ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 4 , April -2017

Research Paper

CLOUD SECURITY USING HOMOMORPHIC ENCRYPTION

NILESH KUMAR SEN[1], NAVDEEP KAUR SALUJA[2]

1. **M.TECH, SCHOLAR, DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, INFINITY MANAGEMENT & ENGINEERING COLLEGE, SAGAR, (M.P.), INDIA**
2. **HOD, DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING, INFINITY MANAGEMENT & ENGINEERING COLLEGE, SAGAR, (M.P.), INDIA**

ABSTRACT

Cloud computing is the process of storing large amount of data in order to have efficient retrieval for future use. Cloud computing doesn't provide storage capabilities only instead it is capable of having many security features. Initially when the data storage of user was encourage using cloud capabilities then it is observed that the plain-text data is intercept by intermediate communicator and manipulated. In our work the encryption is performed by applying the technique of Homomorphic encryption. The storage of data in performed in AWS, where the data is stored in such a form that service provider will not be capable of manipulation hence result in efficient processing. The work will contribute in field of security as in public cloud the accessing is provided to multiple clients.

KEYWORDS:

DATA SECURITY; CLOUD COMPUTING; FULLY HOMOMORPHIC ENCRYPTION; AWS; PUBLIC CLOUD;

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 4 , April -2017

INTRODUCTION

In all the field of cloud security is one of the prime goals. No matter where the data is being kept at network layer, application layer or at presentation layer, the security is always a big question. The cloud computing is associated with so many technologies, some security issues which must be taken into consideration while providing cloud security[6] is mentioned as below:

1. *Availability:*

In cloud security environment availability is highly desired as user needs to access their data anytime they want, hence data must be available to client end, third party as well as server. Third party services are usually important in bulk amount of data. Along with it, access control, authentication and authorization is also needed in cloud security. Network attacks are one of the major threats in communication [2].

2. *Data recovery*

If any unauthorized access to data is being found then the third party which is doing so is discarded as authorized party, in that case there is high risk of data theft and data privacy issues. Hence data destruction is major concern in cloud environment.

3. *Third party services*

User is highly depended on third party vendors for storage and transfer of their data, this data can be witness from intruders as well as sometimes from the third party vendors as well. The work suggest there should not be dependency on one such cloud providers, it should be large in numbers.

4. *Data privacy*

As it is well-known that data is stored in so many data centers hence its physical location is unknown to user. Each country is having legal policies hence users are very much afraid of storing their confidential data on cloud servers. The privacy issues in uploading data on sites can be realized from the work observed by Pearson [9].

The security policy of cryptography provides the feature of encryption which states the data will be converted in unreadable format. The encrypted data is tough to read until decryption is being performed, but there are the techniques which suggest the encrypted data can be converted into readable format using appropriate keys. As the processing on data is desired the decryption have had to done. The data travel in cloud in explained through diagram given below:

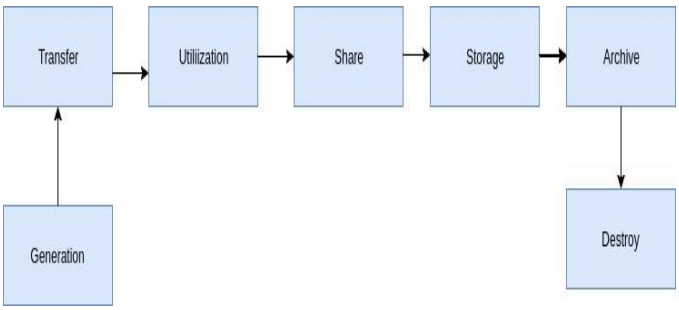

Fig. 1. Data cycle in cloud

Cloud security is one of the major criteria in current scenario. The users are trying to make their data as convenient as possible. The cloud providers are available in large amount and each one is trying to provide their users best possible features. The increase in cloud computing popularity occurs from

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 4 , April -2017

the day to day use of applications like social networking sites, blogs and many others.

