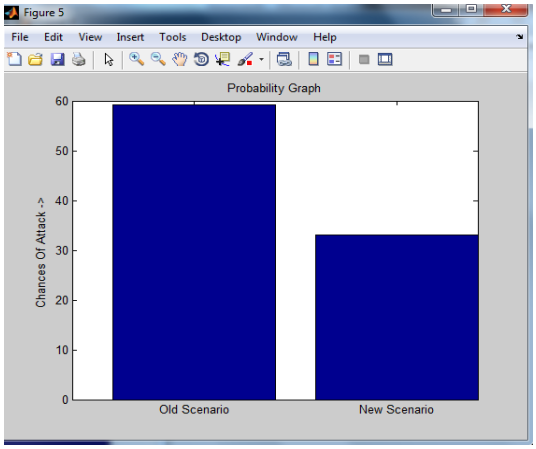

Figure 4: Comparison graph of probability

As shown in figure 4, the comparison between previous and proposed approach is shown in terms of chances to occurrence of an attack. The delay in previous technique is increasing, when numbers of exchange messages are increased. In the proposed approach the delay is less due to increasing the number of message.

V. CONCLUSION

In this thesis, two most popular techniques for cloud data encryption are reviewed. These techniques are full disk encryption and fully homomorphic encryption. In this work, we find that fully homomorphic encryption technique is more efficient than full disk encryption. But the main problem exists in fully homomorphic encryption is of key management and key sharing which reduces the reliability of the scheme. For key management and key sharing, enhancement is been proposed in the encryption scheme and enhancement is based on Diffie-hellman algorithm and HMAC and OTP is generated on the basis of secret key generated from diffie-hellman algorithm. This algorithm create session key between user and cloud. Each time new key is generated between two before communication. This reduces the time takes place in management and sharing of keys and secure channel is established between both i.e. user and the cloud service provider. The simulation shows that proposed enhancement is more efficient and reliable than the existing one. In future we will extend this work for access control management using fully homomorphic encryption scheme.

REFERENCES

[1] John Harauz, Lori M. Kaufman,Bruce Potter, "Data Security in the World of Cloud Computing", IEEE Security and Privacy, pp 61-64, August, 2009

[2] Deepanchakaravarthi Purushothaman[1] and Dr.Sunitha Abburu, "An Approach for Data Storage Security in Cloud Computing", IJCSI International Journal of Computer Science Issues, Vol. 9, No. 2, March, 2012

[3] Vimmi Pandey, "Securing the Cloud Environment Using OTP", International Journal of Scientific Research in Computer Science and Engineering Vol. 1, No. 4, June, 2013

[4] Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore, "Cloud Computing Security" International Journal on Recent and Innovation Trends in Computing and Computation, Vol. 1, No. 1, pp 36-39, January, 2013

[5] Van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V., "Fully homomorphic encryption over the integers", Gilbert, H., ed.: EUROCRYPT. Volume 6110 of Lecture Notes in Computer Science, Springer, June, 2010

[6] Punithasurya K, Esther Daniel, Dr. N. A. Vasanthi, "A Novel Role Based Cross Domain Access Control Scheme for Cloud Storage", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Vol. 2, No. 3, pp 942-946, March, 2013

[7] Simarjeet Kaur, "Cryptography and Encryption In Cloud Computing", VSRD-IJCSIT, Vol. 2 No.3, pp 242-249, 2012

[8] Deyan Chen, Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing", International Conference on Computer Science and Electronics Engineering, Vol. 1, pp 647-651, 2012

[9] Shui Han, Jianchuan Xing, "Ensuring Data Storage Through a Novel Third Party Auditor Scheme in Cloud Computing", IEEE computer science & Technology, pp 264-268, 2011

[10] Sean Carlin, Kevin Curran, "Cloud Computing Security", International Journal of Ambient Computing and Intelligence, Vol. 3 No. 1, pp 14-19, March, 2011

[11] Dr Nashaat el-Khameesy,Hossam Abdel Rahman, "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems", Vol. 3, No. 6, pp 970-974, June, 2012

[12] Dian-Yuan Han, Feng-qing Zhang, "Applying Agents to the Data Security in Cloud Computing", International Conference on Computer Science and Information Processing(CSIP), pp 1126-1128, August, 2012

[13] Young-Gi Min, Hyo-Jin Shin and Young-Hwan Bang, "Cloud Computing Security Issues and Access Control Solutions", Journal of Security Engineering, Vol. 9, No. 2, pp 135-140, 2012

