ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 5, May 2018

To Propose Secure Technique for Cloud Computing Using Elliptic Curve Cryptography

[1] Sapna, [2] Pooja Nagpal
[1] M.tech Scholar, Dept, CSE,Rayat Institute of Engg and Information Technology, Railmajra,Punjab ,INDIA
[2] Assist. Prof., Dept. of CSE, Rayat Institute of Engg and Information Technology, Railmajra, Punjab, INDIA

Abstract: **- The cloud computing is the architecture in which no central controller is present due to which various breaches occurred 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 homomorhic encryption scheme is more security and light as compared to fully disk encryption. In the paper, improvement in the fully homomrphic encryption is proposed using elliptic curve cryptography and OTP generation.**

I. INTRODUCTION

In the cloud computing environment, on-demand and convenient access to the network is provided by the computing resources such as storage, servers, applications, networks and many more. All these services, release the minimum efficiency in the network. In the cloud, three service models have been utilized for the functioning such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). First service model has the capability to use applications which are running on the cloud infrastructure by using internet connection in order to access those applications. The computational resources are provided by the Platform as a Service (PaaS), where services and applications are developed and hosted. The capability of the third model is to process, store and run software, which is provided to the customer [1]. As it provides the resources to a user as a service, it is also known as "Resource Code". In the three types of cloud, these cloud services are available such as public, private and hybrid cloud. Resource allocation in the public cloud is done publically as all the applications are on pay-per-use basis. Government organizations or business managed the public clouds. Resources are limited in the private cloud and used within an organization. The combination of both public and private cloud is known as hybrid cloud. Cloud security is defined as the security provided to the network such as network security, information security etc. [2]. In order to secure the data and applications within the cloud computing environment, this cloud security provides the various technologies, policies and controls measures. This security is not the part of the anti- virus. Nowadays, in every technology the major concern is security, in which there is external security or internal security. In the cloud data, privacy and integrity is the main requirements that is fulfill by the security of data [3]. In the cloud computing, there are various kinds of attacks that affect the functionality of the network. These attacks are possible due to exchange services and communication amongst users. Along various attacks, Denial of service (DOS) is commonly exists in the network, which harms the network and slows down its processing. It is the attack, large number of continuous messages is sends to server, by the attacker, which are zombie process in which wrong query crash the server and damage the resources. The man-in-the-middle attack (MITM) is also known as bucket brigade attack [4]. This attack, affects the communication between the two parties by placing itself in the middle of their communication path. Fully Homomorphic encryption: As compared to full disk encryption, better security is provided by the FHE. In this process, encryption is not applied on the full disk instead it is applied on each function. There is no relation between the cipher text and plain text, but main focus is on the algebraic operation that applied on both of them. The key fundamental of Homomorphic schemes are invented after the invention of RSA, Rivest, Adleman and Dertouzos [5]. There are private homomorphisms, also exists that demands for encryption function in order to operate data as it is not possible without encryption. Full Disk Encryption: Fully disk encryption (FDE) is the technique in which physical key has been utilized, for the process of encryption in order to provide better speed and simplicity in disk firmware [6]. This technique is very

effective in case of stolen laptop which can be protected and identified but it does not provide the data protection requirement as physical theft is not the major concern. Therefore, this techniques is considered as the most effective technique for securing private data on laptops, tapes etc., as personal data can be lost if encryption hard drive is not working properly.

II. LITERATURE REVIEW

Bhavna Makhija, (2013) proposed a Message Authentication Code (MAC) provides integrity to the data and, discussed the different techniques and their merits and demerits in this paper. For the larger file hash tree was used and the larger data into small parts are mitigated by the third party auditor for the maintenance and security. Data integrity and dynamic data operations are described by the proposed algorithm in which encryption key has been utilized in order to provide the data integrity. On the basis of homomorphic authenticator public key is defined in this paper. For the proof of retriveability, a hash function was used [7]. The main limitation of this proposed algorithm was that for the implementation, it causes high computational cost.

Vimmi Pandey, (2013) presented a Dynamic mobile token application, for the mobile phones. In order to generate a code with the help of OTP in the mobile phones this application is widely used. This one time password is used as name defines only once for the login session. Author in this paper describe the working of the OTP by doing various experiments. In this process, two phases were used for login such as Registration phase and Login phase [8]. The generated code is valid for three minutes only. This code is generated in order to prevent eavsdroppers attack and man-in-middle attack in the personal accounts. Therefore, on the basis of obtained results, it is demonstrated that security is provided by OTP and they provide effective security.

