Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 16 Issue 2 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

To Enhance the OTP Generation Process for Cloud data Security using Diffie-Hellman and HMAC

By Gagandeep Kaur Sandhu & Er. Gurjit Singh
Punjabi University

Abstract- Cloud computing is an innovation or distributed network where user can move their data and any application programming on it. In any case, there is a few issues in cloud computing, the main one is security on the grounds that each user store their helpful data on the network so they need their data ought to be protected from any unapproved access, any progressions that is not done for user's benefit. There are diverse encryption methods utilized for security reason like FDE and FHE. To tackle the issue of Key management, Key Sharing different plans have been proposed. The outsider auditing plan will be fizzled, if the outsider's security is bargained or of the outsider will be malicious. To tackle this issue, we will chip away at to design new modular for key sharing and key management in completely Homomorphic Encryption plan. In this paper, we have utilized the symmetric key understanding algorithm named Diffie Hellman, it is key trade algorithm with make session key between two gatherings who need to speak with each other and HMAC for the data integrity OTP(One Time Password) is made which gives more security. Because of this the issue of managing the key is expelled and data is more secured.

Keywords: *OTP, HMAC, diffie-hellman, cloud security, FHE, FDE.*

GJCST-B Classification : *H.2.7 C.2.1 C.2.3*

Strictly as per the compliance and regulations of:

To Enhance the OTP Generation Process for Cloud data Security using Diffie-Hellman and HMAC

Gagandeep Kaur Sandhu[α] & Er. Gurjit Singh[σ]

Abstract- Cloud computing is an innovation or distributed network where user can move their data and any application programming on it. In any case, there is a few issues in cloud computing, the main one is security on the grounds that each user store their helpful data on the network so they need their data ought to be protected from any unapproved access, any progressions that is not done for user's benefit. There are diverse encryption methods utilized for security reason like FDE and FHE. To tackle the issue of Key management, Key Sharing different plans have been proposed. The outsider auditing plan will be fizzled, if the outsider's security is bargained or of the outsider will be malicious. To tackle this issue, we will chip away at to design new modular for key sharing and key management in completely Homomorphic Encryption plan. In this paper, we have utilized the symmetric key understanding algorithm named Diffie Hellman, it is key trade algorithm with make session key between two gatherings who need to speak with each other and HMAC for the data integrity OTP(One Time Password) is made which gives more security. Because of this the issue of managing the key is expelled and data is more secured.

Keywords: OTP, HMAC, diffie-hellman, cloud security, FHE, FDE.

I. Introduction

Cloud computing is the earth which gives on-demand and helpful access of the network to a computing resources like storage, servers, applications, networks and the other services which can be discharged minimum effectiveness way. The five key characteristics made by cloud design. Cloud design likewise advances the accessibility [5]. User retrieved data and changed data which is stored by client or an association in centralized data called cloud. Cloud is a design, where cloud service provider gives services to user on demand and it is otherwise called CSP stands for "Cloud Service Provider" [3]. It implies that the user or the client who is using the service needs to pay for whatever he/she is using or being utilized and served. There are three deployment models and three services models defined by NIST, theses are:

Author α σ : Bhathal Student, Assistant Professor, Department of Computer Science, Punjabi University, Patiala, Punjab. e-mail: sandhugagandeep200@gmail.com

a) Service Models: There are three service models of cloud-

i. *Software as a Service (SaaS)*

This is the ability of using applications which are running on cloud infrastructure. The users access these applications through internet associations. These kinds of clouds offer the usage of some particular business strings that gives particular cloud abilities. For E.g. GMAIL, Facebook [2].

ii. *Platform as a Service (PaaS)*

It gives the computational resources on which services and applications can be host and create. For E.g. Online Photo Editing, Google Docs, YouTube [12]

iii. *Infrastructure as a Service (Iaa* S)

This is the ability of doing processing, storing and run software which is given to the buyer. It's additionally alluded as the "Resource Code" which gives resources as the services to a user. This work is finished by the service provider. For E.g. Host Firewalls [6].

