Novel Approach to Secure Cloud Data

Payal Thakur[1] & Amandeep Kaur[2] & G.N. Verma[3]
[1,2,3]Department of Computer Science & Engineering, Sri Sukhmani Institute of Engineering and Technology, DeraBassi

Received: May 25, 2018 Accepted: July 10, 2018

ABSTRACT *The cloud computing is the architecture in which no central controller is present due to which various breaches occur in the network. To secure data transmission from source to destination two type of encryption schemes. i.e: fully homomorphism and fully disk encryption are introduced. The fully homomorphic encryption scheme is more secure and light as compared to fully disk encryption. In this paper, improvement in the fully homomorphic encryption is proposed using elliptic curve cryptography and OTP generation.*

Keywords: *Homomorphic Encryption, OTP, Elliptic Curve Cryptography.*

Introduction

Cloud Computing is the environment which provides on-demand & convenient access of the network to a computing resources like storage, servers, applications, networks and the other services which can be released in minimum efficiency way. User retrieved data and modified data is stored by client or an organization in centralized data called cloud [1]. Cloud is a design, where cloud service provider provides services to user on demand and it is also known as CSP which stands for "Cloud Service Provider". There are five essential characteristics composed by cloud design. Cloud design also promotes the availability. Network security, information security and many other security types like the computer security together make the term "Cloud Security". Because it consists all of the security mechanism given above, it gives the broad set of technologies, policies and controls that are used to secure the data and applications that exist with the cloud computing environment [2]. It is not the product of computer security like anti-viruses and anti-spam's. Security is the most concerning point to any service. Only security ensures the privacy and integrity of the cloud data. There are many security loopholes exist in the service. There are many types of security issues that exist like DDOS, Man in the middle etc. Fully homomorphic encryption provides better security than full disk encryption. Unlike FDE the encryption is not applied on full disk, encryption is applied on each function [3]. The cipher text and plain text are 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 introduced the idea of fully Homomorphic schemes. They asked for an encryption function that permits encrypted data to be operated on without preliminary decryption of the operands, and they called those schemes privacy homomorphism. The whole physical disk is encrypted with physical key for 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 [4]. Therefore it cannot fulfill the requirement of data protection goals in the cloud but physical theft is not the main threat. Full Disk Encryption is one of the most successful ways protect our private data on laptops, tapes etc. Your data could be permanently lost when an encrypted hard drive goes bad. FDE solution comprises a number of methods for receiving admittance to the drive when a consumer can no longer authenticate [5]. 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 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. It includes exponential key agreement and requires no prior secrets [6]. In the Diffie-Hellman algorithm if two parties, say, Master and Slave wishes to exchange data, both agree on a symmetric key. For encryption or decryption of the messages symmetric key is used. It is known that Diffie Hellman algorithm is used for only key agreement or key exchange, but it is not used for encryption or decryption. Before starting the communication, secure channel is established between both the parties [7]. Both parties select their own random number. On the basis of the selected random numbers, secure channel and shared key is established.

Literature Review

Bhavna Makhija, 2013 proposed different techniques and their merits and demerits like Message Authentication Code (MAC) which protect the data from integrity. A hash tree is used for large files. Third

party auditor is used to relieve the large data into small parts for maintenance and security. The proposed algorithm describes data integrity and dynamic data operations. They use encryption to ensure data integrity. Public key is also defined which is based on homomorphic authenticator. A hash function is used for proof of irretrievability. The proposed algorithm has a main drawback that it requires implementation of the higher resources cost [8].

Vimmi Pandey, 2013 introduced Dynamic mobile token application. This is the application in mobile phones which is used to generate a code with the help of OTP (One Time Password). This OTP code is used only for one time to login session. In this paper, they describe one of the methods of OTP. There are two phases in it Registration phase and Login phase. User first registers itself by filling credentials in the form and then enters to the Login phase. In login phase, OTP will be generated for the login session. OTP is generated by three parameters: The current time, 4-digiti PIN code and Init-secret. This code is valid for three minutes only. This ensures protection against eavesdroppers attack and man-in-middle attack. Hence, they prove OTP is very secure [9].

