ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 12, pp.76377-76379, December, 2018
DOI: https://doi.org/10.24941/ijcr.33584.12.2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

REVIEW ON USAGE OF HOMOMORPHIC ENCRYPTION TECHNIQUE

***Devyani S. Dhokey and A. V. Deorankar**

Department of Computer Science and Engineering, Government College of Engineering, Amravati, Amravati, India

ARTICLE INFO

Article History:
Received 20th September, 2018
Received in revised form
10th October, 2018
Accepted 19th November, 2018
Published online 31st December, 2018

Key Words:
Homomorphic Encryption,
Healthcare Decision Support,
Privacy-Preserving, Data Security.

ABSTRACT

In healthcare industry, clinical decision support system plays an important role. As the clinical data is confidential data, there is a huge requirement of a secure data security system which can maintain secrecy of data. In this paper, we propose a homomorphic encryption technique which is able to perform the different operations on data by preserving the privacy of data. As, the data privacy is the primary concern. All the operations are performed on the encrypted data. An innovated homomorphic encryption algorithm which supports large integer, small integer as well as text data encryption will be designed. We will perform operations on encrypted data rather than decrypting it during processing. As our proposed algorithm includes large integer as well as text data, our system will be more efficient than existing system.

***Citation: Devyani S. Dhokey and A. V. Deorankar.* 2018.** "Review on Usage of Homomorphic Encryption Technique", *International Journal of Current Research*, 10, (12), 76377-76379.

INTRODUCTION

Security of the outsourced cloud data is an important area of research. The homomorphic encryption can make the outsourced cloud data secured. The homomorphic encryption scheme performs the calculation on the encrypted cloud data which makes the data security strong. Nowadays the bulk amount of data is produced there is increasing need of data security. Fully Homomorphic Encryption scheme is the vast area of research and development. The ideal Fully Homomorphic Encryption algorithm is not yet developed. Fully homomorphic encryption can be able to perform the random operation on the encrypted cloud data without decrypting the while performing calculation on the data, and will produce the encrypted result which is being send to the user. Here, Fully homomorphic encryption technique is designed. The outsourced arithmetic and searching operations can be achieved by constructing secure platform for both single key and multiple key setting. Fully homomorphic encryption will be able to overcome the scurity limitations of cloud computing by directly performing computations on encrypted ciphertext data. FHE technique can make multiparties to share there data without any trust. Fully homomorphic encryption will enable highly secure application. In this paper, we are going to describe the method of designing the fully homomorphic encryption technique for security of outsourced cloud data.

Fully Homomorphic Encryption Technique is designed for integer as well as text data with efficiency and high performance. Fully homomorphic encryption (FHE) is a form of encryption where we will be able to do computations on the decrypted form of cipher-texts without performing decryption on those cipher-texts. As a result, an encrypted form of the result of those computations is generated. However, Searchable encryption is a form of encryption where you can search for cipher-texts whose decryption satisfying some condition without decrypting those cipher-texts and looking at the decryption. A collection of cipher-texts has been given in the end result. A fully homomorphic encryption technique will be used to perform the various mathematical operations on the integer data. Since, the efficient fully homomorphic encryption technique not yet designed. So there is a huge scope in developing an innovated homomorphic encryption technique which is able to perform the computations on large integer as well as search on text data. Cloud computing will bulk amount of data generated in day-to-day life in various sectors viz. healthcare industry, revenue department, crime branch, food industries, educational area, etc. Many of the industrial sectors use the cloud storage as an option to store the data securely by keeping the data with third party. Third party uses various encryption techniques such as searchable encryption, homomorphic encryption, etc. The homomorphic encryption technique reduces the chances of data leakage as the computations are performed on the encrypted cipher-texts. A fully homomorphic encryption have the capabilities to perform the high level computations on the data.

Corresponding author: **Devyani S. Dhokey,**
Department of Computer Science and Engineering, Government College of Engineering, Amravati, Amravati, India.

The searchable encryption is used to perform the secure search operation on the encrypted data. A fully homomorphic encryption with some important capabilities are- highly secured data storage, secure data processing can be done on-the-fly, computations acomplished with no involvement of additional servers, easy for use. The advantage of this fully homomorphic encryption technique over existing homomorphic technique is that it can work on large integer data as well as floating point data efficiently. The operations performed on text data also.

