ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 9, Issue, 4(K), pp. 26303-26306, April, 2018

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

IMPLEMENTATION OF HOMOMORPHIC ENCRYPTION SCHEME IN CLOUD BASED MEDICAL ANALYTICAL SYSTEM

Rajesh S. Raut and Sambhare P. B

Department of CSE, Amravati University, India

DOI: http://dx.doi.org/10.24327/ijrsr.2018.0904.2032

ARTICLE INFO

Article History:
Received 12th January, 2018
Received in revised form 24th February, 2018
Accepted 10th March, 2018
Published online 28th April, 2018

Key Words:

Cloud Services, Homomorphic Encryption, cloud computing, Access control, security.

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 security breach on these cloud servers and the leaking 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 from 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.

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 the 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 the 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 upload them on cloud and make available to use by authorized user for the various applications.

LITERATURE SURVEY

After discussing about introduction of security to sensitive patient information in clod base medical, analytical system in the world today. In this section we are briefed about a literature survey on the various solutions proposed by literatures/authors.

In paper [1] 2014 Authors have discussed about providing secure sensitive patient data on cloud servers.

A problem discussed they have analyzed when the data is transferred to the cloud encryption methods used to secure this data, but when we want to do the calculations on data located on a remote server, it is necessary that the cloud provider has access to the raw data, and then it will decrypt them and privacy of sensitive data is broken.

Proposed solution: In this paper, we propose 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

In paper [4] 2017 Authors have discussed with the encryption algorithms help protect sensitive data from outside attackers,

Corresponding author:* **Rajesh S. Raut
Department of CSE, Amravati University, India

but they cannot be used to compute on this sensitive data while being encrypted. Homomorphic Encryption presents a very useful tool that can operate on encrypted data without the need to decrypt it.

Cloud supports storing software, firmware etc. problems like reducing of data storage, collaboration of different files over the cloud. Patient data saved in the cloud actually saved in encrypted format and authorized user can access data for various purposes without breaking the privacy and get the results. Some existing cloud based services and apps are:

HSM - Clinic Management System: It includes demographic information, personal information, personal and family medical history, allergies, diagnosis, medications, visit follow-up, tests and prescriptions. And provide familiar, easy to services for medical application.

Y-HLTH: It is a unified health care app that facilitates communication with the doctor and the patient. Y-HLTH is a community that has been started with the intention of changing the lives of people by making health care access easier and hassle free.

Limitation: All these applications provide the data security using algorithms, but they cannot solve the problem of disease detection on the basis of symptoms.

PROPOSED METHODOLOGY

Proposed methodology has been divided into three phases:

Information security

At the client side sensitive patient information is encrypted using homomorphic encryption algorithm and the data is stored in cloud server. Different user performed operation on encrypted no need to decrypt.

User authentication

In order to view sensitive patient information in the form of PHR report, key to be download which is stored on separate key generation sever at the time of encryption.

Diseases Detection

All the symptoms entered by patient comparisons with predefined dataset and disease detection are performed and display to the doctor and patient.

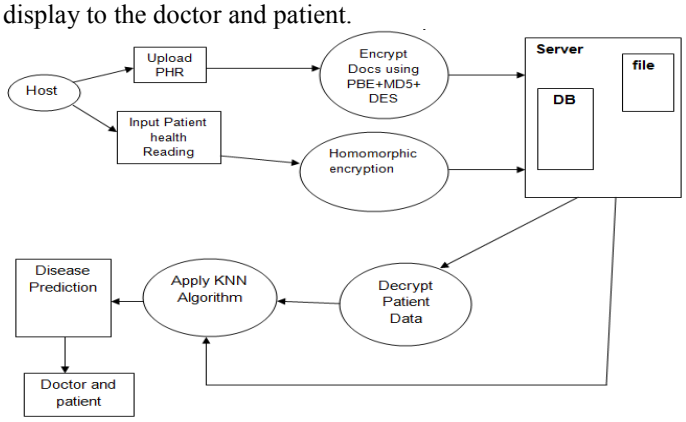


Fig Architecture of proposed system

Homomorphic encryption algorithm

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. Due to the homomorphic encryption algorithm is used for encryption of sensitive patient information and store on cloud based server even though data is present in the database table no one can understand it.