Homomorphic encryption is the encryption technique which allow to have encryption with the feature that doesn't required your text to be decrypted in order to perform processing, hence if any third party vendor is present in mid between then it is very difficult for that to get the confidential information which is exchanged between client and server.

Homomorphic encryption can be to two types first in which only one operation is performed know as partial homomorphism[3], whereas second is one in which all possible operations can be performed. Homomorphic encryption is based on the concept of providing the security from third party data theft. The mechanism allows to have data processing from third party but not anything else apart from them. Researchers also claim that till date fully homomorphic encryption is not achieved. The mechanism of the scenario is shown in figure below:

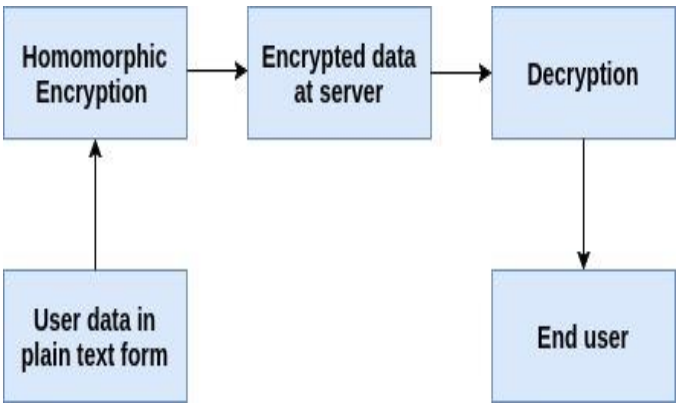

Fig. 2. Homomorphic encryption

LITERATURE REVIEW

At initial Homomorphism is introduced by Rivest, Adleman and Dertouzos in their work, after the invention of RSA crypt-system [10]. In their work they proposed the mechanism but was unable to find the solution. All the inventors of traditional and very secure algorithm of cryptography initiates to find their solution where multiplicative homomorphism is given by RSA [11]. Partial homomorphism scheme is also contributed by Goldwasser and Micali [13], ElGamal [14] and Paillier [15]. Fontaine & Galand [16] has conferred a survey of homomorphic encryption whereas Gentry gives the concept of fully homomorphic encryption in his work [17].

Numerous researchers proposed the variants of Gentry's model with some additional features. Smart and Vercauteren suggested Homomorphic encryption on smaller size cipher-text [18]. The arithmetic operations over integers are proposed by Dijk, Gentry, Halevi, and Vaikuntanathan[19]. Faster improvement to Gentry's model is proposed by Stehle and Steinfield [20]. Y Govinda Ramaiah researched "Efficient Public Key Homomorphic Encryption over Integer Plaintexts"[4].

PROBLEM DOMAIN

It has been finding since very long that data transfer using cloud services is widely adopted. But the data in it doesn't have any assurance of not getting misuse or theft in communication. The sender though sends encrypted data need to get decrypted

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 4 , April -2017

at receiving end. In mid between the cloud vendor perform storage and retrieval, but their always the shared key which allow cloud vendor to have access to data. There should be some encryption technique which facilitates cloud vendor data access but not the content of data.

SOLUTION DOMAIN

Cloud security is one of the major issues in field of computer science. As cloud is not just responsible for not just storing of data but it provides facilities like IaaS, PaaS which signify it can provide services which can have platform and entire infrastructure as well. Cloud services also allows user to have in organization and out organization facilities also with the help of private, public and hybrid cloud. All the large enterprises are funding in this field some of the well-known examples are Google Drive, Amazon AWS, Windows Azure, Hadoop and many such. All this cloud providers are the market achiever from the fact that they designed the well-mannered layered protocol before providing any of the services. Thus in order to make everyone more cloud friendly cloud security is must.

