Fully Homomorphic Encryption Technique for Secure Cloud Computing

Prof. A. V. Deorankar, Devyani S. Dhokey
Assistant Professor, PG Scholar
Department of Computer Science and Engineering
Government College Of Engineering, Amravati, India.

***Abstract* - In today's digital era, the data processing is digitalized. As the data has been processed and stored online, there is a obvious requirement of data security. The huge amount of data is generated in day-to-day life with respect to the increasing population. To protect the data, various cryptography techniques were developed. One of the popular encryption techniques is homomorphic encryption. Homomorphic encryption technique is the way in which all the operations are performed on the encrypted data itself. When the data will be stored on cloud there is chances of data leakage, so in this case the homomorphic encryption is most suitable technique to preserve the data security. Fully homomorphic encryption technique is the efficient way of performing random operations on data (text data as well as numerical data).**

Keywords: Cloud computing, Fully homomorphic encryption, Cloud security, privacy.

I. INTRODUCTION

With respect to the regular increase in population, the data will also be increased in proportion with the population. So as that, the primary concern is to maintain the data secrecy by keeping the data private. Due to the huge amount of data, the cloud technology emerged to maintain data and various applications by using the internet and remote servers. The cloud storage provide the secure online data storage with backup files of data stored on the physical storage devices. As the data stored with the third party , there is a need of security of data. So the term cloud security appear in field of security as an important perspective to preserve the data. As the cloud computing is one of the trending topic in the field of information techology. User can get high computing power and potential benefits of instant availability, scalability and resource sharing by using cloud computing. Cloud provide the number of services to their users such as IaaS(Infrastructure-as- a-service), PaaS(Platform-as-a-service), SaaS(Software-as-a-service). Cloud is characterised with some features viz., on-demand self service, broad network access, multi-tenancy(allows multiple customers to share the same physical infrastructure with privacy and security over their information.) and resource pooling(multiple customers can served from the same physical resources), elasticity and scalability, measured services(Provide pay-per-use policy). Even-though cloud computing becoming an ideal way to maintain the users data and applications, there is an important issue to deal with is of security.

As if now the data is securely stored on the cloud but whenever the user wants to operate or utilize their data they need to share the encryption key with the cloud service provider which create an problem of security. The various mathematical operations on the integer data has been performed using a fully homomorphic encryption technique. 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. Homomorphic encryption is a solution used to solve the issue of cloud security, as it enables the user to perform the operation on the encrypted data itself and the result will the encryption of the result of those computations. Homomorphic encryption is the way in which you can perform a limited form of computations on the encrypted data (ciphertexts) and generate the encrypted result for those computations. Fully homomorphic encryption technique is not yet be practical as its very difficult to perform any random operation on the ciphertext.

Cloud Security includes protecting data from unauthorized access, protecting data from damage and development and implementing policies and procedures for recovery from breaches and data losses. The proposed system has the objectives viz., 1)to develop a cloud based healthcare data storage and searching

system for hospitals, 2)to implement fully homomorphic encryption technique for large integers as well as for text, 3)to include single key as multi key homomorphic technique.

II. LITERATURE SURVEY

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 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. [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 multiuser 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 analysising over the different existing FHE techniques [14], homomorphic encryption technique for known plaintext 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 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 [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].Use of multiple keys for outsourced multiparty computation is explained in [7]. 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.

