6th International Conference on Multidisciplinary Research (ICMR-2019)
Osmania University Campus, Hyderabad (India)
30th-31st May 2019 www.conferenceworld.in
Conference World
ISBN : 978-93-87793-89-7

Implementation of Fully Homomorphic Encryption Technique for Secure Outsourced Cloud Data Calculation

A. V. Deorankar[1], Devyani S. Dhokey[2]

[1]Department of Computer Science and Engineering,
Government College of Engineering, Amravati (India)
[2]Department of Computer Science and Engineering,
Government College of Engineering, Amravati (India)

ABSTRACT

The homomorphic encryption is an encryption technique which allow us to perform calculation on encrypted data and generate the result as a new resultant cipher-text. This paper explain and proposed design of a homomorphic technique without involving the design of complex integer circuit just by operating on the integer plain-text. In this scheme, double encryption has been performed to make the system more secure. Here, we are using the combination of cryptography algorithms such as, ceaser cipher, AES. We too design our own algorithms to operate with large integers, text data as well as floating point numbers. The proposed system is based on the theme of privacy-preserving outsourced calculation toolkit for cloud data (POCKIT) [1]. As homomorphic encryption has power, that it can perform random operation on the encrypted data. Our system has application in many areas where, there is sensitive data developed on daily basis like, medical, criminal records, etc. We proposed our system specially for medical system. The randomized key generation has been done to provide more security. Our system is more efficient, ease to use and developed, as well as reduced time overhead as compared with the existing system.

Keywords— Cloud, Homomorphic encryption, Medical data, Security.

I. INTRODUCTION

Medical is gradually growing industry as everyone became more aware and conscious regarding individuals health. On daily basis, the bulk amount of data has been generated in the medical field. The medical industry contributes 4.2 percent of India's GDP. As with increased industrialization and change in lifestyle, the pollution has been increasing which causes many health issues. Nearly 70% deaths and health issues are created due to pollution in India Close to 90% of worlds data is generated in the field of medical. As the medical data is personal and sensitive information of individuals which must be kept confidential. So there is obvious need of more secured encryption techniques to preserve the data from unauthorized hands.

The proposed system is designed to provide more security to data as it is based on homomorphic encryption. The fully homomorphic encryption is as powerful that it is capable to perform random operation on the encrypted data.

There are numerous homomorphic techniques are developed but none of them is fully homomorphic encryption (FHE). The FHE has vast area of research as its properties make us realize the 100% assurance of data security as all the operations are done on encrypted data without compromising data privacy. Anyone can use our medical information as a weapon to abuse us. So, it is most sensitive information used as a way to defame anyone. Hence, its our duty to keep it private and confidential.

The cryptography has number of encryption techniques. The AES is most common technique used to encrypt data, as it provide the large key space which makes it more secure. AES has block size of 128 bit with 3 variation in key size (128, 192 and 256). It has cryptographic primitives like confusion and diffusion with open standard of design. Anyone can make modification in AES algorithm. Till now, AES paired with RSA is most powerful encryption technique providing symmetric encryption.

Is Fully Homomorphic Encryption design possible in real time/ practicality? Almost the question is till now has big predicament in itself. As it is always not same conditions, situations under which we are going to perform random operations on encrypted data. So, obviously it becomes unpredictable that designing FHE is possible or not. There are many problems occur in while development of FHE, as its might not possible to guess what a human can query? Therefore, even though many of the theories has proven its practical development but no one has succeed in achieving FHE technique.

This paper compare the existing system and try to overcome the problem with it. The Pockit is able to perform addition, subtraction along with division and multiplication on signed/ unsigned integers but inconvenient while working with large integer. The proposed system may not using ring or polynomial as a message space but is able to work on large integers with less time of execution.

Contents of this paper is mainly structured into five section (chapters) as given below:The first section contains the basic introduction behind the development of the homomorphic encryption technique and problem definition with the motivation of the implementation of the idea is also explored. The section two is the literature survey on the various implementation methods and use of the homomorphic encryption technique. The section three contain the proposed system module with brief description over them. This also evolve the diagrammatic view of proposed system (include work flowcharts and DFD's). The fourth section is the comparative and experimental analysis of the proposed work with the existing work. It also showcase the performance analysis of the proposed system with the existing systems. The last section will gives us the final conclusion providing idea for future work scope and application areas of the system. This might helps the researchers to explore their ideas in this area of development.