b) Deployment Models

Cloud services are mainly available in the three types of cloud. These clouds are as follows-

i. *Public Cloud*

In this cloud, resources dispensed are publically. Applications in this cloud are on pay-per-use premise. Public clouds can be managed by government organizations or business. For E. g. Sky Drive and Google Drive [2].

ii. *Private Cloud*

In this cloud, resources are constrained and used within an association. It is more secure as representatives in an association can access the specific data as it were. For E. g. Banks [12].

iii. *Hybrid Cloud*

In this cloud, there is a combination of both Public and Private cloud. The services within the association are control by the client and resources which should be conveyed remotely are controlled by the service provider [12].

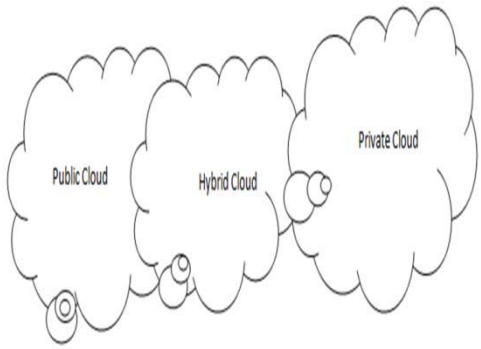

Fig. 1.1 : Deployment model of Cloud

c) Cloud Computing Security

Network security, information security and many other security sorts like the PC security together make the expression "Cloud Security" because it comprise the greater part of the security system as given above. It gives the expansive set of innovations, policies and controls that are used to secure the data and applications exist with the cloud computing environment [8]. It is not the result of PC security like hostile to viruses and against spam's. Security is the most concerning point to any service. Outer security or internal security required to every field. Just security guarantees the privacy and integrity the cloud data. There are many security loopholes exist in the service. There are many sorts of security issues exist like DDOS, Man in the middle and so on. Some security sorts include:

i. *Outages*

This term alludes to the issue of the user where he/she is not ready to access services because of the provider being down. Assume there is some imperative business meeting and user require a document for the presentation and provider's site is down. This may happen part of times [8].

ii. *Data Loss*

Due to lack of security data may be lost during uploading on cloud because of nearness of malicious hub [11].

iii. *Phishing*

It is an email misrepresentation trick which is directed with the assistance of network investigation stream tool to concentrate information from the server.

II. Review of Literature

In this paper [1] they proposed distinctive systems and their benefits and bad marks like Message Authentication Code (MAC) which protect the data from integrity. The proprietor of any information checked the data integrity by recalculating the message authentication code of data got by others however recalculation is conceivable if the measure of data is huge. A hash tree is used for extensive files. Outsider auditor is used to alleviate the substantial data into little parts of maintenance and security. The proposed algorithm depicts data integrity and dynamic data operations. They use encryption to ensuring the data integrity. Public key is likewise defined which is based on homomorphic authenticator. A hash function is used for evidence of retriveability. The proposed algorithm has a main drawback that it require usage of the higher resources cost. In this paper [2] Dynamic versatile token application is introduced. This is the application in cellular telephones which is used to produce a code with the assistance of OTP (One Time Password). This OTP code is used just for one an opportunity to login session. In this paper, they depict one of the techniques for OTP. There are two phases in it Registration phase and Login phase. User first enlists itself by fill credentials in the structure and then enters to the Login phase. In login phase, OTP will produce for the login session. OTP is produced by three parameters: The present time, 4-digiti PIN code and Init-mystery. This code is legitimate for three minutes as it were. This guarantees protection against eavsdroppers attack and man-in-middle attack. Henceforth, they demonstrate OTP is extremely secure. In this paper [3] a design and engineering is recommended that can scramble and unscramble the file at the user side which gives data security in both cases while user is very still or is transferring data. In this paper they used the Rijndael Encryption Algorithm alongside EAP-CHAP. This algorithm has five stages which should be take after for the data security. The users are dependably worry about the privacy protection and security issues before storing their data on cloud. So in this the attention is on client side security in which just the approved user can access the data. Regardless of the possibility that some intruder (Unauthorized user) gets access of the data then the data won't be unscramble. Encryption must be finished by the user to give better security Algorithm. For this, Rijndael Encryption algorithm is used. In this paper [4], two strategies are talked about: Virtualization and Muti-tenancy which gives security about cloud computing. Data is sorted out by outsider organizations that offer Saas and PaaS which is critical for the security. In this way, Virtualization and Multi-tenancy strategies are used for the security purposes. Virtualization is a method for making a physical PC function as though it were two or more PCs where each non-physical or virtualized. There are two sorts of virtualization: Full virtualization and Para virtualization and two designs of virtualization: Hosted and Hypervisor engineering. Multi-tenancy is the capacity to give computing services to different clients by using a typical infrastructure and code base. Multi-tenancy can be connected to various levels i.e. application level, middleware level, operating system, equipment level. Then security of virtualization and multi-tenancy has been talked about. In this paper [5] they talked about various issues identified with cloud

