Predictive Analysis on Homomorphically Encrypted Medical Data

A. Dr. K.Anitha kumari[1], B. S.Kirthika [2]

[1] Associate Professor, Dept. of IT, PSG College of Technology, Coimbatore, India

[2]PG Scholar, Dept. of IT, PSG college of Technology, Coimbatore, India

Abstract- **Data security challenges faced by healthcare sector are increasing day by day. To ensure the security and privacy of data, fully homomorphic encryption schemes can be applied. To make the schemes suitable for applying in real time, light-weight state-of-art homomorphic encryption scheme like Gorti's Enhanced Homomorphic Cryptosystem (EHC) scheme is proposed. Predictive analysis is used for prediction of occurrence of diabetes in future. And to reduce the noise rate, modulus switching technique is proposed. Modulus switching technique manages noise by scaling the size of modulus. The depth of leveled computational circuits in the form of polynomial are predefined prior to the start of computation. The bound on length is known to the evaluator while the secret key is not known. The cipher text c modulo p is transformed in to a different cipher text modulo q. This transformation of cipher text leads to simple scaling and approximate rounding, thereby maintaining value of q sufficiently smaller that of p, noise can be reduced.**

Index terms- **Homomorphic encryption, Predictive analysis, encrypted medical data, Logistic regression, Gorti's Enhanced Homomorphic Cryptosystem (EHC)**

I.INTRODUCTION

Security has now become a primary requirement due to the rise in usage of the public cloud or internet to store the data [22]. Security is needed for ensuring the CIA (confidentiality, integrity, availability) of the information system resources. In order to perform any computation on the data that is encrypted and stored in database then the data has to be decrypted first to perform those operations but it raises many security concerns since the decrypted data are not considered to be safe, so there comes the idea of privacy homomorphism [23] which allows to perform computations directly on the encrypted data. Implicit additions and multiplications can be performed on the encrypted data using homomorphic encryption schemes [21]. There are actually two types of the cryptosystems namely public key cryptosystem and symmetric cryptosystem.

Homomorphic encryption is an encryption scheme that allows us to perform various operations like addition and multiplication on the encrypted data [24]. Homomorphic encryption schemes can be applied on any system by the use of different public key algorithms. Conventional encryption techniques ensures data privacy only in acquisition, storage phase but homomorphic encryption schemes allows us to perform computations directly on encrypted data. In order to process the data on the remote server and also to ensure the privacy and security of data, homomorphic encryption is used.

Homomorphic Encryption has proven to be a revolutionary innovation in healthcare world. However, in the year 2018, 15 million patient records were exposed in 503 healthcare data breaches. Moreover, healthcare industries are more prone to ransom attacks and other issues like hardware failure, patient record tampering or data corruption thus increasing the data security challenges in healthcare. Secure healthcare setup has become essential and there comes the idea of implementing Homomorphic encryption schemes on data which allows to perform operations on encrypted data ensuring privacy and security of data. Only authorized person can access thereby protecting identity of patient from outside sources. This enables secure storage, automates administrative process, secure transfer of information, and improves care for patients.

Data security challenges faced by healthcare sector are increasing day by day. Preserving Personal Health Information (PHI) requires ensuring data privacy at acquisition phase, storage phase and computation phase. Conventional encryption techniques ensure data privacy only in acquisition, storage, computational phase. In homomorphic encryption computations like addition and multiplication can be performed on encrypted data. This system can prove to be a revolution in the healthcare sector. Care can be personalized to each and every individual by making use of predictive analysis to make best decisions in healthcare.

Diabetes is a caused by the increase in level of blood glucose. It is a chronic disease that can result in worldwide health crisis. According to International Diabetes Federation, about 382 million people are affected by diabetes worldwide. By 2035, the number of patients affected by diabetes will be doubled thus resulting in 592 million diabetic patients. To diagnose diabetes many chemical and physical tests re available. However, prediction of diabetes in the earlier stage is challenging for medical practitioners because of the complex interdependence between various factors since diabetes affects different organs such as eye, kidney, nerves, heart, foot etc. Thus, in the proposed work diabetes prediction is included.

