Scrutinizing the Progress of Homomorphic Encryption Scheme in Guaranteeing Data Privacy

Liz George
Dept. of Computer Applications,
St. Joseph's College of Engineering & Technology,
Kottayam, India

Dr. Jubilant JKizhakkethottam
Dept. of Computer Science & Engineering,
Saintgits College of Engineering & Technology,
Kottayam, India

Abstract:- The privacy and security of data is always a major concern in the current era of big data and cloud computing. Storing the data in encrypted form was the approach followed to overcome this problem. Homomorphic Encryption evolved as a technique to perform operations on encrypted data, providing the same results on working on raw data. It eliminates the access of decrypted data by third party (cloud service providers) for performing computation. Since its inception in 1978, there occurred many contributions and enhancements in this area. The main breakthrough was Fully Homomorphic encryption scheme proposed by Craig Gentry in 2009. This paper discuss about the classification of homomorphic Encryption Schemes as PHE,SWHE ,FHE and the additive and multiplicative operations and about various schemes that have been proposed from time to time in view of decreasing the computational cost involved and to widen the range of applications/domains which implements HE. Various practical implementations of Homomorphic encryption scheme are also discussed.

Keywords:- *Homomorphic Encryption, Cloud Storage, Privacy, Security.*

I. INTRODUCTION

With the advent of numerous applications and automation of many traditional systems, there is remarkable increase in the amount digital data available, which needs to be stored without compromising the privacy of the data. Many organizations are relying on Cloud Service Providers for their data storage due to its affordable cost and low maintenance. The data is stored in cloud in encrypted form to retain privacy. To perform computations and analysis, CPS has to decrypt the data, resulting in the violation of the organizations data privacy policy.

Privacy-enhancing Technologiesarea key research area in the current scenario. Homomorphic Encryption provides a promising solution in this regard [1]. It allows to perform computations on encrypted data, without compromising its privacy. It can play a significant role in computation and analysis of data in domains like healthcare and finance, where the need to assure privacy is paramount.

II. WHAT IS HOMOMORPHIC ENCRYPTION?

Homomorphic Encryption is an asymmetric encryption technique with a pair of keys, where encryption is done using a public key which can decrypted only using the corresponding private key. It makes use of an algebraic system, allowing to perform functions on the encrypted data. The holder of the private key alone can access the unencrypted data after the computation, allowing data to remain secure and private while it is used by someone else. One of the key features that distinguishes it from other encryption models is its resistance to quantum attack.

III. HOMOMORPHIC ENCRYPTION: CLASSIFICATION AND OPERATIONS

There multiple types of encryption schemes associated with Homomorphic encryption, which performs diverse computations on cipher text. [2]

3.1 Classification

There are three variants of homomorphic encryption:

Partially homomorphic encryption allows performing single operation either addition or multiplication 'n' number of times on encrypted data

Somewhat homomorphic encryption allows performing different operations(addition and subtraction)but only limited number of times.

Fully homomorphic encryptioncombines the advantage of partially homomorphic encryption with somewhat homomorphic encryption, which allows to perform unlimited amount of operation for unlimitednumber of times

3.2 Operations

Homomorphic Encryption performs operations on encrypted data .The secret key for decryption is with the client alone. After decryption, the result obtained is the same as if the computation on Plain text.

Additive operation

Encryption functionE is additively Homomorphic if

$E(m1 + m2) = E(m1) + E(m2)\ \forall m1,m2 \in M$,without revealing m1 or m2.

where M is the set of all messages

Multiplicative operation

Encryption function E is multiplicatively Homomorphic Encryption if

$E(m1 * m2) = E(m1) * E(m2)\ \forall m1,m2 \in M$, without revealing m1 or m2

where M is the set of all message

IV. HISTORY OF HOMOMORPHIC ENCRYPTION

The phrase homomorphic is derived from Greek words 'homos', which means 'the same' and 'morphe' with meaning 'shape'. The major limitation of systems using encryption schemes are they can be used only for storing and retrieving encrypted data. Performing computations on data needs the decryption of data, which affects data security. The concept of Homomorphic Encryption was first proposed with the name "private Homomorphism' in 1978 by Rivets, Ronald L., Len Ad leman, and Michael L. Dertouzos[3], after the RSA encryption. But little progress was made on developing such a system for the next 30 years.

