IJIRMET
ISSN (Online): 2456-0448
International Journal of Innovative Research in Management, Engineering and Technology
Vol. 3, Issue 3, March 2018

# Secured Analysis Of Iatric Data Using Homomorphic Encryption

[1] Ranjitha.R, [2] Swedha.B, [3] Sowmiya.P
[1] [2] [3] R.M.K. College of Engineering and Technology.
[1] ranji104084.cs@rmkcet.ac.in, [2] swedh104105.cs@rmkcet.ac.in, [3] sowmi104099.cs@rmkcet.ac.in.

*Abstract*: ***Recent advancements in technology has brought many changes in safeguarding, computing and storing of data. The questionable factors in the context of data privacy that is computing and sharing enormous sets of data have also augmented. Homomorphic encryption is one such technique which guarantees franchise in safeguarding information under cryptographic domain .Wise use of four familiar arithmetic operators in a diverse way en routes a powerful homomorphic tool. The paper illuminates the usage of this selfsame tool to provide an efficacious strategy in bringing all security concerns of cloud under check and also analyze these secured datum using big data analytics.***

***Keywords—homomorphic encryption, securedanalysis, medicaldata, ROW's algorithm***

## I. INTRODUCTION

The major concept of confidentiality required for the access of data by third party comes into consideration when they are managed by a wide range of automated networks.Since these mechanized network require less manpower, scrutinizing stipulation has reduced in the long run that is the word of honor need not or will not be kept at all times as most data is not encrypted.Securing one's privileged information may lead the man into an anxious state forever . In order to secure the information, strong encryption algorithm needs to be deployed on regular basis.Encrypted details may be used in various other fields such as predictive analysis [1] , artificial intelligence[3] ,virtual reality and many more.The above specified technologies can be used on the encrypted data if it the data preserves its properties even after encryption.The solution for these problems simply makes use of homomorphic encryption which are usually present in two flavours: fully homomorphic encryption and partial homomorphic encryption schemes. We will further discuss in detail about those schemes in the later sections. Hence by protecting and analyzing the information on which one create can assure satisfied privacy and confidentiality to the end users. The maxim of this paper is how robust is a patient's health record is maintained and issued back to them securely. The field of medical science plays a major role because the information[2] saved about a person be it a one who lives ' in a castle or by a castle' doesn't really matter. In general providing guaranteed security using the idea of homomorphic encryption would be ideal. One can then perform analysis of the translucent record. This paper makes use of native RSA as its base. The paper is designed as follows: Section II describes about the homomorphic encryption in detail. Section III about related work in depth .Section IV illuminates the implementation model of our project. And also particularize on the mathematical formula employed. Section V on various analysis performed. Section VI describes the further work and Section VI sketches the summary in detail.

## II. HOMOMORPHIC ENCRYPTION

Homomorphic encryption is the scheme that allows convoluted calculations to be performed on encrypted data without compromising on encryption. In mathematics, homomorphic encryption describes the transformation of one data set into another while preserving the relationship or operations structure between elements in both sets. The term is derived from the Greek words for "same structure". Hence the records contained in homomorphic encryption system remains the similar schema and logical calculations are performed for encoding records. Homomorphic encryption is expected to play an important role in cloud computing as it provides a way in storing the same data in a different yet similar format.Various companies see this as a break through invention to store to privileged data in public providers . Exemplifying the legitimate use of homomorphism with real time scenario.Consider storing data in Amazon Web

Services (AWS) - S3 buckets or EC2 instances. Autodidacts who'd like to explore and learn might use these public data. What happens if they accidentally or intentionally modify them? What if it turned out to be a catastrophic error ? Similar incidents will not occur if the data had been encrypted not with RSA or AES but with a more advanced property preserving algorithm. The concept of Craig Gentry ,the man who introduced computation to be performed on enciphered data without ever having to decrypt it has proven that it is possible with Rivest–Shamir–Adleman algorithm. Enciphering multiple times a yottabyte sized dataset might turn to be an incompetent approach.So how could you make companies and agencies let such data off their servers in more comfortable way for outsourcing high-value work ? Using one of the predefined approaches be it partial homomorphic encryption scheme or fully homomorphic encryption scheme.