II. HOMOMORPHIC ENCRYPTION

The concept of homomorphic encryption preserves the data based on the properties of underlying algebraic “structures”.

Homomorphic encryption allows data manipulation without decrypting it. There have various practical use cases. From “changing” key used for encryption while the plain text is maintained as secret, doing arithmetic operations like addition, mixed addition, multiplication, mixed multiplication on encrypted data where the results can only be revealed once decrypted or search in encrypted data.

Homomorphic Encryption (HE) is an emerging scheme that allows untrusted parties to compute over encrypted data. With the advent of public key cryptography the researchers search for an encryption scheme which allows arbitrary operations like addition and multiplication which should be performed on the already encrypted data to preserve the integrity. With the use of this homomorphic encryption the computation can be performed over the already encrypted data by replacing the old key with a new key. A variety of optimizations have been recorded in the field of various encryption schemes only after the discovery of homomorphic encryption in the year 2009.

A. Types of Encryption Schemes

Encryption schemes are broadly classified into two types namely symmetric and asymmetric encryption schemes. In symmetric encryption scheme, the sender and the receiver agree on the key before establishment of the session. To communicate with different persons, different keys are generated. The requirement of large number of keys in the symmetric encryption scheme make their key generation management relatively complex. Symmetric schemes, being very fast, they are used in applications where speed of execution is a paramount requirement. In asymmetric encryption schemes every participant has a pair of keys termed as private and public. In a group of members the private key of a particular individual will be known only to that individual, whereas the public key will be known to everyone in that group. So in terms of security the asymmetric encryption schemes are considered to be more secure than the symmetric encryption schemes because of the two keys - public key and private key.

B. Types of Homomorphic Encryption

The different types of homomorphic encryptions are

1. Partially Homomorphic Encryption (PHE)
2. Somewhat Homomorphic Encryption (SWHE)
3. Fully Homomorphic Encryption (FHE).

Only one type of operation is allowed to be performed unlimited number of times is termed as partial homomorphic encryption. Some types of operations are allowed to be performed only a limited number of times is termed as somewhat homomorphic encryption. Fully HE allows an unlimited number of operations with unlimited number of times.

C. Fully Homomorphic Encryption

FHE is an emerging cryptographic technique to permit computation on encrypted data directly in the cloud without the need to bring the data back to the computational node. The use of fully homomorphic encryption algorithm for any application is very extensive mainly in the following 3 aspects,

1) Privacy protection: The user data is to be transmitted by cipher text form to the cloud of data storage, not only ensure the safety of data during transmission, but also ensure the security of data storage. Even the cloud computing service providers cannot easily obtain the plaintext information.

2) Data processing: Fully homomorphic encryption mechanism can make users or trusted third party to encrypt data directly by replacing its original data to get the processed data.
3) Ciphertext retrieval: ciphertext retrieval based on fully homomorphic encryption technology not only ensure researching privacy but also improve the retrieval efficiency and also it carries out the addition and multiplication operation on the retrieved data without altering the corresponding plaintext.