Sanjoli Singla, (2013) presented a model for the encryption and decryption process, in which data security is provided to user in both cases transmitting or receiving. The Rijndael Encryption Algorithm which is based on EAP-CHAP was utilized for the operation in this paper. For the data security, this process is followed by five steps within the proposed algorithm. Before storing data on the cloud, the major concern for the user is security and protection of their stored data [9]. Therefore, it is necessary to use Encryption technique in order to provide security to their saved data, hence Rijndael Encryption algorithm was used which provide optimal results.

Ankur Mishra, (2013) discussed two techniques such as Virtualization and Multi-tenancy by which security is provided to the cloud computing. Third party organizations, arrange all the data that offer Saas and PaaS for the security of the network. Therefore, due to security concerns Virtualization and Multi-tenancy techniques was utilized in this paper for experiments [10]. Computing services are provided by the Multi-tenancy to multiple customers as common infrastructure and code base is utilized in this process. It is also can be implemented to different levels such as application level, middleware level, operating system, hardware level.

Punithasurya, (2013) presented security is the major concern, when dealing with public cloud as it is very essential to protect data from any theft. Authentication, authorization and access control are the essential functions of the security. There are various access control schemes are available in the cloud storage. Privileges are provided by the access control that is the fundamental requirement of the user. Therefore, author proposed the Role Based Access Control (RBAC) method in this paper for security reasons, as it is the major concern nowadays [11]. It is demonstrated that this process increase the time location and availability of the resources.

Dian-Yuan Han, (2012) proposed a module, provides the security service to the user for the protection of their cloud. Three layers has been utilized to protect the cloud in the proposed method such as traditional transport layer, cloud computing layer and requirements, third is application-driven layer. Data security is provided by these three layers in the clod computing. Due to high availability, high fault tolerance and high efficiency accesses to the internet cause the failures which are now common in the cloud data centers [12]. Therefore, it is required to handle these significant issues carefully. Hence for the protection of data security module, agents were introduced that provides the effective and efficient service as minimization of these issues are more important that the requirement of high performance of the network.

III. RESEARCH METHODOLOGY

Elliptic Curve Cryptography methodology has been utilized, in order to protect the channel cryptography. To the well-known public key cryptography, this method is the extension. Public and private are the two keys utilized in the public key cryptography. A public key is applied for the encryption process, on the target information, by using predefined operations that will produce a pseudo-random number. In order to obtain the target information back, private key is applied to the pseudo-random number for which several predefined operations applied. This algorithm is based on the facts that encryption process is easy and decryption is hard as without the key implementation of decryption is impractical. Hence,

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 5, May 2018

security to the transferred information is provided by this system without using a shared key. With the advent in the technology, the utilization of the computers is increased worldwide therefore it is not possible to generate large number of pseudo-prime, in order to prevent attacks within the network. Hence, to overcome this issue elliptic curve cryptography has been utilized as it uses the properties of an elliptical curve, pairing of keys and math for the encryption and decryption of the target information. Generated points by the elliptic curve are represented in the form of graph by the following equation:

$y2 = x3 + ax + b$

Algorithm:

selected node suppose user1

1. Login
2. Key generation

2.1 Enter prime numbers

2.2 Enter random numbers by client and cloud service provider

2.3Secret key generation and secure channel establishment

3. OTP (One Time Password) generation

3.1 cloud server will set count1=0, count2=0...count5=0 for respective user at its side.

3.2 Cloud Server will request for the OTP from user 1

3.3 user1 enter (secret key+count) as OTP

3.3 server match it because server knows both secret key and count of each user.

3.3.1: count1++; // so for user 1 it will be count1=1; for remainig user their count will be still 0;

3.3.2 if (secret_key+count(x) == secret_key+count(y)) {Access granted; display message by server : print ("please enter the operation");}

Else

{Display message by server: print (" wrong password, your login number is count1) ;}

4.4 clinet will enter the operation using HMAC digest

4.4.1 : hmac(already generated secret key || v, file1,ver1 || sha1)

{ if(ope==v)

{server will check the file name and version;

if

(file1,ver1== file1,ver1)

{ printf("file is valid"); }

Else

{ print (file is invalid, please replace the file)}}

if (ope==I) { insert new file file2 }

5. encryption/decryiton
6. data operation

7 .logout;

note: // 1.at client side, user will enter prime number, random number for generating secret keys, once generating secret key user will enter otp , after inserting otp, user will enter operation(Insertion) with corresponding file name(file1 or file2).

IV. EXPERIMENTAL RESULTS

V.