In our work, we are providing the algorithm for implementing Homomorphic encryption by implementation of it of Amazon web services. The aim is to have the processing which must be strong enough to ensure no data theft in process of transfer.

Cloud server is responsible for data storage and accessibility is provided only to registered user. The IDE used in this work is Eclipse in which there is inbuilt capability of connecting through Database of Amazon. Each user will have some credentials and can login and logout to system as per the need. Initially the instance on AWS of database is created, and then tables and proper schema are designed. Access control policies are planned to provide different access rights to different users. The installation of Amazon SDK [23] is performed with the help of previous work and the version of Eclipse which is desired is Kepler. The algorithm is given in next part.

1) Algorithm

In the given algorithm the parameters input are given as under:

a) Secret key: S_{pr1}, S_{pr2}

b) Public key: $P_{pu1,}$ P_{pu2}

c) Number which is input: N

d) Random numbers: $Rand_1$, $Rand_2$

e) Input is given as S_{pr1}=64 bit, S_{pr2}= 16 bit and number to be encrypted N=any natural number, then $Rand_1$ and are $Rand_2$ calculated as

f) $Rand_1$=256 bit number

g) $Rand_2$= 256 bit number

Consider four bit number K' compute

h) $P_{pu1} = S_{pr1} * Rand_1$ and

i) $P_{pu2} = (S_{pr1} * Rand_2) + KK'$

j) T_1 , T_2 are a 4-bit random integer

Perform Encryption and get

k) $P_0 = [T_1 P_{pu1}] \bmod P_{pu2}$

Encryption

l) Cipher Text $C = [N + T_2 P_0] \bmod P_{pub1}$

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 3 , Issue- 4 , April -2017

Decryption is performed and get back plain text N=input natural number.

2) Modules

- Client Machine- The client request for the data using its terminal, in order to access the desired data.
- Login- Each user will have the definite credentials with the help of which user will sign in to the system if input given are validated only.
- Key Selection- Each user will have certain key with the help of which user will login into the system, the keys are responsible for encryption and decryption.
- Query- After one connection of assigning the credentials, user is allow to have connection as many times he wants to , user fires the query and get the desired result.
- Computations- In order to get the result the computations are performed based on the query feed by the user.
- Encrypt and store- The data is converted into unreadable form and then feed to cloud server in the same format in order to achieve security.
- Retrieve and decrypt- The receiving end accept the data , decrypt it using necessary key and then utilize it for future use.
- AWS Cloud- The necessary functionality are provided by cloud service provider which retrieves the data and then present to user. The cloud service provider performs all the necessary validations check, if user is authenticating only then it allows the data transfer to user. Cloud server is responsible for data storage and accessibility is provided only to registered user.

Once the required step up is formed the Java code with respect to it is created. The flowchart of given work is mentioned below:

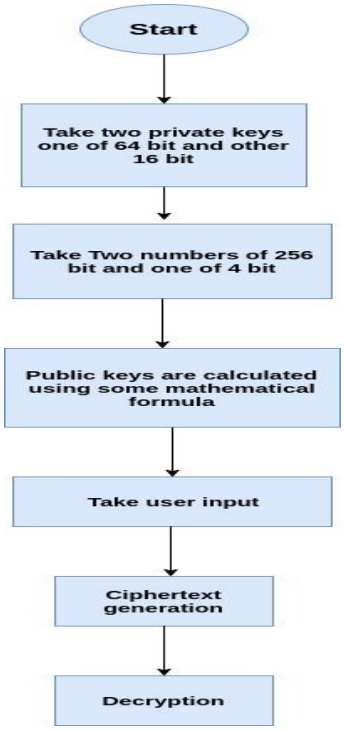

Fig. 3. Algorithm for given work

REFERENCES

[1] Tebaa, M.; El Hajji, S.; El Ghazi, A., "Homomorphic encryption method applied to Cloud Computing," in Network Security and Systems (JNS2), 2012 National Days of , vol., no., pp.86-89, 20-21 April 2012