computing security. To protect cloud computing system and to counteract different attacks many security instruments have been created. To enhance the security of cloud computing new innovations has been created by the analysts. Distinctive sorts of attacks like SYN flood, malware injection, account hijacking are examined in this paper. The main center of this paper is on detecting and preventing SYN flood in cloud computing. The creator created two algorithm one detecting algorithm and one preventing algorithm. They will actualize and test these algorithms on cloud computing.

III. Diffie-Hellman and OTP

Diffie Hellman was the primary public key algorithm or we can say that it is symmetric key agreement ever invented, in 1976. Diffie Hellman key agreement protocol is [6]:

1. It allows exchanging a secret key between two parties.
2. Exponential key agreement
3. Requires no prior secrets

a) Definition of Diffie Hellman

Before establishing a symmetric key, the both the two parties need to pick two numbers n and p. Give n a chance to be a prime number and p be an integer. The Diffie Hellman Problem (DHP) is the issue of computing the estimation of p^{ab}(mod n) from the known estimations of p^a (mod n) and p^b (mod n).The setup of Diffie Hellman algorithm

Assume that we have two parties Alice (Master) and Bob (Slave), they need to convey to each other.

They don't need the eavesdropper to know their message.

Alice and Bob concur upon and make public two numbers n and p, where n is a prime number and p is a primitive root mod n. Anybody has admittance to these numbers.

Table 1 : Private computations

Alice	Bob
Choose a secret number a. Compute M≡ p^a (mod n)	Choose a secret number b Compute S≡ p^b(mod n).

Generated public values are exchanged.

- Alice sends M to Bob ==M
- S= Bob sends S to Alice
- Alice calculate the number K≡ $S^a \equiv (P^a)^b$ (modn).
- Bob calculate the number K≡$M^b \equiv (p^b)^a$ (mod n).

Here Alice and Bob have the same key that is K=p^{ab} (mod n).

In the Diffie-Hellman algorithm if two parties, say, Master and Slave wishes to trade data, both concur on a symmetric key. For encryption or decryption of the messages symmetric key is used. We realizes that Diffie Hellman algorithm is used for just key agreement or key trade, however it doesn't used for encryption or decryption. Before starting the correspondence, secure channel is set up between both the parties [5]. Both parties select their own particular random number. On the premise of the chose random numbers, secure channel and shared key is built up.