Sanjoli Singla, 2013 proposed a design and architecture that can help to encrypt and decrypt the file at the user side which provides data security in both cases while user is at rest or is transferring data. In this paper they used the Rijndael Encryption Algorithm along with EAP-CHAP. This algorithm has five steps which need to be followed for the data security. The users are always concerned about the privacy protection and security issues before storing their data on cloud. Even if some intruder (Unauthorized user) gets access of the data then the data will not be decrypted. Encryption must be done by the user to provide better security Algorithm . For this, Rijndael Encryption algorithm is used [10].

Ankur Mishra, 2013 discussed two techniques: Virtualization and Multi-tenancy which provides security about cloud computing. Virtualization is a way of making a physical computer function as if it were two or more computers which are non-physical or virtualized. There are two types of virtualization: Full virtualization and Para virtualization and two architectures of virtualization: Hosted and Hypervisor architecture. Multi-tenancy can be applied to different levels i.e. application level, middleware level, operating system, hardware level. Then security of virtualization and multi-tenancy has been discussed [11].

Punithasurya, 2013 presented that when dealing with public cloud, security should be taken care. Security is very important in cloud computing. Security includes authentication, authorization and access control. In cloud storage, there are many access control schemes available. Control is the main part of cloud computing. Only access control is the one that provides authorization to many users or authorized users. Access control has access privileges that are required by the user. Security is the major concern in cloud computing. For security purpose, Role Based Access Control (RBAC) is used. By the use of this technique time location and availability can be enhanced [12].

Chimere Barron, 2013 discussed different issues related to cloud computing security. To protect cloud computing system and to prevent various attacks many security mechanisms have been developed. To improve the security of cloud computing new technologies has been developed by the researchers. Different types of attacks like SYN flood, malware injection, account hijacking are discussed in this paper. The main focus of this paper is on detecting and preventing SYN flood in cloud computing. The author developed two algorithm one detecting algorithm and one preventing algorithm. They will implement and test these algorithms on cloud computing [13].

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 enhance the reliability and security of the existing fully homomorphism encryption scheme. In this new modal, secure channel establishment algorithm will be used for key management and key sharing. The secure channel establishment algorithms are Elliptic Curve Cryptography and RSA. On the basis of algebraic structures of elliptic curves across finite fields, the Elliptic Curve Cryptography (ECC) is computed. In order to provide security equivalent to non-elliptic curve cryptography techniques, there is a need of smaller keys in ECC. We have embedded the Elliptic Curve Cryptography algorithm for authentication procedure. Here, a plane curve is presented across a finite field that has points present within it that can satisfy the equation which is:

$$y^2 = x^3 + ax + b$$

A distinguished point is also involved here at infinity, which is represented as ∞. The point at infinity is known as the Abelian group which includes within it a set of operation related to the elliptic curves. The divisor group helps in inheriting the structure of the group which also has the algebraic variety within it.