III. 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 operation has to be performed on the encrypted data itself.

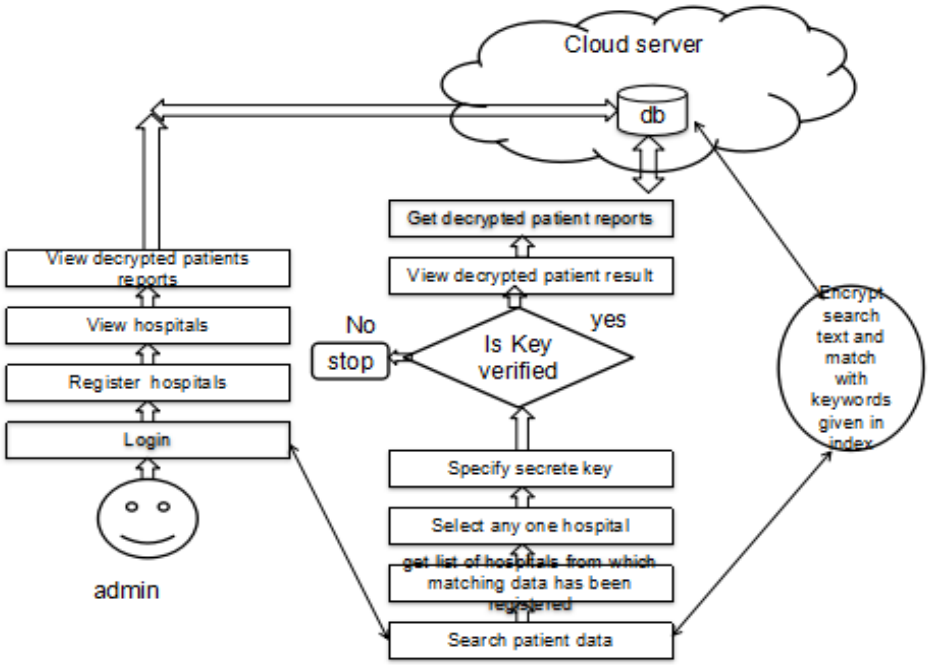

Fig a. Work-Flow of Proposed System

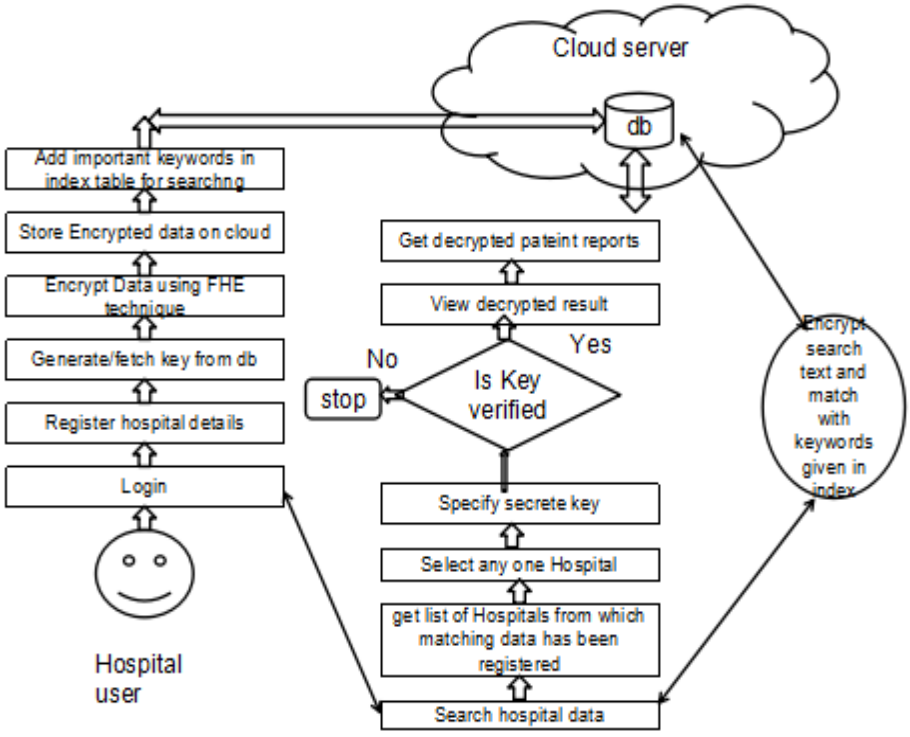

Fig b. Work-Flow of Proposed System

In proposed system, hospital users like doctors, pathology admin, new patients can be registered and manage by the hospital admin. The patients can also register themselves by their own and the id, password will be auto-generated and get stored at the cloud in encrypted format. Only the admin can see the users credentials *(userid and password).* Here, the key for records has been generated using random key generation algorithm. The key will then be encrypted and store it on the cloud. The technique will also work with single key as well as multiple keys. The multiple keys are associated with different hospitals. The patient will have the unique and single user-id associated with all the registered hospitals. The registered hospitals can access the patient register with any of the registered hospital i.e. User-id of patient can be used universally over the system.

The system will also support the searching operation. At the time of searching, the data will be extracted from database in encrypted format only. Client will receive encrypted data coming from server and decrypt the data by using key and then it will show the decrypted data to the user. While searching has been performed in following manner. At first, we have to specify search query then search query will be encrypted. The query has been matched with index and if any match found, system will show matching data according to search criteria. User will select any of the matched hospital, the key then fetch according to the hospital wise. The remaining details will be match by using search query and hospital wise key. To maintain security the user's authenticity verified by using otp and then only the data sent on client side. On the client side the decryption will be performed and data will be shown to the requested user.

IV. CONCLUSIONS

The devised innovated fully homomorphic encryption technique will be more effective than the existing homomorphic encryption techniques. It support the operations on the large integers as well as text data. The proposed system is user-friendly and robust in nature. It can also work faster with accuracy in result. It is also used for searching the data records in the database. The system uses the number of encryption algorithms at different levels to maintain the security.

There are several advantages of the proposed system viz., 1) It is more secure and faster than that of existing systems, 2) It can work with large integer and text data, 3) It will auto generate the use-rid and password associated with users and will be stored in the database in the encrypted format.

REFERENCES

[1] 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.
[2] 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.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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.
[8] 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.
[9] 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.
[10] Cyrielle FERON, Vianney LAPOTRE, and Loic LAGADEC, "Fast Evaluation of Homomorphic Encryption Schemes based on Ring-LWE," 2018 IEEE
[11] 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.
[12] 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.
[13] 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).
[14] 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.
[15] 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.
[16] 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.
[17] Baohua Chen, Na Zhao, "Fully Homomorphic Encryption Application in Cloud Computing," 2014 11th International Computer Conference on Wavelet Active Media Technology and Information Processing(ICCWAMTIP), 19-21 Dec. 2014.
[18] Jian Liu and Jing-Li Han Zhao-Li Wang, "Searchable Encryption Scheme on the Cloud Via Fully Homomorphic Encryption," 2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control, 21-23 July 2016.

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