4.1 Different Homomorphic Schemes

Several cryptosystems based private homomorphism were proposed. But most of them were either additively or multiplicatively homomorphic. A few which were fully homomorphic, but had the limitation that ciphertext size grows with the number of operations[4]. An additive Homomorphic encryption, which can encrypt only a single bit was proposed by ShafiGoldwasser et al.[5]

Additive-Multiplicative Homomorphism was proposed[6], which guarantees that the result obtained after performing computation on two encrypted values is equivalent to the result found by encrypting the value obtained after performing computation on two unencrypted values. The main drawbacks were, absence of single system which was additively and multiplicatively homomorphic and lack of functions which had compatibility with HE.

In 1999, Paul Paillier[7] proposed a partial fully homomorphic encryption scheme which allows addition of two cipher texts and multiplication of a ciphertext by a plaintext number. In 2005, a homomorphic scheme devised by Boneh, Goh, and Nissim allowed both additions and multiplications using a ciphertext with constant-size. However, only one multiplication is permitted, making the system somewhat homomorphic[8].

The emergence of cloud computing technology in early 2000 triggered the attention back on Homomorphic Encryption[9]. In 2009 Craig Gentry's thesis[10] on fully homomorphic encryption, provided a basic outline for achieving fully homomorphic encryption. It was a major breakthrough for researchers who were relentlessly working for a solution to growing attacks on data privacy. He describes it as a glovebox where everyone can get their hands into the glovebox and handle what's inside, but nothing can be taken out of the glovebox. The raw materials inside the glovebox can be accessed by all and they can build inside the box. But only the person with key alone can retrieve the newly built product. But the main limitations of this work were the noise is attached with cipher text and increases in each operation. In 2010, Smart and Vercauteren generated an encryption scheme with smaller ciphertext and key as an extension of Gentry's original scheme [11] without sacrificing the security. The main motivation behind this scheme was conceptual simplicity.

The homomorphic cryptosystems which are popular now is based on the scheme put forward by ZvikaBrakerski et al.[12].The encryption schemes introduced after this are known as second-generation FHE schemes, where growth in the noise during the homomorphic computation is slower.

The main highlight of homomorphic encryption is the ultimate data privacy it offers, since computations can be performed within ciphertext, eliminating the burden of decryption. In the era of Internet, where, everything's public: our browsing information, location, inclinations etc. the complete data privacy offered by homomorphic encryption has broad applications, especially in fields like Health care and Finance.

V. APPLICATIONS

The first and foremost application of Homomorphic encryption can be identified as the secure computation on data stored in cloud environment [13]. It ensures data privacy by allowing the cloud provider to perform computation on encrypted data.The IoT technology implementation in healthcare has reformed personal health care by enabling remote monitoring of terminally ill patients using sensors attached to them [14]. One of the important advantages of cloud computing is the effective storage space it can provide for health records and the data provided by sensors , that can be shared with healthcare providers and researchers making the medical research more effective. Meanwhile, using appropriate homomorphic encryption schemes, authorized entities can retrieve relevant information from the encrypted health records eliminating the concern of data privacy. [15]

Use of Genome sequences plays a significant role in the study of complex diseases or epidemiology. But the broad sharing of these data always raises threat as DNA sequences are biometric identifiers, similar to finger prints. Any leakage of these information into wrong hands will have wide destructive impacts and it will be the utmost violation of the identity privacy.Homomorphic encryption schemescan be incorporated, ensuring the security of different genomic datasets uploaded to the cloud and they can be effectively shared for studies to provide precision medicine and thus improving the health and wellbeing of patients [16].

By combining the properties of Blockchain technology and Homomorphic encryption concepts, it is possible to create an efficient e-Voting system which is public and transparent, meanwhile protecting the identity of voters [17]. Using signature homomorphism scheme in Electronic voting system can effectively manage the workload involved in verification that occurs with the increase in the voters or contenders. [18] It also ensures privacy of voters and security of voting.

Watermarks are used to show the identity of its owner, thereby ensuring the copyright.Finger printing is another scheme that prevents illegal copying of digital data. It helps to trace the source of an illegal redistribution, thus allowing copyright holder to take legal action.Homomorphic Encryption can be effectively used in digital watermarks and fingerprinting schemes, allowing to add a mark in to an encrypted document [19].

