A Survey on Implementation of Homomorphic Encryption Scheme in Cloud based Medical Analytical System

Mr.Rajesh S. Raut [#1], Prof. P. B. Sambhare [*2], Prof. C. J. Shelke [#3]

[#]Department of Computer Science and Engineering, P. R. Pote College of engineering, Amravati, Maharashtra, India

[1]*rraut64@gmail.com*

[2] *sambhareprafu1832@gmail.com*

[3]*chetanshelke7@gmail.com*

Abstract**—** The privacy of sensitive personal information is more and more important topic as a result of the increased availability of cloud services. These privacy issues arise due to the legitimate concern of a) having a security breach on these cloud servers or b) the leakage of this sensitive information due to an honest but curious individual at the cloud service provider. Standard encryption schemes try to address the first concern by devising encryption schemes that are harder to break, yet they don't solve the possible misuse of this sensitive data by the cloud service providers. Homomorphic encryption presents a tool that can solve both types of privacy concerns. The clients are given the possibility of encrypting their sensitive information before sending it to the cloud. The cloud will then compute over their encrypted data without the need for the decryption key. By using homomorphic encryption, servers guarantee to the clients that their valuable information to have no problems after being in a difficult situation..

Keywords- *Cloud Services, Homomorphic Encryption,cloud computing,Access control,security.*

*****

I. INTRODUCTION

The term "cloud" originates from the world of telecommunications when providers began using virtual private network (VPN) services for data communications. The definition of cloud computing provided by National Institute of Standards and Technology (NIST) says that: "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In cloud computing there is no need to store the data on desktops, portables etc. You can store the data on servers and you can access the data through internet. Cloud computing provides better utilization of distributed resources over a large data and they can access remotely through the internet.

Homomorphic encryption presents a tool that can solve problem of privacy concerns. The clients are given the possibility of encrypting their sensitive information before sending it to the cloud. The cloud will then compute over their encrypted data without the need for the decryption key. Homomorphic encryption can be used to encrypt the data measured by wearable and portable medical devices to uploading them on cloud and make available to use by authorized user for the various applications.

II. EXISTING SYSTEM AND THEIR LIMITATIONS

In [1] Aderonke Ikuomola, O. O. uses Homomorphic Encryption to secure patients medical records and Bilayer Access Control to gives access right to the records and developed a Secured e-Health System called SECHA. SECHA comprises of five basic components namely; patient, PHR/object, Access Control Module, User/Subject and Cloud. A cloud based patient privacy system has been presented. PHR is stored in the cloud, and can be accessed through a web portal by multiple owners and users.

The security and privacy of health-data break in variety of ways. For example, health data may be susceptible to access by unauthorized external entities when stored or is in transit from a general practitioner to a remote medical specialist.

In [2] Ciara Moore, M. O. proposed the use of graphics processing units (GPUs) and field programmable gate arrays (FPGAs) for implementations of homomorphic encryption schemes. This review presents the current state of the art in this promising new area of research and highlights the interesting remaining open problems. Practical FHE implementations, further research into suitable hardware designs and optimizations of existing schemes could provide a large speed up. One major bottleneck in the implementation of these schemes is memory storage Large parameter sizes and very large cipher text sizes consume large amounts of memory, which requires memory management. Lastly, optimizations to target specific devices, such as using the embedded multipliers on an FPGA, are required.

In [3] Iram Ahmad, A. K. implement a method to perform the operation on encrypted data without decrypting and provide the same result as well that the calculations were carried out on raw data and use proxy re-encryption technique that prevents cipher text from chosen cipher text attack. In this paper they proposed RSA and Paillier algorithm for homomorphic encryption using proxy-Re-encryption algorithm that prevents cipher data from Chosen Cipher text Attack (CCA) and system is more secure than existing system. One of the bottleneck is size of key and there is no proxy re-encryption method for other homomorphic encryption scheme.

In [4] Khedr A.,Prposed a system "SecureMed: Secure Medical Computation using GPU-Accelerated Homomorphic Encryption Scheme" which Optimized and implemented an NTRU based variant of the HE scheme achieves much slower growth of noise, and thus much better parameters than previous HE schemes

In[5] Manish M. Potey, M. H., Proposed a system "Homomorphic Encryption for Security of Cloud Data" In which Algorithm used which simplified, efficient version applied in AWS public cloud. It can be used for various applications such as online auctioning, medical purposes and business purposes.

In[6] Ovunc Kocabas, T. S., proposed a system "Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing" which Demonstrated results on an FHE-driven program by using a 24-hour set of ECG samples from the THEW database.

