International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S, August 2019

Homomorphic Encryption – Need of the Hour

Dakshita Sharma, Purushottam Sharma, Vikas Deep

Abstract*: Every common day the headlines of the newspaper are buzzed with data leaks and mobbing of data. The hackers are considering human just as a moving data. As the technology is advancing, we are more prone to cyber-attacks. With the ease of advancement there are certain cons which are approaching towards us. To protect the individuality of a human being, few governments of different countries have taken a step ahead to demoralize the illegal access to data hence inhibiting security. Homomorphic encryption is the trend or technique by which data can be protected as the encryption is done on the ciphertext. In this paper different types and techniques of homomorphic encryption is discussed. The techniques provide a secure environment for data to run on any application.

***Keywords*: Hackers, Technology, Cyber-attacks, Security, Homomorphic Encryption, Ciphertext.**

I. INTRODUCTION

Homomorphic Encryption (HE) is a type of encryption which allows computations to be done on ciphertexts, which generates a result in encrypted form. When that result is decrypted it match the result of operations which had been performed on the original plaintext. The main basic functionality of homomorphic encryption is that it allows computations and calculations to be performed on the encrypted form of data. It is used for securing many different services without exposing their sensitive content. With the use of homomorphic encryption now-a-days voting systems are being made secure, it provides hash functioning: collision-resistant, even private data of individual can be retrieved. If we talk in the terms of malleability, homomorphic schemes are considered to have a bit weaker security property as compared to non-homomorphic schemes.

A cryptosystem is a system which contains a set of cryptographic algorithms which target to protect the confidentiality of user and hence securing the service. It mainly consists of three algorithms: first for key generation, second for encryption and third for decryption. Fully homomorphic encryption (FHE) system is a cryptosystem which supports random computation on the ciphertext and is the far more powerful than other schemes of encryption. It enables construction of codes for a particular functionality, it can run on any of the provided encrypted inputs to generate a result. It does not need to decrypt its inputs, thus making it impossible for an untrusted party to know about the inputs and internal state of text. Cloud the latest hype word, works on the functionality of fully homomorphic encryption. Many computations are performed using FHE techniques in securing the cloud. According to the definition given by National of Standards and Technology (NIST), "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider". The 5 essentials characteristics of cloud computing are given as on demand self-service, greater network access, pooling of resources, rapid elasticity and measured service [1].

In this paper we will discuss about the various homomorphic encryption techniques and how these techniques are helping keeping the cloud storage system safe. The aim will be to analyze the pros and cons of different schemes in order to preserve the confidentiality of data storage. The rest of the paper is described as follows: Section II tells about the literature review; Section III gives techniques of homomorphic encryption.

II. LITERATURE REVIEW

Homomorphic encryption technique is used by various researcher in order to secure the cloud, learn more about the existing schemes of encryption, designing of algorithms, construction of safe models etc. Basically, it is the area of interest as homomorphic encryption is being widely used in the fields of finance and medicine. In 2011, there was a news that the network of Sony's play station was hacked and more than billions of personal data was leaked as it was uncrypted. This is like one of the incidences that took place but there are many such events take place much more rapidly. An individual's private data is stolen hence hampering the privacy of a person. Such outsourcing has become common so HE techniques are being used so that cloud store can be made much more secure than it is currently.

Maya Louk and Hyotaek Lim talked about the implementation and assessment of homomorphic encryption in mobile and multi cloud computing environment. Maya Mohan et al took a survey on various HE techniques on the categories involved like security considerations, encryption – decryption mechanisms, hammerphic properties etc. the techniques with best properties were considered much suitable for applications that are based on data privacy and security.

Manuscript published on 30 August 2019.
***** Correspondence Author (s)
Dakshita Sharma, Department of Information Technology, Amity University, Sector – 125, Noida, Uttar Pradesh, India.
Dr. Purushottam Sharma, Department of Information Technology, Amity University, Sector – 125, Noida, Uttar Pradesh, India.
Mr. Vikas Deep, Department of Information Technology, Amity University, Sector – 125, Noida, Uttar Pradesh, India.