II. LITERATURE REVIEW

The Leveled Fully Homomorphic Encryption without bootstrapping technique is described in [1]. 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 [2].Here, the various optimization's 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. [3][4] 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 PCOR [4] 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 [9] 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 multi-user setting [11]. 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 [12]. Here, to improve the system performance opposition based particle swarm optimization is used for encryption with Homomorphic Encryption scheme. There are many feasible homomorphic encryption techniques are available but till now the key size has limited and restricted size. In [13] 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.

By analysing over the different existing FHE techniques [14], homomorphic encryption technique for known plain-text attack is proposed. 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 [15].Cloud provide facility for storing large amount of data from different vendors [16]. 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 [5] 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 unauthorized 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 [16] which help the clinical representative to take the critical decision. 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 [16].

III. PROPOSED METHODOLOGY

FHE (Fully Homomorphic Encryption) technique to perform secure computation on outsourced cloud data is proposed. The proposed FHE is strong enough to perform the operations on encrypted data of type large integers as well as text. The proposed system uses the random integer generation algorithm to randomized the key of the user. Hence, it becomes more secure to perform the calculations on the outsourced cloud data. The proposed system has following modules: 1)Admin Panel, 2)Patient data management, 3)Data Searching, 4)Homomorphic Encryption, 5)Client side Data Decryption.

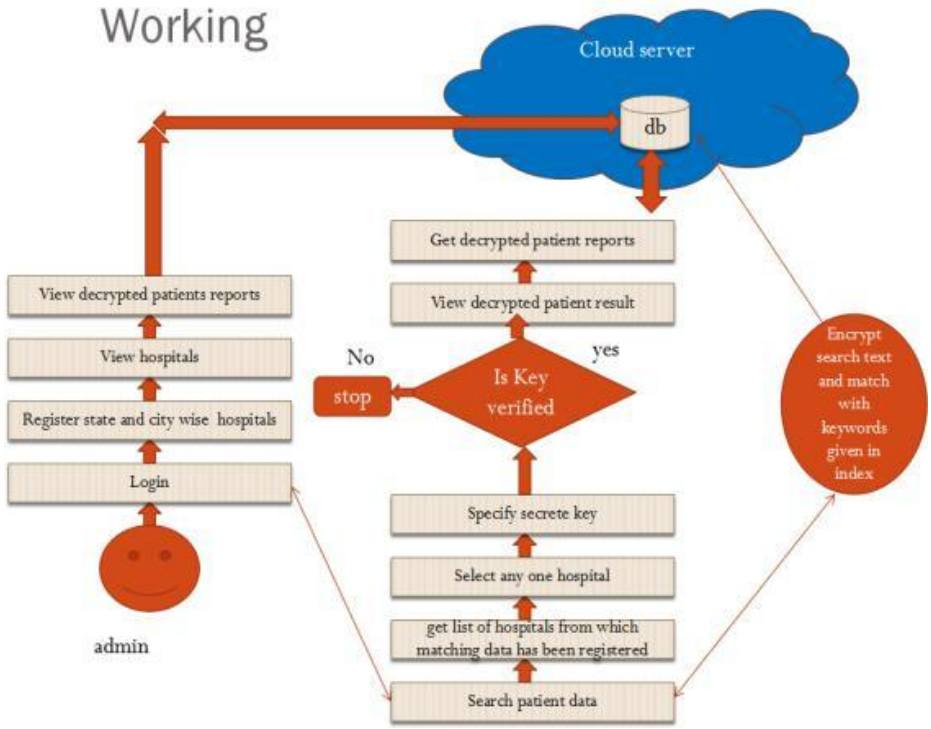

Figure 1 Flowchart of Proposed System

The figure1 shows the actual flow of the system in details. There are two admin users one at cloud and one at hospital to maintain the cloud and hospital respectively. The other users are patient, doctor and pathologist, etc. The cloud admin register itself at once. And after which city wise hospitals will register themselves to the system by sending a request to register. The hospital will get registered only after the confirmation of request by the cloud admin. Patients can register themselves with system by their own. The login credentials of users will be system auto-created as per user type. The cloud can view the user information except the login details of user to preserve privacy of data. The flow is as follows, after successful registration patient can login to system and can able take treatment from any of the respective registered hospitals. At the time of login the key of user has been generate for the first login and at further login the key has been fetched from database. Then, after fetching the key, the key is used to encrypt data of user and will store encrypted data on cloud. For more security and ease search, important keywords are add into an index table. At the time of searching any details regarding patient, the

ISBN : 978-93-87793-89-7

search query in encrypted format has been fired and list of the hospitals for which the searched data will matched with registered data. Among them select one of the hospital and specify secret key, if the key is verified successfully then the patients decrypted data will be shown to respective user else error of authenticity occurs. Cloud storage usage and payment all will be managed by cloud admin.