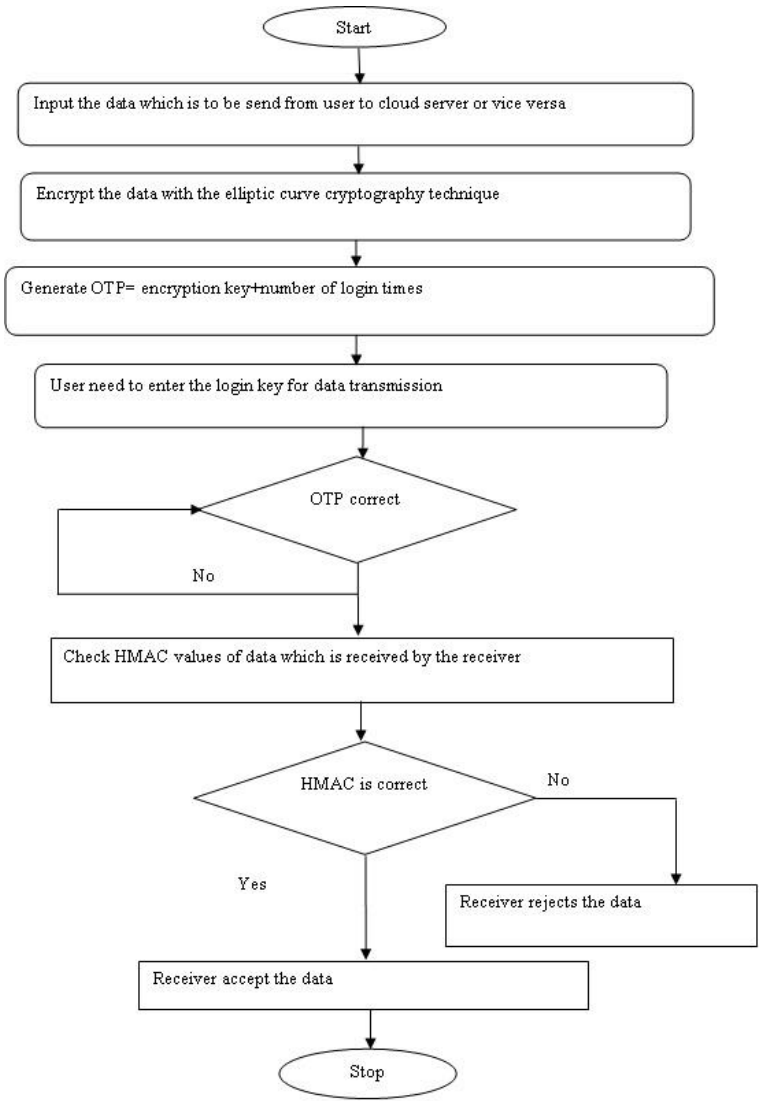

Figure 1: Proposed Flowchart

Experimental Results

The proposed work has been implemented in MATLAB and the results are evaluated in terms of several parameters.

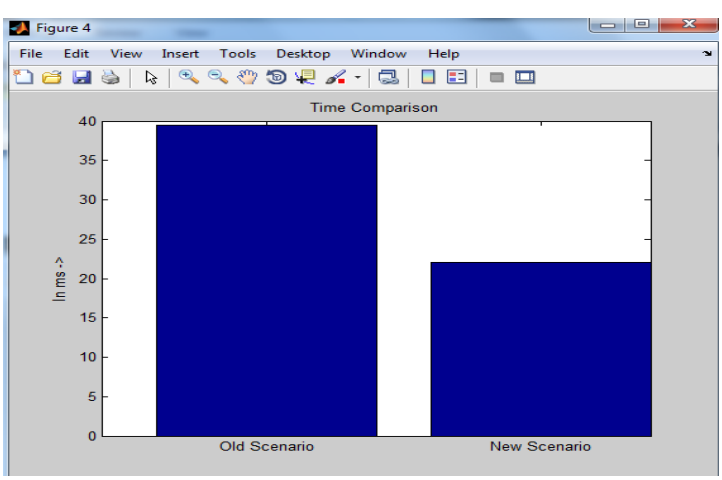

Figure 2: Comparison graph of delay

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.

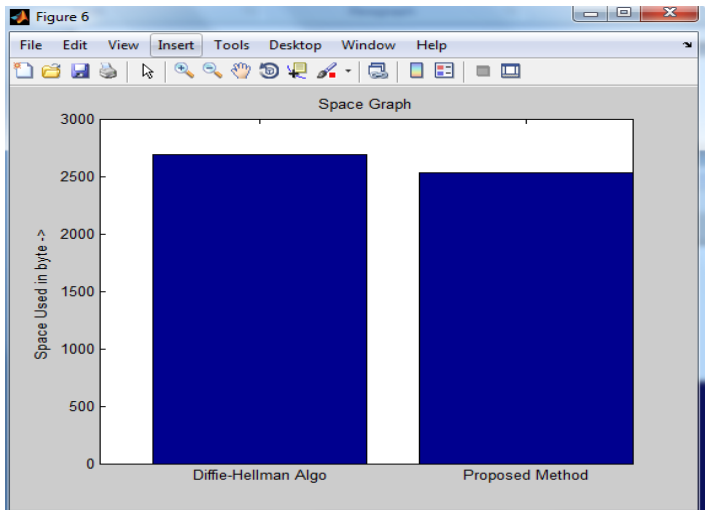

Figure 3: Comparison graph of Space

As shown in figure 3, the space utilization of existing Diffie-Hellman Algorithm is higher in comparison to the space utilization of proposed algorithm.