Baohua Chen and Na Zhao talked about principles of homomorphic encryption, analyzed its scheme and improved its algorithm which being used in cloud computing. Dalia Tourky firstly discussed about the concepts of homomorphic encryption and used its complicated algorithms from the starting spark of algebraical methods.
Jing-Li Han et al proposed a new notion of secure searchable encryption scheme. They used multikey fully homomorphic encryption (MFHE) scheme that is capable of operating under multiple unrelated keys. Their scheme can make servers eavesdropping user's personal data and I return can target according to the query which has been requested. The scheme ensures the security and privacy, and not too much to reduce the query efficiency [6]. Rahal Romadi et al concentrated on distributed computing and its appropriation in various area to portray the job of HE plots for safeguarding security information partaking in the cloud and propose a framework that guarantees privacy of information utilizing halfway HE calculations [7]. Marek R. Ogiela and Marcin Oczko showed general concepts, likelihoods and restrictions of HE and compared two cryptosystems in an accesile way. They constructed a homomorphic circuit and analyzed it in broad aspect. Yong Ding and Xiumin Li structured a plan dependent on technique utilizing completely homomorphic encryption which bolster for multi-client registering and sharing of ciphertext, fine grained access control and realized that one doesn't have to remain web based amid the key repudiation, it decreases the effect on related clients' legitimate unscrambling, at long last a given ciphertext recovery conspire in an understanding with the encryption calculation is created. The very first implementation of homomorphic encryption scheme was done by Gentry and Halevi. They reported the timing of 30 minutes per bit basic operation. They were able to evaluate 54 different input in 36 hours.

III. CLASSIFICATION OF HE TECHNIQUES

A homomorphic encryption plot is effective if and just if the measure of ciphertext is polynomial limited as for the security parameter when rehashed calculations are finished. Fundamentally, the homomorphic encryption plot has a place with any of the principle three classifications i.e.:

- **Fully Homomorphic Encryption:** It allows any number of operations of multiplications and additions to be completed on the encrypted data. The circuit in this design is evaluated homomorphically. It is considered perfectly suitable for any kind of application that is waging with encrypted data. It is a bit less efficient as compared to other techniques because of additional computational overhead.
- **Partially Homomorphic Encryption:** It allows either one of the operations from addition or multiplication to be achieved on the encrypted data. But does not allow both operations. This idea is useful for claims which require some precise computation to be performed. Helios Voting scheme uses PHE to count the number of votes without disclosing the third party.
- **Somewhat Homomorphic Encryption:** It allows more than one action to be performed on encrypted data but in limited way. Not all operations can be done on all the types of data. This scheme is suitable for applications in which real time analysis of data is done. In it their limited operations and hence it is considered faster than other schemes.

There are other categories also like additive, multiplicative, algebraic homomorphic encryption which allows only that particular operation to be achieved on the coded data. Like additive homomorphic encryption only adds the encrypted data and so with other categories.

IV. VARIOUS HOMOMORPHIC ENCRYPTION SCHEMES

In general, homomorphic encryption consist of 3 steps:

- **Key generation –** It consist of private and public key used for encryption and decryption.
- **Encryption –** It involves a plaintext and a public key as an input to convert it into a ciphertext.
- **Decryption –** It involves a ciphertext and a private key to get the output as the plaintext.
- **Evaluation –** It requires a function, public key and a ciphertext which performs homomorphic encryption on the ciphertext.

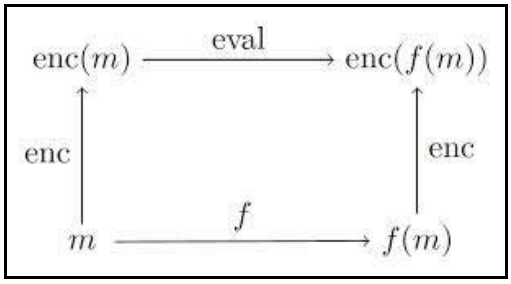

Figure 1: Evaluation using, HE

Figure 1 illustrates that how message is being encrypted using homomorphic scheme. A function is being applied to a ciphertext.