In our proposed system, we proposed the unique key management encryption mechanism based on the idea of homomorphic encryption. Here, we are going to maintain the single unique key for hospital and multiple keys for multiple users. The patient user will have single common key used on the platform of the proposed system. Along with this the proposed system is using a single server with no proxy server to perform operations. This will reduce the chances of data leakage and will maintain more security. The Homomorphic encryption devised is as given below:

Homomorphic Encryption algorithm
Register Clinical data
Set input=patient data
If k exist then
Fetch key from db if exist
Set k=key as per disease
Else
Set k=generate key randomly
End if
If isNumber(input) then
Encrypt input using numeric encryption algorithm Else
Encrypt input using text encryption algorithm End if

Here, we present some screen-shots of the proposed system as follows:

Figure 2 Home Page of Proposed System

ISBN : 978-93-87793-89-7

Figure 3.2 Admin Home

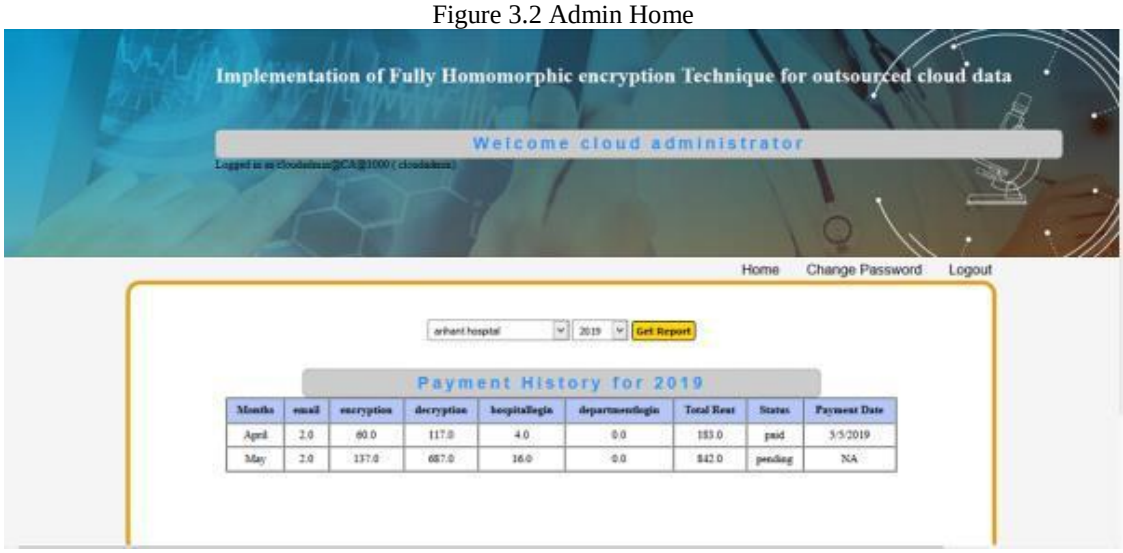

Figure 3.3 Cloud Payment Summary

Figure 3.4 Hospital Admin Home

Figure 3.5 Patient Registration Window

IV. PERFORMANCE ANALYSIS

This chapter deals with the experimental analysis of the proposed system. We provide the details regarding time required to perform encryption as well as decryption on data. Here, data considered of type integer, floating point along with text data. We present the required time in tabular format. Subsequently, we provide the evaluation in graphical representation as well.

Original No	Encrypted No	Decrypted No	Encryption Time (in Mili-Sec)	Decryption Time (in Mili-Sec)
4.5	71.6	4.5	0.06274533333333333	0.03553866666666667
81.2	157.1	81.2	0.5629171621621621	0.06195905405405406
0.0	8.0	0.0	0.0436906	0.03517753333333334
234.0	242.0	234.0	0.03995633333333334	0.013352333333333334
343.0	349.0	343.0	0.043369500000000005	0.019426
32.0	40.0	32.0	0.052405	0.01977733333333333
11.0	17.0	11.0	0.070174	0.032678
111.0	117.0	111.0	0.046079499999999995	0.020932
22322.0	22330.0	22322.0	0.039455	0.016565
5.5	15.6	5.5	0.11665566666666667	0.03724566666666667
23.0	33.0	23.0	0.053007	0.034033
12.0	24.0	12.0	0.036141	0.012349
22.0	34.0	22.0	0.037045	0.013252
222.0	234.0	222.0	0.053007	0.024546
212.0	224.0	212.0	0.039755	0.015661
12321.0	12331.0	12321.0	0.050297	0.021082
2132.0	2144.0	2132.0	0.042466	0.018974
555.0	565.0	555.0	0.05361	0.025901
666.0	678.0	666.0	0.050598	0.017167
7.0	17.0	7.0	0.04096	0.014456
888.0	900.0	888.0	0.043972	0.030118
9999.0	10009.0	9999.0	0.043671	0.027106
333.0	343.0	333.0	0.058127	0.03072