Homomorphic Encryption is capable of ensuring the security of sensitive data in financial sector. This may vary from sensitive information pertaining to companies like Intellectual Property and trade secrets to the personal information of individuals. The capacity of homomorphic encryption to perform computation on encrypted data allows to perform, secure search, analytics and collaboration of sensitive data and assets. [20]

VI. CONCLUSION

Homomorphic encryption had come great far ever since its launch in 1978. Different HE schemes have evolved based on application and security requirements. The biggest barrier that restricts the popularity of homomorphic encryption is its lack of speed due to the large computational overhead involved. The lattice-based cryptosystem implemented in fully homomorphic encryption is sophisticated. Performing even basic operations need massive computations and large cipher size.[21] Approaches for tuning the system to improve efficiency may result in compromising the security of the system. The high cost involved in reducing the noise in Fully Homomorphic Encryption Schemes is a major apprehension. Even though, Fully Homomorphic encryption schemes proposed can play a significant role in enhancing the privacy of various applications, the efficient and cost effective practical implementation of such systems in numerous platforms are yet to be evolved.Introduction of FHE inculcated hope to solve other long waiting problems(applications) such as Functional Encryption (FE),Identity-based encryption (IBE) and Attribute-base d encryption[22].

REFERENCES

[1] S. E. H. E. G. Maha Tebaa, "Homomorphic encryption method applied to Cloud Computing," *2012 National Days of Network Security and Systems*, 2012.

[2] C. B. C. C. G. A. J. Frederik Armknecht, "A Guide to Fully Homomorphic Encryption," 2011.

[3] L. A. M. L. D. Ronald L. Rivest, "On data banks and privacy homomorphisms," in *foundations of secure computation*, 1978.

[4] D. M. Freeman, "Homomorphic Encryption and the BGN Cryptosystem," 2011.

[5] S. M. Shafi Goldwasser, "PrProbabilistic encryption and how to play mental poker keeping secret all partial information," in *proceedings of the14th Annual ACM Symposium on Theory of Computing,*, 1982.

[6] C. F. T. Tomas Sander, " Protecting Mobile Agents Against Malicious Hosts," *Mobile Agent Security*, pp. 44-60, 1998.

[7] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," *Advances in cryptology*, pp. 223-238, 1999.

[8] E.-J. G. N. Dan Boneh, "Evaluating 2-DNF formulas on ciphertexts," in *Theory of cryptography* , 2005.

[9] L. X. W. B. Zhang Shaomin, "Study on the Protection Method of Data Privacy Based on Cloud Storage," *International Journal of Information and Computer Science*, pp. 46-51, 2012.

[10] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," in *Proceedings of the forty-first annual ACM symposium*, 2009.

[11] F. V. N.P. Smart, "Practice and Theory in Public Key Cryptography," 2010.

[12] Z. B. a. C. G. Vaikuntanathan, "Fully Homomorphic Encryption without Bootstrapping," in *International Conference on Information Technology Convergence and Services*, 2012.

[13] H. L. Maya Louk, "Homomorphic encryption in mobile multi cloud computing," in *International Conference on Information Networking*, 2015.

[14] D. R. K. Anjali S. Yeole, "Use of Internet of Things (IoT) in Healthcare: A Survey," in *Proceedings of the ACM Symposium on Women in Research* , 2016.

[15] T. S. Övünç Kocabaş, "Medical data analytics in the cloud using homomorphic encryption," *E-Health and Telemedicine: Concepts, Methodologies, Tools, and Applications* , 2016.

[16] A. G. Y. P. S. G. Marcelo Blatt, "Secure large-scale genome-wide association studies using homomorphic encryption," *Proceedings of the National Academy of Sciences of the United States of America*, 2020.

[17] R. T.-M. C. M.-E. W. Jen-Ho Hsiao, "Decentralized E-Voting Systems Based on the Blockchain Technology," in *International Conference on Ubiquitous Information Technologies and Applications* , 2017.

[18] T. W. Q. Z. C. A. X. Xingyue Fan, "HSE-Voting: A secure high-efficiency electronic voting scheme based on homomorphic signcryption," *Future Generation Computer Systems,* vol. 111, pp. 754-762, 2020.

[19] D. P. T. S. S. R. N. S. G. Dinesh Kumar, "An Efficient Watermarking Technique for Biometric Images," in *7th International Conference On Advances In Computing & Communication*, 2017.

[20] M. N. a. V. V. Kristin Lauter, "Can Homomorphic Encryption be Practical," in *Proceedings of the 3rd ACM workshop on Cloud computing security workshop*, 2011.

[21] L. Morris, "Analysis of Partially and Fully Homomorphic Encryption," 2013.

[22] H. A. A. S. U. ABBAS ACAR, "A Survey on Homomorphic Encryption Schemes: Theory and Implementation".