Framework of Cloud Based Hospital Management Data Security By Fully Homomorphic Encryption

S Gnana Sophia[1], Dr. K. K Thanammal[2], Dr S S Sujatha[3]
[2, 3]Associate Professor, Dept of Computer Science and Applications
[1, 2, 3] S.T. Hindu College, Nagercoil, Affilated by: Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli-627012,TN,India

Abstract- *Cloud computing is getting more popularity day by day . Because the more growth of the companies which are in need of the location to store their data. So they have much more competition to administer large space to store data with features and the service with high quality. It is an on request of network access to mutual computing appliances . It is a model for administering, accumulating and handling data online through the internet. Cloud computing is the important concept in hospital management These assets incorporate apparatuses and applications like information stockpiling, servers, information bases, systems administration, and software. The cloud provides services to hospital management system. There is an important performance of homomorphic encryption algorithm to perform the availability , security and performance. The proposed system uses the types of homomorphic encryption systems to achieve the more competent homomorphic encryption algorithm to encrypt the hospital records and do useful computations without breaking the original data.*

Keywords- MMS, Eigen, Homomorphic Encryption, Cloud computing

I. INTRODUCTION

Cloud is used in various services such as servers, storage, and software development platforms over the internet. Medical Management System (MMS) do the job by following the cloud option. Increasingly, the hospital's technology lieutenants are concluding that remote hosting and information storage is more secure as the local option. Cloud computing makes life more secure on hospital administrators by issuing additional advantages. This paper covers various methods of security in cloud computing. A new mechanism in which the security can be made through the dimensionality reduction of eigen values in Fully Homomorphic Encryption scheme.

Cloud computing concept has attracted many resources like infrastructure, platform and software can be used using web based tools and advantages through internet. Nowadays the path has improved very much and provides more advantages

1.Modular: The cloud service provider issues additional storage space instead of buying and preparing servers. These servers are online already and produce the part of our IT operations quickly

2.Financial Asset: The hospital's expense cost low or providing cloud storage.

3.Fraternization: Cloud storage consists of huge set of databases for storing files and documents.

II. CLOUD SERVICES

1. SaaS (Software as a service): It approaches an application and it has little or no control over the delivery Eg: Gmail, Salesforce.com
2. PaaS (Platform as a service): It routes to a software development environment to allow them to create their own applications of cloud. Eg: Cloud Foundry
3. IaaS (Infrastructure as a service): It has Quick and easy provision of full computing resources including processing storage and network. It has no control Eg: SUSE open stack cloud

III. CLOUD SECURITY

It is the protection of data stored online through cloud computing platforms from burglary, exposure, and deletion. Methods of given cloud security include firewalls, infiltration testing, virtual private networks (VPN), and avoiding public internet connections. Security in cloud consists of technology, tasks and practicing. Users have fear that their information are retrieved by unauthorized persons, since many users are using cloud service with heavy overload. Because of the usage of cloud storage by more users, the security will be affected.

- Confidentiality: Patient's data are disclosed from only authorised identities.
- Integrity: Patient's information is protected from manipulations by unauthorised persons.
- Availability: Only authorized patient can access and use their personal data when ever information is required.

IV. CHARACTERISTICS OF CLOUD COMPUTING

- On-Demand self-Service: A consumer can have independent computing capacities, such as server time and network storage as needed automatically without the need of user interaction with each service provider
- Wide range network access: Capabilities are accessed by client platforms eg: mobile phones, tablets, Laptops, workstation
- Set of Resources: The provider's computing resources are grouped to provide many consumers
- Scalable Provisioning: The capabilities available for provisioning shows to be unlimited and can be appropriate in any quantity at any time.

APPLICATIONS OF FHE

- Circulating data with confidentiality has become a limiting stride for the field of genomics. DNA and RNA sequences can be achieved briskly and as a result large quantities of such arrangements are concentrating in different labs and medical institutes.
- Current strategies for preserving genomics data have proven to place a high overhead on researchers.
- Confidentiality Problem
- Ability to compute over ciphertext instead of Plaintext
- One could use information without knowing the control of that information
- Privacy generated
- Performance

V. RELATED WORK

In [1], the own health record is partitioned into many security domains. This can reduce key response. In [2], the authors used to encrypt their personal information. The cloud will calculate over the encrypted data without the use of decryption key. In [3], they used symmetric cryptography algorithm called AES. In [4], the authors mentioned that the cloud providers should have the responsibilities on the conservation of isolation and confidential information stored in theirdata processing centre sharing by Virtualization

VI. PROBLEM IDENTIFICATION

The techniques used in securing the medical information are kept with the patient itself. Suppose if the patient has no knowledge about the security of data, there may be a chance to leak out the password. So there will be a way for insecurity problem.