A. Partially Homomorphic Encryption System:

A cryptosystem is considered partially homomorphic if it exhibits either additive or multiplicative homomorphism but not both. Some examples of partially homomorphic encryption systems are:

- RSA-multiplicative homomorphism
- ELGAMMAL-multiplicative homomorphism
- PALLIER-additive homomorphism

B. Fully Homomorphic Encryption System:

A cryptographic system that promotes random calculations on encrypted texts are said to be fully homomorphic encryption and known to be much strong. Such a scheme enables construction of programs for many desirable functionally, which can be run on encrypted inputs to produce the encryption of desired result. This is because homomorphic encryption system doesn't require the purpose to decrypt its inputs and can be used like a black boxed glove inside a transparent medium. It can be run by entrusted party without revealing its inputs and internal state. Fully homomorphic cryptosystems have great practical implications as their key generation is dynamic and does depend on the one who lends and the one who with holds.

C. Partial ++ Homomorphic Encryption System:

Partial ++ homomorphism is a modernistic approach proposed by the author and co-authors of this paper (Ranjitha-sOwmiya-sWedha-). The main motive of this paper is to correlate two flavours of homomorphism to help secure data in the best possible way.Upon reaching big ears, crypto experts may suggest this to one of the finest solution found in this generation .
The most confidential data in any patient record will be the patient's personal details such as name, phone number,email-address ,location and many more.The less confidential data will be the medical report (medical report without patient details is of least importance), diagnosed disease etc.So here in this case confidential data will be encrypted initially by a division-addition non-existing relation and later the the first half ciphertext and the second half plaintext will be encrypted using any partially homomorphic algorithms.Here in this case we make use of RSA.Fig 1.1 shows a sequence diagram of encrypting data using partial ++ homomorphism.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 3, March 2018

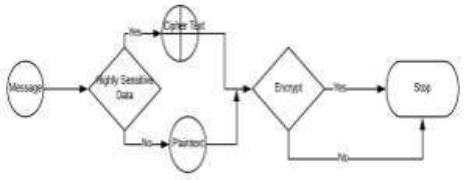



Fig 1.1 :Flow of encryption using Partial ++ homomorphism

## III. RELATED WORK

A.Private Predictive Analysis On Encrypted Data

Storage of confidential medical records in data centers which are being used by reputed hospitals are increasing. With an era of homomorphism , a technique which doesn't subsume decryption stacks up privately preserving data on the run. This system as a proof of concept makes use of Amazon to carry out an experiment by analyzing the patient's health and the input it took is the encrypted health information and in return it produced the occurrence of cardiac disease in encrypted form.They make use of fully homomorphic encryption(FHE).They give the user a set of parameters so as to choose their desired FHE type The work has not used the famous pallier instead it focussed on building it own one with a different tool.Hence this model, cloud service proves that it is possible predict the data even after encryption.

B. Security And Privacy For Cloud Based Data Management In Health Network

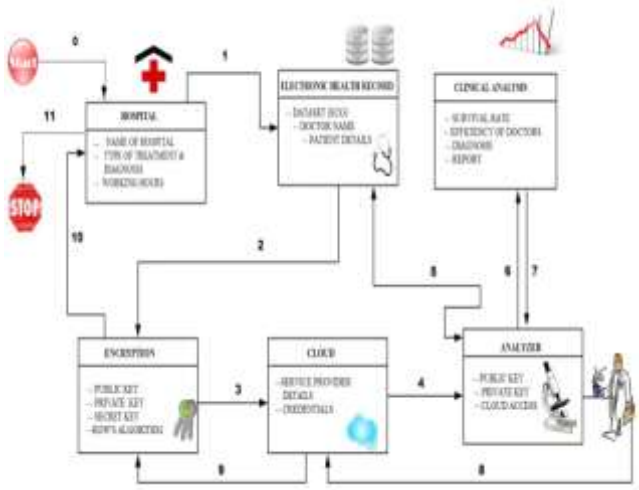
The advanced technology that support acceptance and affinity of health records in clouds lead to the reason of keeping watch over it for privacy concerns. The issues in security challenge can be solved by using cloud based services. In this system it has been proved that medical data management is done by employing combined security measures with a microservices method. Apart from the cloud services, the combination of current technology with cloud produces much more improvement in span of life and readiness therapeutic systems and makes them much more focused on the patients thereby marking down the costs imposed on the task for carrying out tasks and errors that occur in reports of the patients. To be valid and well accepted health care it has to possess proper security and privacy concerns.