III. RELATED WORK

In [1], Craig Gentry, Shai Halevi and Nigel P. Smart has proposed to go from a somewhat homomorphic encryption scheme to fully homomorphic encryption scheme bootstrapping is used. Gentry introduced recryption which works by encrypting a cipher text (becomes doubly encrypted) and then removing inner encryption by homomorphically evaluating doubly encrypted plain text and the encrypted decryption key using decryption circuit. When a cipher text becomes too noisy the encoder can use SWHE to evaluate decryption function on cipher text, using encrypted private key that is the part of public key. So this re-encryption process encrypts the plain text again, that is less noisy. It is impractical because of the slow implementation, size of key and cipher text are too large.
In [2], Zvika Brakerski Weizmann, Craig Gentry, Vinod Vaikuntanathan has proposed a new way of constructing leveled fully homomorphic encryption schemes which is capable of evaluating arbitrary polynomial-size circuits, without using Gentry’s bootstrapping procedure that is based on the LWE. Applying known results on learning with error, the security of this scheme is based on the worst-case hardness of “short vector problems” on arbitrary lattices. The new scheme which is based on somewhat encryption scheme, allowed to perform any number of additions operations, but only one multiplication operation for the plain data. The main advantage of new scheme is encryption of the m × m size bit matrix at a time. The learning with error based fully homomorphic encryption scheme introduces a new dimension-modulus reduction technique, which shortens the cipher texts and also reduces the decryption complexity, without introducing additional assumptions.
In [3], Khalil Hariss, Maroun Chamoun and Abed Ellatif Samhat has proposed two important HE schemes are considered: DGHV and BV-BGV. DGHV is based on computing over real integers while BV-BGV is based on Lattice based Encryption. DGHV scheme is an asymmetric encryption scheme which provides homomorphic behavior for limited circuit depth but bootstrapping enables FHE and unlimited circuit depth. BGV scheme provides homomorphic behavior for limited circuit depth but using modulus switching enables unlimited circuit depth and FHE.A cipher text is partitioned into slots. Each slot can pack a multi-bit message. Packing multiple messages into one cipher text allows computing homomorphic operations in SIMD fashion. The expensive recrypt operation can also be eliminated by using the leveled version of the BGV scheme. In the leveled version of the BGV scheme, homomorphic operations are up to L levels can be performed. Each homomorphic addition and multiplication results in increase of noise in the ciphertext, so to reduce noise limited number of homomorphic operations can be done. Homomorphic addition doubles noise level whereas homomorphic multiplication roughly squares the noise amount. Thereby the L is determined by the depth of multiplication operations for the function to be evaluated. The level of the function to be computed can be stated beforehand and then during the key generation the parameters of the scheme can be adjusted. Practically impossible due to computation and storage overhead.
In [4], Craig Gentry and shai halevi has proposed FHE scheme that can perform arbitrary number of additions and multiplications homomorphically. It is based on ideal lattices. In Gentry’s FHE scheme, encryption is done by mapping a message to a lattice point and t a small random noise is added to create the final cipher text. The decryption can be done by using a good basis known only by the secret-key holder. Homomorphic addition and multiplication operations are performed by adding and multiplying lattice points respectively. It has several inefficiencies both in terms of storage and computation. Messages are encrypted bitwise and to increase the noise threshold the size of ciphertext must be large, which results expansion in storage space. The computation of homomorphic operations on large size ciphertexts are computationally

intensive and recryption operation cost is high thus making Gentry’s FHE scheme to be impractical.

In [5], Zhigang Chen, Jian Wang, Liqun Chen and Xinxia Song has proposed modulus switching technique to design and implement a FHE scheme and to choose concrete parameters. On one hand, they proposed a function of the lower bound of dimension value in the switching techniques depending on the LWE specific security levels. On the other hand, modified the Brakerski FHE scheme by using the modulus switching technique and also provides security analysis. Based on the analysis of result the modified FHE scheme is far more efficient than that of original Brakerski Scheme in the same security level.

In [6], Jan-Sebastien Coron, David Naccache and Mehdi Tibouchi used Public Key Compression to reduce the public key size of DGHV-like schemes by several orders of magnitude. Modulus Switching and Leveled DGHV Scheme is used. The noise ceiling in BGV framework does not increase exponentially rather it increases linearly in accordance with multiplicative depth. Thus a costly bootstrapping procedure is not essential to get FHE scheme. Improved Attack against the Approximate-GCD problem reduction of complexity.

In [7], Joppe W. Bos, Kristin Lauter, and Michael Naehrig have presented the implementation of a prediction service running in the cloud which is hosted on Microsoft’s Windows Azure. Input is taken as private encrypted health data, and as a result the probability of a patient to suffer from cardiovascular disease in encrypted form is given. Since homomorphic encryption is used in the cloud service, it predicts cardiovascular disease depending only on encrypted data, knowing nothing about submitted confidential medical data. They have also proposed a module for automated parameter selection which ensures security and correctness of results during evaluation of functions that are used in predictive analysis like Cox proportional hazard regression and logistic regression. They have also provided an overview of scenarios for private computation where functions that are prevalent in predictive analytics are relevant. Future work sheds light on increasing the scalability and improving the efficiency of the systems.