[2] Mather, Tim, Subra Kumaraswamy, and Shahed Latif. Cloud security and privacy: an enterprise perspective on risks and compliance. "O'Reilly Media, Inc.", 2009

[3] Samyak Shah, Yash Shah, Janika Kotak, “Somewhat Homomorphic Encryption Technique with its Key Management Protocol”, Dec 14

[4] Volume 2 Issue 12 , International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), ISSN: 2321-8169,PP: 4180 – 4183

[5] Ramaiah, Y. Govinda, and G. Vijaya Kumari. "Efficient public key homomorphic encryption over integer plaintexts." Information Security and Intelligence Control (ISIC), 2012 International Conference on. IEEE, 2012.

[6] Gentry, Craig. "Computing arbitrary functions of encrypted data." Communications of the ACM 53.3 (2010): 97-105.

[7] Atayero, Aderemi A., and Oluwaseyi Feyisetan. "Security issues in cloud computing: The potentials of homomorphic encryption." Journal of Emerging Trends in Computing and Information Sciences 2.10 (2011): 546-552.

[8] Catteddu, Daniele, and Giles Hogben. "Cloud computing." Benefits, Risks and Recommendations for Information Security/European Network and Information Security Agency, ENISA (November 2009) (2009).

[9] Deyan Chen; Hong Zhao, "Data Security and Privacy Protection Issues in Cloud Computing," in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on , vol.1, no., pp.647-651, 23-25 March 2012.

[10] Pearson, Siani. "Taking account of privacy when designing cloud computing services." Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. IEEE Computer Society, 2009.

[11] Rivest, Ronald L., Len Adleman, and Michael L. Dertouzos. "On data banks and privacy homomorphisms." Foundations of secure computation 4.11 (1978): 169-180.

[12] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems."Communications of the ACM 21.2 (1978): 120-126.

[13] A. C. Yao. Protocols for secure computations (extended abstract). In 23rd Annual Symposium on Foundations of Computer Science (FOCS '82), pages 160-164. IEEE, 1982.

[14] Goldwasser, Shafi, and Silvio Micali. "Probabilistic encryption." Journal of computer and system sciences 28.2 (1984): 270-299.

[15] ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." Advances in cryptology. Springer Berlin Heidelberg, 1985.

[16] Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity classes." Advances in cryptology—EUROCRYPT'99.Springer Berlin Heidelberg, 1999..

[17] Fontaine, Caroline, and Fabien Galand. "A survey of homomorphic encryption for nonspecialists." EURASIP Journal on Information Security 2007 (2007): 15.

[18] Gentry, Craig. "Fully homomorphic encryption using ideal lattices." STOC. Vol. 9. 2009.

[19] Smart, Nigel P., and Frederik Vercauteren. "Fully homomorphic encryption with relatively small key and ciphertext sizes." Public Key Cryptography–PKC 2010. Springer Berlin Heidelberg, 2010. 420-443.

[20] Van Dijk, Marten, et al. "Fully homomorphic encryption over the integers." Advances in cryptology–EUROCRYPT 2010. Springer Berlin Heidelberg, 2010. 24-43.Stehlé, Damien, and Ron Steinfeld. "Faster fully homomorphic encryption." Advances in Cryptology-ASIACRYPT 2010. Springer Berlin Heidelberg, 2010. 377-394.

[21] Amazon Web Services DynamoDB, Available: Amazon Web Services Online,http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/Introduction.html.

[22] Amazon Web Services DynamoDB, Available: Amazon Web Services Online, https://github.com/amazonwebservices

[23] AWS Toolkit For Eclipse,http://docs.amazonaws.cn/en_us/AWSToolkitEclipse/latest/GettingStartedGuide/aws-tke-gsg.pdf?

[24] Gentry, Craig. A fully homomorphic encryption scheme. Diss. Stanford University, 2009.