A. RSA Encryption Scheme

The RSA Encryption Scheme uses the property of multiplication homomorphism. The basic RSA is not much secure as it does not randomize the value and making it easier for the attacker. They can use a number of inputs and can easily observe the outputs. As the output they get to know about the key.

Key Generation: 1. Choose two prime numbers p and q. 2. Analyze n = p * q 3. Compute modulus of n so that it is equal to n.
Encryption: $c = m^e \pmod n$
Decryption: $c^d = (m^e)^d = m \pmod n$

B. EIGamal Encryption Scheme

This scheme was introduced in 1985 and it also uses multiplicative homomorphism. It generates a cyclic group G, of order q. It provides more security as asymmetric private keys are used to encrypt symmetric messages.

Key Generation: 1. Choose a number (x) randomly from q-1. 2. Calculate g^x. 3. G, q, g are public key and x is private key.
Encryption: 1. Choose a number (y) from q-1. 2. $C_1 = g^y$ and $C_2 = m'.s$ 3. $(C_1, C_2) = (g^{y,} m'.g^{xy})$
Decryption: $C_2 s^{-1} = m'.h^y . (g^{xy})^{-1}$

C. Goldwasser Micali Scheme

It was developed in 1982 and it was first public key generation scheme which worked on probabilistic method and uses standard cryptographic assumptions. It was not much efficient as a ciphertext can be generated more than the size of plaintext.

Key Generation: 1. Choose two prime numbers p and q. 2. Calculate n = p * q 3. Generate x such that (x/p) = (x/q) = -1. 4. x, n are public key and p, q are private keys.
Encryption: 1. Generate a random value y_i such that gcd(y_i, n) = 1. 2. $C_i = y_i^2 x^{m_i}$
Decryption: 1. To decrypt the text for each value of i factorization of p and q is done.

D. Benaloh Encryption Scheme

It is the extended version of Goldwasser Micali Encryption Scheme. It was created in 1994 and the main advantage was that it can take larger chunk of data to encrypt the plaintext while the former scheme uses to tale data by a bit.

Key Generation: 1. Select 2 larger prime numbers p and q such that r(p-1), gcd (r, (p-1)(r)) = 1 2. Calculate n = pq
Encryption: 1. Choose a arbitrary number u. 2. Calculate $E_r(m) = y^m u^r \bmod n$.
Decryption: 1. Compute $a = c^r \bmod n$ 2. The output will be such that $x^m = a$.

E. Paillier Encryption Scheme

It uses probabilistic based approach of encryption which was developed in 1999. There was a problem of calculating residue for large values of n. It uses additive property of homomorphism, we have two keys k_1 and k_2 and we get $k_1 + k_2$.

Key Generation: 1. Select two large prime numbers such that gcd = (pq, (p-1)(q-1)) 2. Calculate n = pg and z = lcm((p-1)(q-1)). 3. By using modular multiplicative inverse we get a = $(l(g^2 \bmod n^2))^{-1} \bmod n$. 4. Public key is n, g and private key is z, a.
Encryption: $C = g^m r^n \bmod n^2$
Decryption: $M = l(c^z \bmod n^2) . z \bmod n$.

F. Gentry's Encryption Scheme

It was the first Fully Homomorphic Encryption (FHE) technique developed by Craig Gentry in the era of 2009. He developed a sort of re-encryption technique to get fully homomorphic text. He worked on the noise parameter attached with ciphertext. A threshold value was set, once the noise value reaches post the threshold value it starts re-coding the already encoded data. He used the technique of bootstrapping to re-encrypt the encrypted data. The generation of key in this methodology takes place by Smart Vercauteren method.