In [8], Marten van Dijk, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan proposed “somewhat homomorphic” encryption scheme .This scheme uses elementary modular arithmetic and then to convert it into a fully homomorphic scheme Gentry’s techniques are used. Rather than working with ideal lattices over a polynomial ring this scheme uses addition and multiplication over the integers which in turn improves the efficiency and also preserves the hardness of the approximate-gcd problem whereas the security of this scheme is compromised due to finding of approximate integer gcd.

In [9], Al – Mashhadi. H, and Ala'a A. K proposed an efficient hybrid homomorphic encryption technique for image encryption to ensure the safe exchange of private images in the public cloud based on the block pixel position. These three techniques solve the potential issues related to security and privacy because cloud systems are usually in public domain when the users upload and offload the data to the cloud using client devices. The proposed techniques constraints on elgamal and EHC. The EHC method is very efficient in terms of security and time because it takes the good characteristics of elgamal and so it provides very good security and small run time executions. The drawback is that huge resource and storage space is needed. In [29], Santhiya B and Anitha Kumari K analyzed DGHV and NTRU scheme elaborately.

In [10], Bahman p. Tabaei, William h. Hermanhas developed and validated an empirical equation to predict diabetes. They have developed this predictive equation using multiple logistic regression analysis. They have collected data from 1,032 Egyptian subjects with no prior history of diabetes. The equation incorporated sex, postprandial time, age, BMI, and glucose are taken as independent covariates to predict undiagnosed diabetes. They have validated the equation with the dataset collected from 1,065 American subjects. Comparison of performance with that of proposed and recommended static plasma glucose cut points for diabetes prediction.

IV. PROPOSED SYSTEM

The project aims to ensure privacy of healthcare data using homomorphic encryption scheme that allows performing operations on encrypted data and to reduce the noise rate by using modulus switching technique. Also prediction analysis is applied for future predictions of occurrence of diabetes.

Our proposed system provides a holistic solution to healthcare data security challenges thereby providing greater accessibility of patient data at any time and also ensures privacy of patient data.

- To ensure privacy and security of health care data using Fully Homomorphic Encryption (FHE) Schemes.
- To reduce the noise rate using modulus switching technique.
- To implement predictive analysis on healthcare data to predict occurrence of diabetes in patients.

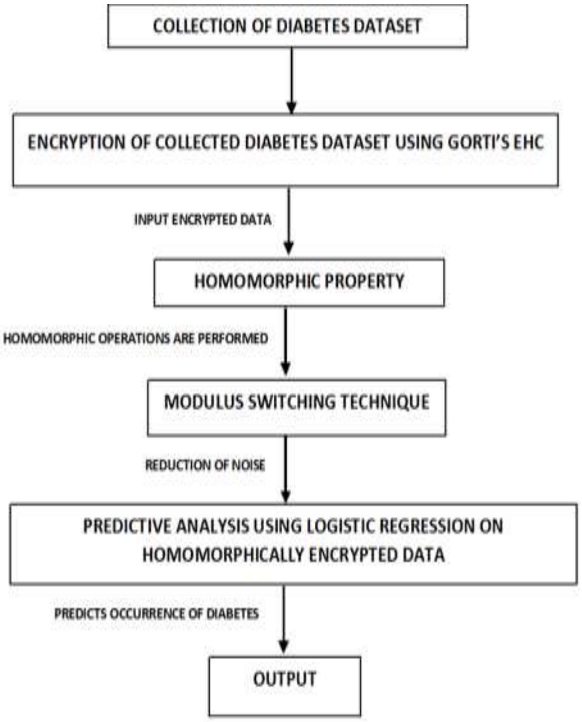
COLLECTION OF DIABETES DATASET
ENCRYPTION OF COLLECTED DIABETES DATASET USING GORTI'S EHC
INPUT ENCRYPTED DATA
HOMOMORPHIC PROPERTY
HOMOMORPHIC OPERATIONS ARE PERFORMED
MODULUS SWITCHING TECHNIQUE
REDUCTION OF NOISE
PREDICTIVE ANALYSIS USING LOGISTIC REGRESSION ON HOMOMORPHICALLY ENCRYPTED DATA
PREDICTS OCCURRENCE OF DIABETES
OUTPUT

Fig 1: System design

Fig 1 shows the system design.