Author Name	Year	Paper / System	Description
Aderonke Ikuomola, O. O	2014	Securing Patient Privacy in E-Health Cloud Using Homomorphic Encryption and Access Control	PHR is stored in the cloud, and can be accessed through a web portal by multiple owners and users.
Ciara Moor, M´aire O'Neill	2014	Practical homomorphic encryption: A survey	Major bottleneck in the implementation of these schemes is memory storage Large parameter sizes and very large cipher text sizes consume large amounts of memory, which requires memory management.
Iram Ahmad, A. K.	2014	Homomorphic Encryption Method Applied to Cloud Computing	Proposed RSA and Paillier algorithm for homomorphic encryption using proxy-Re-encryption algorithm that prevents cipher data from Chosen Cipher text Attack (CCA) and system is more secure than existing system.
Payal V. Parmar, S. B.	2014	Survey of Various Homomorphic Encryption algorithms and Schemes	Described various homomorphic encryption schemes which can be used for mixed homomorphic encryption property.
Ovunc Kocabas, T. S.	2015	Towards Privacy-Preserving Medical Cloud Computing Using Homomorphic Encryption	Present a working implementation of a long-term cardiac health monitoring application using a well-established open source FHE library. They demonstrated that, the afore- mentioned three fundamental computations.
Ovunc Kocabas, T. S.	2015	Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing	Demonstrated results on an FHE-driven program by using a 24-hour set of ECG samples from the THEW database.
Manish M. Potey, M. H.	2016	Homomorphic Encryption for Security of Cloud Data	Algorithm used which simplified, efficient version applied in AWS public cloud. It can be used for various applications such as online auctioning, medical purposes and business purposes.
Khedr A.	2017	SecureMed: Secure Medical Computation using GPU-Accelerated Homomorphic Encryption Scheme	Optimized and implemented an NTRU based variant of the HE scheme achieves much slower growth of noise, and thus much better parameters than previous HE schemes.

III. Proposed System

In proposed system separate cloud data sever and key generation server is provided which protect patient data by unauthorized access. It is possible due to use patient data anytime and anywhere by the use of internet for patient, doctors, analyst, and hospital staff and at various laboratories. First step of proposed system will be data collection. In this database will be constructed which includes collection of records of different patient with their health records. On the basis of the data it is possible to doctor and analyst to predict the disease of patient so it is very important data and need to protect it from unauthorized user and cloud admin also. It helps to manage all these tasks using homomorphic encryption technique.

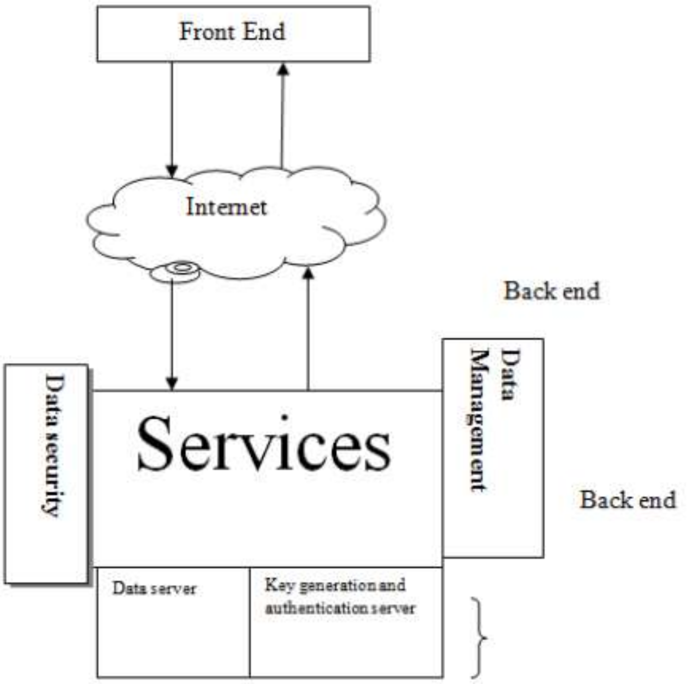

Fig-1: Architecture of the Homomorphic Encryption scheme in cloud based medical analytical system

IV. Applications of Proposed System

1. Proposed system is used to handle medical data measurements, analysis, and key distribution.
2. It is used as tool for diseases diagnosis based on symptoms.
3. It is used to store and analysed patient sensitive data by analyst.