Literature review: The Leveled Fully Homomorphic Encryption without bootstrapping technique is described in (Brakerski, 2012). Bootstrapping increases the computation overhead as it involves the encryption of each bit of the plaintext is replaced by large cipher-text. Hence, here the encryption algorithm involves the ring-LWE scheme. Homomorphic encryption for AES circuit computation is described in (Gentry, 2012). Why AES chose because it is widely used in security based applications (AES with 128-bit key size). Various operations of AES circuit can be calculated homomorphically. This system is based on the BGV-Scheme where the basics of practical implementation of homomorphic encryption are mentioned. Here, the various optimizations such that it might be used for calculating other circuits. The comparative study of homomorphic encryption technique with and without bootstrapping is explained. The polynomial ring is used for calculating AES circuit. The *et al*. (2016), (Liu *et al*., 2016) state an efficient way of performing computation on the outsourced data using multiple keys. Large number of users can effectively outsource their data on the cloud without compromising security of the individual user's data as well as the final computed result. The platform is designed in a way that the different users will be able to post their data securely using own public key. Use of multiple keys can make it more secure. The PCOR (Liu *et al*., 2016) can be able to perform the computations on the rational numbers. The operations can be done on-the-fly. An effective technique is introduced in (Alhassan Khedr and Glenn Gulak, 2018) for sharing the medical records among medical representative throughout the world. Here, the advanced NTRU-based technique is developed on the basis of the homomorphic encryption scheme where there is small growth of noise with increasing size of data. A verifiable public key encryption algorithm is designed in multiuser setting (Wu *et al*., 2018). The server can be able to build an inverted index structure for key encryption to reduce the complexity. As security issues in outsourced data computation is a trending research topic. An innovative plan for outsourced database and query point is proposed in (Shankar, 2018). Here, to improve the system performance opposition based particle swarm optimization is used for encryption with Homomorphic Encryption scheme. The query is processed on encrypted data with the help of homomorphic keys for sharing the data over the platform. To preserve the security the optimization has been accomplished with homomorphic encryption. There are many feasible homomorphic encryption techniques are available but till now the key size has limited and restricted size. In (Kavita Aganya and Iti Sharma, 2018) the authors provide a scheme of homomorphic encryption which can able to handle the large message space by emphasizing some advancement in existing techniques. Here, they process the large message by encoding it as a coefficients of polynomial and then perform the encryption on encoded polynomial's coefficient. Nowadays there is much advancement in hacking techniques as well as there is huge number of types of attacks among them one of most common attack is known plaintext attack. By doing analysis over the different existing FHE techniques (Babenko *et al*., 2018), homomorphic encryption technique for known plaintext attack is proposed. The crypto-system is based on the Residue Number System (RNS). In this case, RNS increase the efficiency of HE technique by processing some of the operations in parallel as well as it helps in error correction. The main focus is here to maintain the secrecy of data storage. Both the cloud computing and big data environments have the huge scope of homomorphic encryption technique as they produces the bulk amount of data on daily basis. And the data security is the primary concern in both of the fields. Here, they proposed a symmetric FHE scheme based on association rule mining technique to preserve the data privacy (Baocang Wang *et al*., 2015). Cloud provide facility for storing large amount of data from different vendors (Ayantika Chatterjee and Indranil Sengupta, 2018). Cloud should provide the security for data at enterprise level to maintain secrecy of sensitive data. Arbitrary operations can be performed on the encrypted data by the usage of FHE technique.

An idea is proposed (Cheon, 2016) to preserve the privacy of the encrypted database. While performing the computations on the encrypted data, it maintains precaution for the exposure of confidential data to the unauthorised user. It explains the advantages of using FHE over the usage of multiple encryption algorithms to maintain the privacy policy. Here, the encryption is done for search and compute operation. The devised framework has used the primitive circuits for encryption. Clinical decision support system has been devised in (Ayantika Chatterjee and Indranil Sengupta, 2018) which help the clinical representative to take the critical decision. The decision has been taken by using naïve Bayesian Classifier. The patient's historical data can be protected by using an innovated method namely an additive homomorphic proxy aggregation scheme. Top-k retrieval method is used to mark out the top matching records. It terminates the client-server connection by message passing phenomenon. The issues related to instruction executions, loop handling, variable definition translation, conditional termination of method while working with encrypted data and controls. They highlight the challenges while handling the encrypted data translation of recursive codes to their counterparts. An idea of encrypted auxiliary stack has been devised with two methods viz., encrypted pop and encrypted push to handle the recursion of encrypted data (Ayantika Chatterjee and Indranil Sengupta, 2018). Use of multiple keys for outsourced multiparty computation is explained in (Peter, 2013). A novel technique is developed with the use of two non-colluding untrusted servers jointly perform the complex computation. Here, there is no user interaction is required to carry out the different computations on the encrypted data search the place. In that new thing you get the idea how it looks and map the location. They recommend an own travel sequence the system mined user's and routes travel. First choice giving own POI, cost, time and season and now recently study on not only POIs (point of interest) but also travel sequence, turn over famous and user's travel choice at the similar time (Brakerski, 2012).

PROPOSED METHODOLOGY

The proposed system provides a secure encryption technique to provide the security to outsourced data calculation. It mainly focused on the homomorphic encryption technique to securely perform the operation on the data which has been stored online storage. In proposed system we focus on user's data security and preserve the privacy of the data. An efficient homomorphic encryption technique has been devised to perform the calculation on large integer, floating point data as well as query evaluation on the text data. The data stored on the third party cloud and while performing the calculation on that data the encrypted data has been fetched from the storage. And then the operations has to be performed on the encrypted data itself.