- Dataset is taken from UCI ML Repository and certain parameters are chosen from the dataset and the values of the parameters are encrypted using Gorti's EHC Scheme.
- Once they are encrypted homomorphic operations are performed on the encrypted data.
- Modulus switching technique is used to reduce the noise emerged from the operations performed on encrypted data.
- Finally Logistic regression equation generated in accordance with the dataset are used to predict the occurrence of diabetes in patient.

V. GORTI'S ENHANCED HOMOMORPHIC CRYPTOSYSTEM (EHC)

In 2013, Gorti et al. proposed EHC that is a fully homomorphic public-key encryption scheme. It uses multiplication, addition, mixed multiplication and mixed addition over integers. The random private key is generated for every encryption process. During each encryption process same cipher text is not generated for same plain text, so that it would be difficult for the intruder to break the cipher text.

A. *Key Generation*

The first step of key generation process is to generate two large prime numbers 'p' and 'q' where p>q and then public key 'n' value is computed using the formula n = p*q.

B. *Encryption*

The first Input for the encryption process is message 'm' then a random number 'r' is generated that is kept as secret and finally the cipher text is computed using the formula,

$C = m + r * p^{q} \bmod n$ …………….. (1)

Where,

n– Public key,

p – Is a random integer that is kept secret,

q – Is a random integer that is kept secret,

m – Message,

r – Random parameter.

C. *Decryption*

In the decryption process, the original message can be retrieved from their corresponding cipher texts using their private keys

Decrypt (p, m) = c mod p……….. (2)

VI. PREDICTIVE ANALYSIS

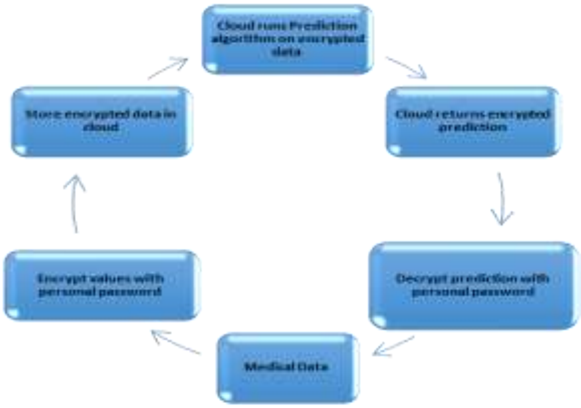
Cloud runs Prediction algorithm on encrypted data
Cloud returns encrypted prediction
Decrypt prediction with personal password
Medical Data
Encrypt values with personal password
Store encrypted data in cloud

Fig 2: Private computation on Medical data

Fig 2 shows an example scenario where private computation on medical data is desirable.

The medical data are collected and then encrypted using Gorti's EHC scheme. The encrypted data is then stored on cloud where the prediction algorithm is run on the encrypted medical data to predict diabetes. The predicted value is then returned. This value is then decrypted to learn about the likelihood of occurrence of diabetes.

In predictive analysis, various machine-learning techniques and statistical algorithms are applied on collected data, to predict the likelihood of future outcomes depending on past data. The goal of predictive analysis is to go beyond descriptive statistics and to report on what has happened in the past to provide a better assessment on what will happen in the future. The end result of predictive analysis is to refine decision making to produce better new insights that will lead to better actions.