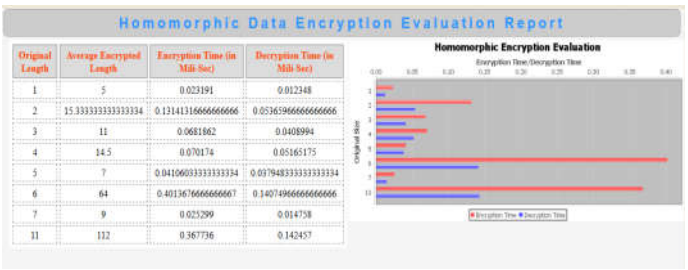
Take input as no or text
If input is text then convert it into ASCII value n= ASCII of text
Else n=input no
Reverse the no n
Generate key k=random (1, (Len (no)/2))
If k is not even, convert it into even no
Divide n by k
Final results will be the cipher no
If input is a text value to convert the no into char
Store the cipher text/no into DB

Algorithm for homomorphic encryption

Take cipher text/no as input from DB
If input is text then convert it into ASCII value n=ASCII of text
Else n=input no
Get key k
N=n*k
Reverse N s.t Len (N) =Len of original cipher which is stored in DB
N= (Reverse (N))
N is original no
If input is text, convert N into char

Algorithm for homomorphic decryption

RESULT ANALYSIS

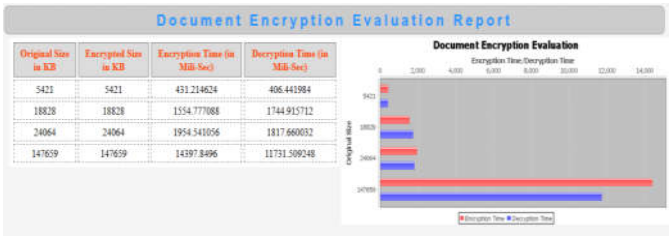


Graph Homomorphic data encryption evaluation report

In system simulations, we evaluate the performance of IHECBMAS by analyzing the time required. Among currently known privacy-preserving approaches, system apply homomorphic encryption to the application. As the server, we use a powerful PC with 2.5 GHz P4 processor, and as the client a PC with 1GHz P3 processor. The figure shows that the encryption and decryption time decreases.

For example, when original length is 1 then the average encrypted length is 5 the encryption time is 0.023191 and decryption time is 0.012348.

For example, when original length is 7 then the average encrypted length is 9 the encryption time is 0.025299 and decryption time is 0.014758.



Graph Encryption Computation time

Encryption Computation Time

The encryption computation time is the time which taken by the algorithms to produce the cipher text from the plain text. The encryption time can be used to calculate the Encryption Throughput of the algorithms.

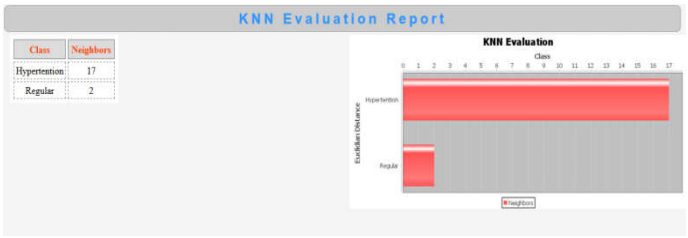
The decryption computation time is the time taken by the algorithms to produce the plain text from the cipher text. The decryption time can be used to calculate the Decryption Throughput of the algorithms.

Encryption Throughput (Kb/Sec) ∑ Input files / ∑ EET

And in same we to calculate decryption rate per unit time in the second we use following formula as,

Decryption Throughput (KB/Sec) = ∑ Input files / ∑ DET

We have taken five files for testing purposes of different sizes as 15,550,1020,2040,5470 KB size and evaluate all this file by using IHECBMAS and two other mailing service provider security techniques.



Graph KNN Evaluation Report

KNN Algorithm is used to detect the possible diseases, according to user input is compared with predefined dataset and the result is displayed to the doctor and customer.
KNN Alorithm

CONCLUSIONS

Although a huge security parameters are there in the world and few of them only discussed here. But main and vital security parameters get applied in this project. Information security is achieved by using the Homomorphic encryption technique. The combination of homomorphic encryption algorithm and MD5 algorithm we have achieved the maximum security level. And hence information can now transmit and store on a cloud in a secure way. We also have achieved, the user sensitive data security by restricting the access of data only by authorized users only by sending mail with user id and password in registered user. Now by using proposed system patient store sensitive data on the cloud more securely. In this way we restrict the unauthorized access of sensitive data on cloud sever. The patient can access different reports from any part of the world in secure way. Last but not least it is possible to detect the disease of the patient on the basis of different reading, which is helpful for both patient and doctor.

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.

How to cite this article:

Rajesh S. Raut and Sambhare P. B.2018, Implementation of Homomorphic Encryption Scheme in Cloud Based Medical Analytical System. *Int J Recent Sci Res.* 9(4), pp. 26303-26306. DOI: http://dx.doi.org/10.24327/ijrsr.2018.0904.2032

****