References

[1] Aderonke Justina. Ikuomola and Oluremi O. Arowolo.“Securing Patient Privacy in E-Health Cloud Using Homomorphic Encryption and Access Control” , International Journal of Computer Networks and Communications Security, vol.2, pp15-21,2014.

[2] Ciara Moor. M´aire O’Neill, Elizabeth O’Sullivan, Yarkın Dor¨oz, Berk Sunar,“Practical homomorphic encryption: A survey” International Symposium on Circuits and Systems, Australia IEEE. 2014.

[3] Iram Ahmad, A. K.”Homomorphic Encryption Method Applied to Cloud Computing”, International Research Publication House,vol.5, pp. 15119-1530,2014.

[4] Khedr, A. “SecureMed: Secure Medical Computation using GPU-Accelerated Homomorphic Encryption Scheme”. IEEE Journal of Biomedical and Health Informatics,vol.8., pp. 1 – 1, 2017.

[5] Manish M.Potey, M. H.”Homomorphic Encryption for Security of Cloud Data”. ScienceDirect”, International Conference on Communication, Computing and Virtualization, vol.79,pp.175-181,2016

[6] Ovunc Kocabas, T. S. “Utilizing Homomorphic Encryption to Implement Secure and Private Medical Cloud Computing”. IEEE 8th International Conference on Cloud Computing,vol45.pp23-31,2015.

[7] Payal V. Parmar, S. B.“Survey of Various Homomorphic Encryption algorithms and Schemes”. International Journal of Computer Applications,vol.91,pp.26-32,2014.

[8] Ovunc Kocabas, T. S.” Towards Privacy-Preserving Medical Cloud Computing Using Homomorphic Encryption”, vol.34,pp. 213-246,2015.

[9] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, “(Leveled) Fully Homomorphic Encryption Without Bootstrapping,” in Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ser. ITCS ’12, New York, NY, USA, 2012, pp. 309–325.

[10] Z. Brakerski and V. Vaikuntanathan, “Efficient Fully Homomorphic Encryption from (Standard) LWE,” in Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on, 2011, pp. 97–106.

[11] C. Gentry, A. Sahai, and B. Waters, “Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based,” in Advances in Cryptology – CRYPTO 2013, ser. Lecture Notes in Computer Science, R. Canetti and J. Garay, Eds. Springer Berlin Heidelberg, 2013, vol. 8042, pp. 75–92.

[12] M. Naehrig, K. Lauter, and V. Vaikuntanathan, “Can Homomorphic Encryption Be Practical?,” in Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, ser. CCSW ’11, New York, NY, USA, 2011, pp. 113–124.

[13] C. Gentry, S. Halevi, and N. Smart, “Homomorphic Evaluation of the AES Circuit,” in Advances in Cryptology – CRYPTO 2012, ser. Lecture Notes in Computer Science, R. Safavi-Naini and R. Canetti, Eds. Springer Berlin Heidelberg, 2012, vol. 7417, pp. 850–867.

[14] J. Hoffstein, J. Pipher, and J. Silverman, “NTRU: A ring-based public key cryptosystem,” in Algorithmic Number Theory, ser. Lecture Notes in Computer Science, J. Buhler, Ed. Springer Berlin Heidelberg, 1998, vol. 1423, pp. 267–288.

[15] W. Wang, Y. Hu, L. Chen, X. Huang, and B. Sunar, “Accelerating fully homomorphic encryption using GPU,”

in High Performance Extreme Computing (HPEC), 2012 IEEE Conference on, 2012, pp. 1–5.

[16] Y. Doroz, Y. Hu, and B. Sunar, “Homomorphic AES Evaluation using NTRU,” Cryptology ePrint Archive, Report 2014/039, 2014.

[17] R. Lindner and C. Peikert, “Better Key Sizes (and Attacks) for LWE-based Encryption,” in Proceedings of the 11th International Conference on Topics in Cryptology: CT-RSA 2011, ser. CT-RSA’11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 319–339.

[18] Dor¨oz and B. Sunar, “Flattening NTRU for Evaluation Key Free Homomorphic Encryption,” Cryptology ePrint Archive, Report 2016/315, 2016.

[19] S. Halevi and V. Shoup. (2013) Design and Implementation of a Homomorphic-Encryption Library. researcher.ibm.com/researcher/files/ us-shaih/he-library.pdf.

[20] D. Cousins, K. Rohloff, C. Peikert, and R. Schantz, “An update on SIPHER (Scalable Implementation of Primitives for Homomorphic EncRyption) ; FPGA implementation using Simulink,” in High Performance Extreme Computing (HPEC), 2012 IEEE Conference on, 2012, pp. 1–5.,”