Predictive models use known results to train a model that can then be used to predict values for new data. The modeling results in future predictions that represent probability of the target variable based on estimated significance from a set of input variables. This is far more different than that of diagnostic models that help you understand key relationships and determine why something happened or descriptive models that helps to understand what happened. Predictive analysis in healthcare uses various statistical methods and technology that was developed by many data scientists, and it gathers large amounts of data then, it uses techniques such as AI, and creates a prediction algorithm from past patients. That algorithm can be applied to a new patient, given that all the variables that exist in that particular individual's current and past medical history, lifestyle, etc.

A. Dataset and Parameter Description

The dataset used is taken from the National Institute of Diabetes and Digestive and Kidney Diseases (UCI ML Repository [25]). To predict if a patient has diabetes through diagnosis, diagnostic measurements from the dataset are used. The Pima Indian Diabetes (PID) dataset has diagnostic measurements of 768 female patients out of which 268 were positive instances about 34.9% and 500 were negative instances about 65.1% with 9 Class Attributes. The detailed description of all attributes is given in table 1

SNo	Parameter	Description
1	Skin Thickness (mm)	Fold Thickness of Skin
2	Insulin (mu U/mL)	Serum Insulin for 2 h
3	Blood Pressure (mmHg)	Diastolic Blood Pressure
4	Diabetes Pedigree Function	Diabetes pedigree Function
5	Pregnancies	Number of pregnancies
6	BMI (kg/m2)	Body Mass Index (weight/(height)^2)
7	Age	Age (years)
8	Glucose (mg/dl)	Glucose concentration in oral glucose tolerance test for 120 min
9	Outcome	Class variable (class value 0 for Negative and 1 for positive)

Table1: Parameter and Parameter description

The following features have been taken to predict whether a person is diabetic or not:

- Glucose: Concentration of plasma glucose over 2 hours (oral glucose tolerance test).
- BMI: Body mass index
- Age: Age (years)
- PT : Postprandial time
- Outcome: Class variable (1 if diabetic, 0 if non-diabetic).

B. Logistic Regression

Logistic Regression is a classification method. It is based on Linear Regression. Logistic Regression is a statistical analysis method that is used to predict a data value based on prior observations of a data set. In logistic regression model a prediction of a dependent data variable is made by analyzing relationship between already existing independent variables (one or more). Logistic regression multiplies each input by a coefficient, and then sums them up, and then adds a constant. In logistic regression, the output is actually the log of the odds ratio. In the of prediction of occurrence of diabetes, the odds ratio is the odds that diabetes will occur divided by the odds that it won't occur and then the log of this ratio is taken so that output is a continuous real number. This output doesn't make as much intuitive sense, but for some output y, following transformation can be applied:

(exp (y) / (1+exp(y))…………. .(3)

To get the probability of the event occurring (just reversing the log and the odds ratio here).

The result of a logistic regression is that for a given set of independent variables it gives a binary value 1 or 0 for a single dependent variable. To get a better model, then the independent variable values can be plugged for a new observation to predict if the value of dependent variable will be 0 or 1.

If a dataset has input variables and an output variable, then the relationship between the inputs and the output can be learnt by the machine learning algorithm. This learning helps the machine learning algorithm to predict the output for new set of inputs.

P= 1/ 1+ e-(b0+b1x1+b2x2+…..+bpxp)…………………... (4)

P= 1/ 1+ e-(-5.9316208) + (-0.04283968*AGE) + (0.09928878*GLUCOSE) + (-0.02214916*BMI) + (-0.83612044*PT)… (5)

- Intercept value : -5.9316208
- Co-efficient values
- AGE : -0.04283968
- GLUCOSE : 0.09928878
- BMI : -0.02214916
- PT : -0.83612044

The most essential part of a predictive modeling is the learning. When considering discrete outputs and one or more inputs, the learning is done through Maximum Likelihood Estimation. In the predicative modeling method, the Likelihood measure of various output classes is computed then it is used for estimating probability of each of the output class. The likelihood should not be confused with probability.