Table 4.1 Encryption Time Evaluation Table (Floating point number)

ISBN : 978-93-87793-89-7

Original No	Encrypted No	Decrypted No	Encryption Time (in Mili-Sec)	Decryption Time (in Mili-Sec)
110	118	110	0.001506	0.001606
100	108	100	0.0013555	0.016108499999999998
45	114	45	0.001205	0.054965
120	128	120	0.0013549999999999999	0.020028
67	77	67	0.001054	0.042767
180	192	180	0.001205	0.021685
90	102	90	0.0013555	0.0274065

Table 4.2 Integer Encryption Time Evaluation Table

Original Text	Encrypted Text	Decrypted Text	Encryption Time (in Mili-Sec)	Decryption Time (in Mili-Sec)	Original Text Length	Encryption Text Length
9898767654	6565434321	9898767654	0.3250985714285714	0.08549128571428573	10	10
MD	zq	MD	0.21799150000000003	0.050959	2	2
6yrs	3b%.	6yrs	0.20338014285714284	0.07710099999999999	4	4
19/7/1987	86m4m8654	19/7/1987	0.28026144444444445	0.125758	9	9
Female	srzmyr	Female	0.3156633	0.12182590000000001	6	6
nikita@D@1004	!vxv*neqe8771	nikita@D@1004	0.6457233333333333	0.4203423333333333	13	13
Nikita Joshi	!vxv*n w@.uv	Nikita Joshi	0.5185256666666668	0.19988133333333336	12	12
spiderprojects1@gmail.com	#\vqr%#%@wrp*.$etznvyip@z	spiderprojects1@gmail.com	0.6163362857142857	0.3915725714285715	25	25
mohanish@P@1005	fha$gblauiu8772	mohanish@P@1005	0.8082663	0.36863999999999997	15	15
Mohanish	fha$gbla	Mohanish	0.43906736842105265	0.19522568421052633	8	8

Table 4.3 Text Encryption Time Evaluation Table

V. CONCLUSIONS

We have proposed innovated Fully Homomorphic Encryption technique for outsourced cloud data. Only authenticated users can either access the data and can able to perform operations (evaluation or searching) on the data stored on to the cloud storage. Communication link between users and cloud is secured by devising Encryption and Decryption algorithms. As in existing system it involves the multiple complicated integer circuits and still inefficient while working with large integers. Hence, to overcome the problem of existing system our system has been proposed. Therefore, our system is more efficient and more secure than the existing system.

As the homomorphic encryption has large area of development and endless field to explore with modification to make system more efficient. The researchers can make move to develop the FHE with some more operations.

REFERENCES

[1] X. Liu, R. Deng, K.-K.R. Choo, Y. Yang, H. Pang, "Privacy-preserving outsourced calculation toolkit in the cloud", IEEE TDSC, 2018.

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

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

ISBN : 978-93-87793-89-7

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

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

[6] J. H. Cheon, M. Kim, and M. Kim, "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, 2016.

[7] X. Liu, R. Lu, J. Ma, L. Chen, and B. Qin, "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, 2016.

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

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

[10] Alhassan Khedr and Glenn Gulak, "SecureMed: Secure Medical Computation Using GPU-Accelerated Homomorphic Encryption Scheme," IEEE journal of biomedical and health informatics, vol. 22, no. 2, march 2018.

[11] Cyrielle FERON, Vianney LAPOTRE, and Loic LAGADEC, "Fast Evaluation of Homomorphic Encryption Schemes based on Ring-LWE," 2018 IEEE.

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

[13] K.Shankar and M. Ilayaraja, "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, 2018.

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

[15] M. Babenko, N. Chervyakov, G. Radchenko, A. Tchernykh, P. OA Navaux, N. Kucherov, M. Deryabin, and Viktor S., "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 2018.

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