Conclusion

Study of various existing homomorphic encryption techniques with variation has been done in this paper. This paper demonstrates the different uses of the homomorphic encryption technique while maintaining the security of the data. Efficiency and accuracy of variants of HE is observed and compared.

REFERENCES

Alhassan Khedr and Glenn Gulak, 2018. "SecureMed: Secure Medical Computation Using GPU-Accelerated Homomorphic Encryption Scheme," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 2, march.

Ayantika Chatterjee and Indranil Sengupta, "Translating Algorithms to handle Fully Homomorphic Encrypted Data on the Cloud," IEEE Transactions on Cloud Computing, Volume: 6, Issue: 1 , Jan.-March 1 2018.

Babenko, M., Chervyakov, N., Radchenko, G., Tchernykh, A., OA Navaux, P. Kucherov, N., Deryabin, M. and Viktor S. 2018. "Security Analysis of Homomorphic Encryption Scheme for Cloud Computing: Known-Plaintext Attack," 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 29 Jan-1 Feb.

Baocang Wang, Yu Zhan, and Zhili Zhang, 2015."Cryptanalysis of a Symmetric Fully Homomorphic Encryption Scheme," *Journal of Latex class files*, vol. 14, no. 8, august.

Baohua Chen, Na Zhao, 2014."Fully Homomorphic Encryption Application in Cloud Computing," 2014 11th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 19-21 Dec.

Brakerski, Z., Gentry, C. and Vaikuntanathan, V. 2012. "(leveled) fully homomorphic encryption without bootstrapping," in Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. ACM, pp. 309–325.

Cheon, J. H., Kim, M. and Kim, M. 2016. "Optimized search-and-compute circuits and their application to query evaluation on encrypted data," IEEE Transactions on *Information Forensics and Security*, vol. 11, no. 1, pp. 188–199.

Cyrielle Feron, Vianney Lapotre, and Loic Lagadec, 2018. "Fast Evaluation of Homomorphic Encryption Schemes based on Ring-LWE," IEEE

Gentry, C., Halevi, S. and Smart, N. P. 2012. "Homomorphic evaluation of the aes circuit," in Advances in Cryptology–CRYPTO 2012. Springer, pp. 850–867.

Jian Liu and Jing-Li Han Zhao-Li Wang, 2016. "Searchable Encryption Scheme on the Cloud Via Fully Homomorphic Encryption," 2016 Sixth International Conference on Instrumentation and Measurement, Computer, Communication and Control, 21-23 July.

Kavita Aganya and Iti Sharma, 2018. "Symmetric Fully Homomorphic Encryption Scheme with Polynomials Operations," Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA).

Liu, X., Choo, K. R., Deng, R. H., Lu, R. and Weng, J. 2016. "Efficient and privacy-preserving outsourced calculation of rational numbers," IEEE Trans. Dependable and Secure Computing.

Liu, X., Deng, R. H., Choo, K. R. and Weng, J. 2016. "An efficient privacy preserving outsourced calculation toolkit with multiple keys," IEEE Trans. Information Forensics and Security, vol. 11, no. 11, pp. 2401–2414.

Liu, X., Lu, R., Ma, J., Chen, L. and Qin, B. 2016. "Privacy-preserving patient-centric clinical decision support system on naïve Bayesian classification," IEEE journal of biomedical and health informatics, vol. 20, no. 2, pp. 655–668.

Naehrig, M., Lauter, K. and Vaikuntanathan, V. 2011. "Can homomorphic encryption be practical?" in Proceedings of the 3rd ACM workshop on Cloud computing security workshop. ACM, pp. 113–124.

Peng Zhang, Xiaoqiang Sun, Ting Wang, Sizhu Gu, Jianping Yu, Weixin Xie, 2016. "An Accelerated Fully Homomorphic Encryption Scheme Over the Integers," 2016 4th International Conference on Cloud Computing and Intelligence Systems (CCIS), 17-19 Aug.

Peter, A., Tews, E. and Katzenbeisser, S. 2013. "Efficiently outsourcing multiparty computation under multiple keys," IEEE transactions on information forensics and security, vol. 8, no. 12, pp. 2046–2058.

Pramod Kumar Siddharth, Om Pal and Bashir Alam, 2016."A Homomorphic Encryption Scheme Over Integers Based on Carmichael's Theorem," 2016 International Conference on Electrical, Electronics, Communication, Computer and Optimization Techniques (ICEECCOT), 9-10 Dec.

Shankar, K.and Ilayaraja, M. 2018. "Secure Optimal *k*-NN on Encrypted Cloud Data using Homomorphic Encryption with Query Users," 2018 International Conference on Computer Communication and Informatics (*ICCCI* -2018), Jan. 04 – 06.

Wu, D. N., Gan, Q. Q. and Wang, X. M. 2018. "Verifiable Public Key Encryption With Keyword Search Based on Homomorphic Encryption in Multi-User Setting," IEEE Acess, August 20.

****