## IV. IMPLEMENTATION

This section will act as a proof of concept for all that has been explained theoretically in this paper.The cloud use is google cloud, dataset chosen from UCI repository (ECG data),codes written using python language and statistical analysis (such as clinical data analysis and also time series ) has be computed via R programming. Visualization of the analysed data can be seen using tableau public.Fig 1.2 picturizes the flow of working and the expected parameters

Fig 1.2 Class diagram on various entities and their relation

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 3, March 2018



STEP 1: Firstly the dataset to be encrypted is loaded (be it from a local machine or remote data server/ repository such as UCI, kaggle etc) in cloud.

STEP 2:
In this stage , the serving end(such as hospital management ) gets to know the public key of the analyst using a third party authenticator or tries getting a symmetric key using diffie-hellman key exchange.Along with this key(the recently fetched analyst's key) the server(serving side) generates its own public and private key.

STEP 3:
The main ingredient of this spark is the newly proposed ROW's ALGORITHM.

**Mathematical Notations of ROW's algorithm**

$Zp \rightarrow \{2, 3 \ldots\ldots 128 \ldots\ldots 256\}$

$p \rightarrow \{1, 2, 3, 4 \ldots 11, 12 \cdots 22 \ldots\}$

$Zp \; != Zp+1 \; != Zp+2 \; != Zp+3 \; != \ldots\ldots\ldots Zp+n$

$\alpha \rightarrow Zp, Zp+1Z, \quad \beta \rightarrow Zp+2, Zp+3 \; Z \rightarrow Zp+11$

$\alpha 1 \rightarrow Zp, Zp+1, Zp+2, \quad \beta 1 \rightarrow Zp+2, Zp+3, Zp,$

$\lambda \kappa 1 \rightarrow ((Zp * Zp+1 + (Zp \; \%Zp+1) - Zp+2),$

$\lambda \kappa 2 \rightarrow ((Zp+2 * Zp+3 (Zp+2 \%Zp+3) - Zp)$

**PartiallyHomomorphic**

$P1 <= (Z\hat{} \; \lambda \kappa 1) \%(abs(ceil(Zp/Zp+2)) - E$

$P2 <= (Z\hat{} \; \lambda \kappa 2) \%(abs(ceil(Zp/Zp+2)) - D$

$P3 \Rightarrow (Z\hat{} - \lambda \kappa 2) \%(abs(ceil(Zp/Zp+2)) - E$

$P4 \Rightarrow (Z\hat{} - \lambda \kappa 1) \%(abs(ceil(Zp/Zp+2)) - D$

**Fully Homomorphic:**

$\lambda \kappa 3\text{-}e = ((\lambda \kappa 1 * Z) \% \alpha)) - E$ -------- $\lambda \kappa 3\text{-}d = ((\lambda \kappa 1 * Zp+1) \% \alpha)) - D$

$\lambda \kappa 4\text{-}e = ((\lambda \kappa 2 * Zp+3) \% \beta)) - E$------ $\lambda \kappa 3\text{-}d = ((\lambda \kappa 1 * Zp+4) \% \beta)) - D$

Notations:
Zp denotes public and private key, Z denotes common message α1,β1-lcm ,P1:P2 (Diffie Hellman Key Exchange), E-Encryption and D-Decryption.