VII. PROPOSED FRAMEWORK

The high dimensional data can be replaced by its projection into most important value. These are corresponding to the largest eigen values. The upgrading of security can be made through dimensionality reduction and through Fully Homomorphic Encryption system. Then the security is maintained.

FULLY HOMOMORPHIC ENCRYPTION

Homomorphic with respect to two operations i.e., addition and multiplication

- Elgamal : f(m0, m1) = m0m1

This algorithm is proposed by TaherElgamal in 1984. It exhibits multiplicative homomorphism. They multiply each component of multiple ciphertexts with their corresponding r components. The decrypted result is equivalent to the multiplication of the plaintext values.

- Paillier: f (m0, m1) = m0 + m1 . It exhibits additive homomorphism. By multiplying each component of multiple ciphertexts with their corresponding respective components, the decrypted result is equivalent to the addition of the plaintext values.
- Goldwasser-micali = m0 (+) m1 Entities A and B create a public key and a corresponding private key for encryption. Each of these entities must be
  1. Select two large distinct primes p and q.
  2. Compute n = p * q
  3. Select y € Zn such that y is a quadratic non-residue modulo n and the Jacobi symbol y/n = t (y is a pseudo- square modulo n)
  4. A's public key is (n , y) and A's private key is (p , q)

B encrypts a message m for A which A decrypts B should do the following

a. Obtain A's authentic public key (n, y)
b. Represent the message m as a binary string m = m1m2.....nt of length t.
c. For i from 1 to t do
i. Choose x €Zn
ii. If mi = 1 then set Ci ←yx^2 mod n, otherwise set Ci ← x^2 mod n
d. Send the t-tuple C = (C1, C2,.... Ct) to A

VIII. CONCLUSION

The approach of cloud computing security on homomorphic encryption produce results of operations on encrypted data without the acknowledgement of the plaintext

data. A descriptive way of holding most of the details in the data is by converting from high dimensionality data into low dimensionality data. The security problem is overcome by the advantage of homomorphic encryption.

REFERENCES

[1] Nishitha Ramakrishnan and B Sreerekha: "Enhancing security of Personal Health records in Cloud Computing by Encryption" Inernational Journal of Science and Research ReferencesISSN(online: 2319 – 7064

[2] Mr. Rajesh S. Raut, Prof. P. B Sambhare and Prof C. J Shelke "A survey on Implementation of Homomorphic Encryption Scheme in Cloud based Medical Analytical System"

[3] Karim Abouelmehdi, Abderrahim Beni-Hessane and Hayat Khaloufi "Big Data in Medicial Security", Journal of Big data 2018

[4] Suraj Shesheshrao Gaikwad and Amar R. buchade "Homomorphic Encryption Approach for cloud data security Inernational Journal of Engineering and Technology Volume: 03 Issue:09| September- 2016.

[5] Mohd Rahul, Hesham A Alhumyani, Mohd Muntjir and Minakshi Kambojl "An improved Homomorphic Encryption for Secure Cloud Data Storage" International Journal of Advanced Computer Science and Applications Volume: 8, No. 12, 2017.

[6] Maha TEBAA, and Said EL HAJII "Secure Cloud Computing Through Homomorphic Encryption"

[7] M. Subhashini and Dr P. Srivaramangai "A study on Cloud Computing Securitied and Algorithms " International Journal of Scientific Research in Computer Science, Engineering and Information Technology 2018 IJSRCSEIT | Volume 3| Issue 3 | ISSN : 2456 – 3307.

[8] Mohd Rahul, Hesham A. Alhumyani and MohdMuntjir " An Improved Homomorphic Encryption for Secure Cloud Data Storage " International Journal of Advanced Computer Science and Applications Vol. 8 No. 12 , 2017

[9] Yuan Zhang, Hongwei Li "Health Dep: An efficient and Secure Deduplication Scheme fot Cloud – Assisterd eHealth Systems"

[10] Michael Miller "Cloud Computing " WEB BSED Applications that change the way you work and Collaborate Online.