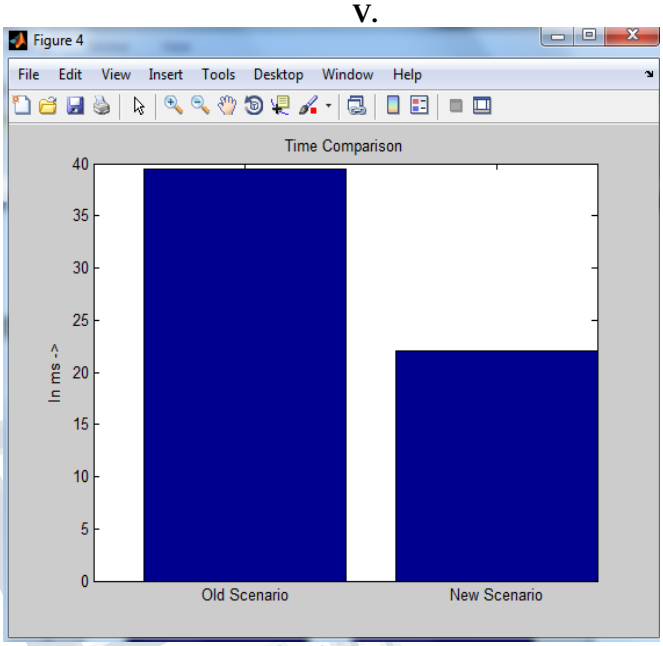

Figure 1: Comparison graph of delay

As shown in figure 1, it is the comparison graph in which proposed approach is compared with previously given method in terms of delay. With the increase in the numbers of exchange messages, there is increase in delay as well in the previous technique. But in case of proposed method there is decrease in delay with the increase in number of messages.

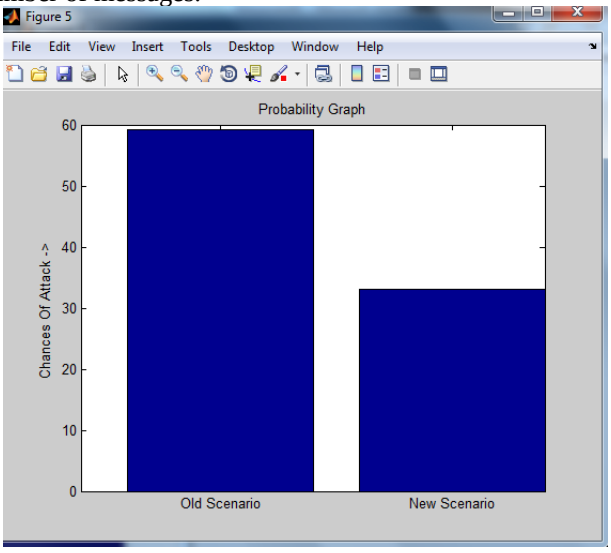

Figure 2: Comparison graph of probability

As shown in figure 2, in terms of probability, the comparison between previous and proposed approach is shown in the graph. With the increase in the number of exchange messages, there is increase in the probability in previous technique. However, there is decrease in the probability, in the proposed approach with the increase in number of messages.

V. CONCLUSION

In this paper, two most popular techniques were utilized for the encryption of data in the cloud computing environment. Full disk encryption (FDE) and fully homomorphic encryption (FHE) are the two fumndamental techniques were utilized. As per perforemed experiments, it is demonstrated that more efficient results are provided by the homomorphic encryption as compared to disk encryption. But, key management and key sharing are the major limitation of the homomorphic encryption which reduces the consistency of the method. Therefore, in order to mitigate the effects of these limitations, enhancement was done in the proposed method in the encryption by utilizing, Elliptic Curve Cryptography algorithm and HMAC. By using, Elliptic Curve Cryptography algorithm an OTP was generated that for the security. Hence, on the basis of simulation results, it is concluded that efficient and reliable results are provided by the enhanced proposed algorithm.

REFERENCES

[1] Deepanchakaravarthi Purushothaman1 and Dr.Sunitha Abburu2 ,2012" An Approach for Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1

[2] Dr Nashaat el-Khameesy,Hossam Abdel Rahman, 2012 "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems" vol-3

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

[4] Sean Carlin, Kevin Curran, 2011 "Cloud Computing Security" International Journal of Ambient Computing and Intelligence, pp 14-19

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

[6] Vimmi Pandey, 2013 "Securing the Cloud Environment Using OTP" International Journal of Scientific Research in Computer Science and Engineering vol-1, Issue-4

[7] 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

[8] Vimmi Pandey, 2013 "Securing the Cloud Environment Using OTP" International Journal of Scientific Research in Computer Science and Engineering vol-1, Issue-4

[9] 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

[10] 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

[11] 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

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