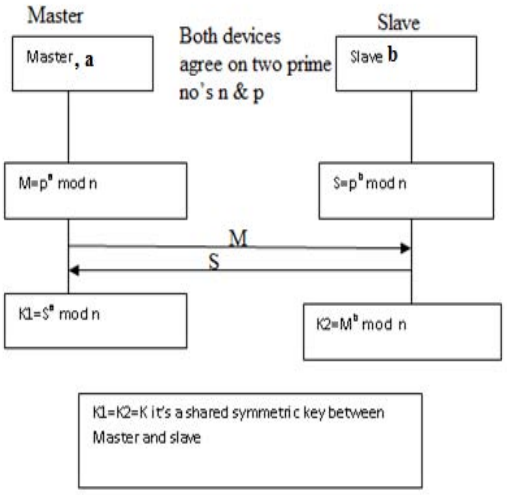

Fig.1.2 : Diffie-Hellman Key exchange

Figure1.2 demonstrates that Master and Slave needs to speak with each other. To begin correspondence both parties need to build up secure channel. To set up secure channel, two random prime number p and n are chosen, both gadgets are concurred on these two numbers. Chosen p and n are the public numbers. Both parties, say gadget 1 get to be master and gadget 2 get to be slave; both master and slave select their private numbers "an" and "b" individually. Master and slave use their public and private number and computed their private keys [15].

Master computes:

M= p^a mod n

Slave computes:

S= p^b mod n

Now both master and slave exchange their private keys such as 'M' and 'S'. After getting 'M' and 'S', master and slave calculates the secret keys such as K1, K2.

From S, master computes:

K1= S^a mod n

From M, slave computes:

K2= M^b mod n

If both master and slave calculate same values of K1 and K2, then secure channel is established between them. The combination of K1 and K2 becomes the shared symmetric key between master and slave.

To encrypt the messages, they used the public key or shared key (K) of both parties. For decryption of

messages private key of both parties which is randomly chosen by the users i.e. 'a' and 'b' are used [16].

a) One Time Password

Password is used for authentication by all the business and association. In addition Static passwords have many impediments. Password can be get hacked. Lackadaisical representative may note down passwords some place, system with spared passwords might be used by different users or a malicious user may reset all passwords just to make destruction. So it is exceptionally useful to use dynamic password i.e. one time password [10]. Dynamic passwords are more secure when contrasted with static. There is no compelling reason to record these passwords and recollect these passwords. For each login session every time another password is produced. One time passwords are more reliable and user friendly also for authentication. OTP generation should be possible by different OTP generation algorithms for generating strings of passwords. OTP guarantees security. This prompts authenticating them again and again over the period of time for each login session. To maintain a strategic distance from the overhead we can use OTP for multi cloud environment.

IV. Proposed Methodology

There are many encryption algorithms to give security to the cloud. "Fully Homomorphic" is more reliable. It gives more privacy and security as contrast with plan of "Full Disk Encryption". The main issue which is there in Fully Homomorphic Encryption is a key storage, key management, Access control and Data Aggregation list maintaining. To tackle issue of Key management, Key Sharing different plans have been proposed in a years ago. The different security attacks are conceivable in these plans. The outsider auditor is the plan for key management and key sharing. The outsider auditing plan will be fizzled, if the outsider's security is bargained or of the outsider will be malicious. To take care of this issue, In this thesis we will take a shot at to design new model for key sharing and key management in fully Homomorphic Encryption plan. In this work, we find that fully homomorphic encryption system is more effective than full disk encryption. Yet, the main issue exists in fully homomorphic encryption is of key management and key sharing which decreases the reliability of the plan. For key management and key sharing, improvement has been proposed in the encryption plan and upgrade is based on Diffie-hellman algorithm and HMAC and OTP is created on the premise of mystery key produced from Diffie-hellman algorithm. This algorithm makes session key amongst user and cloud. Every time new key is produced between two preceding correspondence 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).

V. Exprimental Results

The whole scenario has been implemented on MATLAB tool.