STEP 4:

Now the encrypted content has been modified to a unique way that is a way which retains all the structural properties and operations it possessed before encryption .The encrypted data can now be stored in public clouds or can be shared to any individual or a group. Any kind of analyzation/ prediction can be done on this data.In general any kind of data such as data about financial, voting , defence technology, new bots in the market can be encrypted to the preferred form using this technique.Invalid users will not gain access to the dataset as the algorithm provides a provision to check authenticity of end user.

STEP 5:
The type of analyzation considered according to this paper is to understand the efficiency of cardiologists and hospitals based on surgeries performed annually. Considering parameters such as pericardial_effusion,wall_motion_score, survival ratio will determine the completeness and competence of doctors in services.

STEP 6:
The analyst retrieves the document by entering his private key.The relation between the public key will persist as that is immutable.The program to decrypt will be present in the

cloud as an executable file.The analyzer needs to run the program and would require the basic prerequisites which is free of cost. If the password/key is right then the analyst can download a copy of the dataset. After analysis the result will be uploaded in cloud and the report(text) will be hidden inside the resultant output.This is none other than steganography. The most important thing to be remembered is that the confidential data such as personal details will still be encrypted(double) and cannot be decrypted at any cost.The state of fact that decryption is not possible is because it has been encrypted using the serving side's/provider's public key as to decrypt it will require the private(private key will be known only to one individual)

## V. ANALYSIS ON ENCRYPTED DATA:

Analyzation can be done using various tools[1]. Out of which the authors here have chosen R programming. In R programming inbuilt packages such as HomomorpheR exist and that can be used on pallier programmed encryption data. So now in a case where we use ROW (algorithm) to encrypt and decrypt we cannot use the existing package, so we allow the non confidential data such as various ranges of the valve or wall motion score or even wall motion index to be accessed by the user using his credentials.Then the data can be striped column wise and predictions can be done.Predictions such as successful surgeries that will be occur, doctor wise comparisons and many more . Fig 1.3 show a sample predictive graph that describes the working strategy of a doctor.

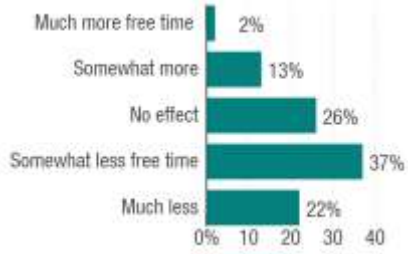



Fig 1.3 has been used for illustration only.It has been taken from google with no copyright issues.

## VI. OPEN ISSUES AND FUTURE WORK

As this project is testing stage(Final year project) time complexity can be assured.Space/Memory requirements are quite less as the data can be accessed from any remote server using
cloud.
It does not suffer from malleability as the hacker will not know one has used this partial ++ homomorphic technique.The
hacker might get irrelevant even if brute force unethical technique
is used .

Extension:
The project can further be extended like checking a person validity using fingerprints, iris/pupil tracker and many more.Using other real time datasets such as cancer ,tuberculosis,
cholera or any other disease one can perform enormous prediction that will help save a million lives . All these will add feathers to the cap by making the idea more powerful.

## VII. SUMMARY

A scintillating paper break opens traditional homomorphism and gives a new technique called as partial ++ homomorphic approach Where the most confidential data gets hidden and acts as black glove that acts as a translucent medium where one knows data exist but decrypting or bringing to equivalent form is unattainable. Even if gaps persist the data inside is impermissible.Thus the paper presented is to be an established and sought after project in the near future.

## VIII. REFERENCES

[1] Private Predictive Analysis On Encrypted Data Joppe W. Bos, Kristin Lauter, and Michael Naehrig

[2] Security And Privacy For Cloud Based Data Management In Health Network Christian Esposito, Aniello Castiglione, Constantin-Alexandru Tudorica

[3] Privacy-Preserving Patient-Centric Clinical Decision Support System on Na¨ıve Bayesian Classification Ximeng Liu, Student Member, IEEE, Rongxing Lu, Member, IEEE, Jianfeng Ma, Le Chen, and Baodong Qi