G. Zaryab Khan's Encryption Scheme

It is also fully homomorphic encryption scheme which is considered perfect for colorblind functions. It is one of the fastest scheme for encryption as it does involve any dull parameter. Here both homomorphic addition and multiplication is performed to get the public and private key. It is considered less expensive than Gentry's scheme beacsuse it does not use the concept of ideal lattices which are very expensive.

V. ADVANTAGES AND DISADVANTAGES

Advantages-

- It is approach which enhances privacy in the following sub-systems:
  - Cloud Computing
  - Bank Transactions
  - Voting Computations
- It helps in easy retrieval of private information of user.

Disadvantages-

- It is a complex approach as it involves formation of different ideal lattices.
- It is very prone to malware attacks once the is disclosed.

There are certain performance issues as sometimes the algorithm becomes infeasible to approach..

VI. APPLICATIONS OF HOMOMORPHIC ENCRYPTION

- **Geonomics** – Clinical sequence of genetic variants can be understood in detail using data sharing approach.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

- **National Security** – Smart grid network can be developed for nuclear/critical sites.
- **Education** – Discrimination of students can be prevented from schools and colleges.
- **Healthcare** – It can be used to balance the risk and utility of health-related sharing of data.
- **Control System** – To protect the data of sensing systems so that only authorized person can use it.
- **Finance** – The money related transactions are most crucial it can be protected using HE.

VII. FUTURE SCOPE

In this paper we discussed about what is homomorphic encryption and its types. Further the techniques used in encryption process were discussed. Basically, it was a comparative study of different techniques.
My future work would be to implement these techniques on some plaintext. Comparison of the techniques will be done on the basis of which technique gives the best output within less amount of time. The target will be to find an efficient technique. There can be modification in the techniques if the complexity of the algorithm will be decreased.

VIII. CONCLUSION

A detailed glimpse is given on the topics linked with homomorphic encryption. The types and techniques of the former are discussed to get a clear concept on the scheme. Discussions are done on the safekeeping and proficiency aspect of the scheme. The main task of homomorphic encryption is to protect the privacy of users and how that privacy is protected is shown in the various mentioned techniques. It would be useful to work on the techniques and generate efficient results.

REFERENCES

1. Joshi, R. H., Rathi, D. P., Khan, A., & Jain, M. (2018). A Survey on Various Security Issues and Challenges to Secure Cloud Computing.
2. Mollah, M. B., Azad, M. A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications, 84, 38-54.
3. Aldossary, S., & Allen, W. (2016). Data security, privacy, availability and integrity in cloud computing: issues and current solutions. International Journal of Advanced Computer Science and Applications, 7(4), 485-498.
4. Wadiwala, K. K., & Patel, H. N. (2018). Homomorphic Encryption Property Algorithms. Journal of Embedded System & Applications, 5(3), 7-11.
5. Jabbar, I., & Najim, S. (2016). Using fully homomorphic encryption to secure cloud computing. Internet of Things and Cloud Computing, 4(2), 13-18.
6. Floriano, E., Alchieri, E., Aranha, D. F., & Solis, P. (2017). Providing privacy on the tuple space model. Journal of Internet Services and Applications, 8(1), 19.
7. Liu, J., Han, J. L., & Wang, Z. L. (2016, July). Searchable Encryption Scheme on the Cloud via Fully Homomorphic Encryption. In Instrumentation & Measurement, Computer, Communication and Control (IMCCC), 2016 Sixth International Conference on (pp. 108-111). IEEE.
8. Bensitel, Y., & Romadi, R. (2016, May). Secure data storage in the cloud with homomorphic encryption. In Cloud Computing Technologies and Applications (CloudTech), 2016 2nd International Conference on (pp. 1-6). IEEE.
9. Ogiela, M. R., & Oczko, M. (2018, May). Comparison of Selected Homomorphic Encryption Techniques. In 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA) (pp. 1110-1114). IEEE.
10. Ding, Y., & Li, X. (2017, July). Policy Based on Homomorphic Encryption and Retrieval Scheme in Cloud Computing. In Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on (Vol. 1, pp. 568-571). IEEE.