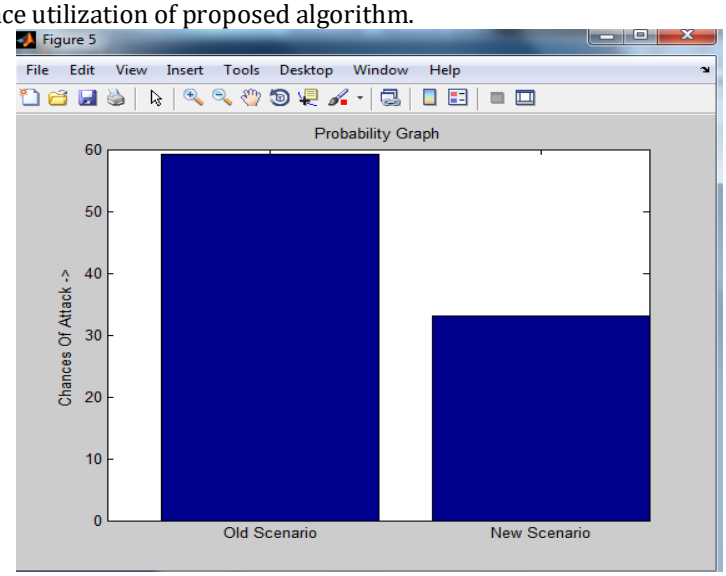

Figure 4: Comparison graph of probability

As shown in figure 4, the probability of attacks in existing scenario is higher and there is reduction in probability of attacks in novel proposed algorithm.

Conclusion

In this work, we find that fully homomorphic encryption technique is more efficient than full disk encryption. But the main problem that 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 has been proposed in the encryption scheme and enhancement is based on Elliptic Curve Cryptography algorithm and HMAC and OTP is generated on the basis of secret key generated from Elliptic Curve Cryptography algorithm. This algorithm create session key between user and cloud. Each time new key is generated between two before communication. This reduces the time that 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. M. Akinwande, "Advances in homomorphic cryptosystems." J. UCS, vol. 15, no. 3, pp. 506–522, 2009.
2. M. Togan and C. Plesca, "Comparison-based computations over fully homomorphic encrypted data," in Communications (COMM), 2014 10th International Conference on, 2014, pp. 1–6.
3. A. Chatterjee, M. Kaushal, and I. S. Gupta, "Accelerating sorting of fully homomorphic encrypted data," in Proceedings of the 14th International Conference on Cryptology in India, ser. INDOCRYPT '13, 2013 (Accepted).
4. C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009, crypto.stanford.edu/craig. [14] S. Rass and D. Slamanig, Cryptography for Security and Privacy in Cloud Computing. Norwood, MA, USA: Artech House, Inc., 2013.
5. C. Gentry, "Fully homomorphic encryption using ideal lattices," in STOC, M. Mitzenmacher, Ed. ACM, 2009, pp. 169–178
6. T. Toft, Sub-linear, Secure Comparison with Two Non-colluding Parties. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 174–191.
7. T. Veugen, F. Blom, S. J. A. de Hoogh, and Z. Erkin, "Secure comparison protocols in the semi-honest model," IEEE Journal of Selected Topics in Signal Processing, vol. 9, no. 7, pp. 1217–1228, 2015.
8. Bhavna Makhija, VinitKumar Gupta, 2013 "Enhanced Data Security in Cloud Computing with Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, pp 341-345
9. Vimmi Pandey, 2013 "Securing the Cloud Environment Using OTP" International Journal of Scientific Research in Computer Science and Engineering vol-1, Issue-4
10. Sanjoli Singla, Jasmeet Singh, 2013 "Cloud Data Security using Authentication and Encryption Technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013, pp 2232-2235
11. Ankur Mishra, Ruchita Mathur, Shishir Jain, Jitendra Singh Rathore, 2013 "Cloud Computing Security" International Journal on Recent and Innovation Trends in Computing and Computation, pp 36-39
12. Punithasurya K, Esther Daniel, Dr. N. A. Vasanthi, 2013 "A Novel Role Based Cross Domain Access Control Scheme for Cloud Storage" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013, pp 942-946
13. Barron, C., Yu, H., & Zhan, J., 2013 "Cloud Computing Security Case Studies and Research". Proceedings of the World Congress on Engineering 2013 Vol II