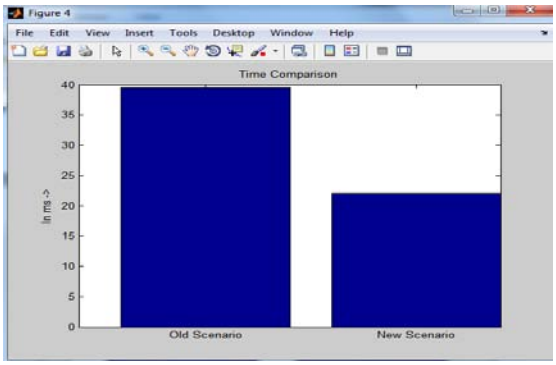

Fig. 1.3 : Comparison Graph

As appeared in figure 1.3, the comparison amongst previous and proposed methodology is appeared as far as delay. The delay in previous system is increasing, when numbers of trade messages are increased. In the proposed approach the delay is less because of increasing the number of message.

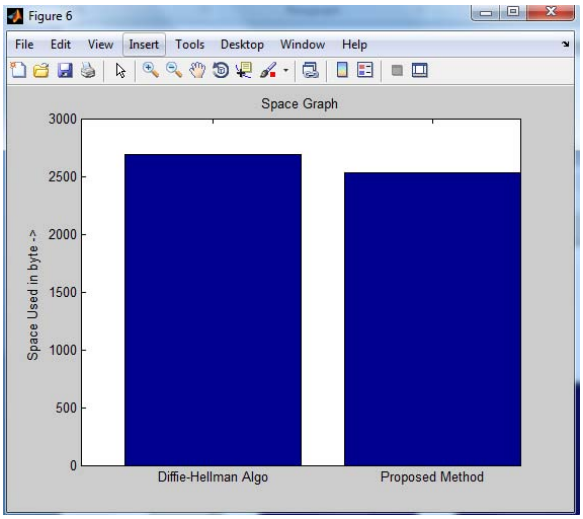

Fig.1.4 : Comparison with Diffie Hellman in terms of used bytes

As appeared in figure 1.4, the comparison amongst previous and proposed methodology is appeared as far as used bytes. The used byte in previous method is increasing, when numbers of trade messages are increased. In the proposed approach the data utilization is less when contrasted with existing strategy.

VI. Conclusion

Cloud computing is the environment which gives on-demand and helpful access of the network to a computing resources like storage, servers, applications, networks and the other services which can be discharged minimum productivity way. In this user can store their data and use diverse services and pay according to those services. The main component is security that how we can store our data while storing into the cloud. In this thesis, we audited two most prevalent procedures for cloud data encryption. These systems are full disk encryption and fully homomorphic encryption. In this work, we find that fully homomorphic encryption method is more proficient than full disk encryption. Yet, the main issue exists in fully homomorphic encryption is of key management and key sharing which lessens the reliability of the plan. For key management and key sharing, improvement has been proposed in the encryption plan and upgrade is based on Diffie-hellman algorithm and HMAC and OTP is produced on the premise of secret key created from diffie-hellman algorithm. This algorithm makes session key amongst user and cloud. Every time new key is produced between two preceding correspondence. This decreases the time happens in management and sharing of keys and secure channel is set up between both i.e. user and the cloud service provider. The simulation demonstrates that proposed improvement is more proficient and reliable than the existing one.

References Références Referencias

1. 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.
2. Vimmi Pandey, 2013 "Securing the Cloud Environment Using OTP" International Journal of Scientific Research in Computer Science and Engineering vol-1, Issue-4.
3. 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.
4. 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
5. 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.
6. Barron, C., Yu, H., & Zhan, J., 2013 "Cloud Computing Security Case Studies and Research". Proceedings of the World Congress on Engineering 2013 Vol II.
7. Craig Gentry, 2009,"full homomorphic encryption scheme" .
8. Dawn Song, Elaine Shi, 2012 "Cloud Data Protection for the Masses" IEEE Computer Society, pp 39-45.

9. Deyan Chen, Hong Zhao, 2012" Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering, pp 647-651.
10. Deepanchakaravarthi Purushothaman[1] and Dr.Sunitha Abburu[2] ,2012" An Approach for Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1.
11. 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.
12. Dr Nashaat el-Khameesy, Hossam Abdel Rahman, 2012 "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems" vol-3.