VII. MODULUS SWITCHING

Modulus switching was created by Brakerski and Vaikuntanathan. The primary thought of Modulus switching is utilized to downsize the cipher text after every increase, that outcome in another cipher text, this scaling procedure switches the value of first modulus to the new modulus value and furthermore diminishes the noise in the cipher text to the new noise in the new cipher text. By using this procedure, the total size of the new noise in the new cipher text really diminishes. Modulus switching subsequently can be utilized to oversee noise at the expense of relinquishing the size of modulus. A leveled FHE without bootstrapping can be accomplished by modulus switching. In this strategy, the profundity of leveled computational circuits is prearranged before the calculation begins. The profundity is introduced as a polynomial. For any prearranged polynomial indicated by, one can assess circuits of profundity via cautiously picking the stepping stool of diminishing modulus.

Modulus switching is a lightweight and incredible approach to oversee noise and one can effectively assess a number of arithmetic circuit with an arbitrary polynomial size without turning to bootstrapping. Bootstrapping implements slowly and, keys and cipher texts are large and, costly and complex so Modulus Switching technique is preferred over bootstrapping technique.

C’=n’/n * c mod n’ + l(s)…………… ….(6)

n’ – value relatively prime to n.

c- Cipher text

l(s) - Encryption noise.

Parameters	Encryption	Probability of decryption	Result
Age	67234.88616832	0.01	0
Glucose	67243.74452484		
BMI	67235.31337604		
PT	67231.81939775		
Intercept	67241.93162		

Table 2: Result of Sample Row Data.

Table 2 shows the result of Sample row data. It shows the results of encryption of a parameter values. Homomorphic operations are performed on these values and prediction equation based on logistic regression is used to predict the diabetes. This value is then decrypted and probability of decryption is calculated. Based on the probability of decryption value, result value shows whether the patient is diabetic or not (1 if diabetic, 0 if non-diabetic).

No of Medical Records	Computation time
500	2 secs

Table 3: Computation time

Table 3 shows the time required to encrypt, decrypt and also to calculate the probability of decryption to predict the occurrence of diabetes for about 500 medical records.

VIII. CONCLUSION AND FUTURE WORK

In the proposed system privacy and trust is ensured by Gorti's encryption scheme. Diabetes data are encrypted using EHC scheme. Modulus switching technique can be applied on the encrypted data to reduce noise. After the results are achieved, EHC ensures security of patient data against different attacks by allowing to perform prediction of occurrence of diabetes using logistic regression in future on encrypted data.

REFERENCES

[1] Gentry, Craig, Shai Halevi, and Nigel P. Smart. "Better bootstrapping in fully homomorphic encryption." International Workshop on Public Key Cryptography. Springer, Berlin, Heidelberg, 2012.

[2] Brakerski, Zvika, Craig Gentry, and Vinod Vaikuntanathan. "(Leveled) fully homomorphic encryption without bootstrapping." ACM Transactions on Computation Theory (TOCT) 6.3 (2014): 13.

[3] Hariss, Khalil, Maroun Chamoun, and Abed Ellatif Samhat. "On DGHV and BGV fully homomorphic encryption schemes." 2017 1st Cyber Security in Networking Conference (CSNet). IEEE, 2017.

[4] Gentry, Craig, and Shai Halevi. "Implementing gentry's fully-homomorphic encryption scheme." Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 2011.

[5] Chen, Zhigang, et al. "A Regev-type fully homomorphic encryption scheme using modulus switching." The Scientific World Journal 2014 (2014).

[6] Coron, Jean-Sébastien, David Naccache, and Mehdi Tibouchi. "Public key compression and modulus switching for fully homomorphic encryption over the integers." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2012.

[7] Bos, Joppe W., Kristin Lauter, and Michael Naehrig. "Private predictive analysis on encrypted medical data." Journal of biomedical informatics 50 (2014): 234-243.

[8] Van Dijk, Marten, et al. "Fully homomorphic encryption over the integers." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2010.

[9] Hybrid Homomorphic Cryptosystem for Secure Transfer of Color Image on Public Cloud Haider M. Al-Mashhadi and Ala'a A. Khalf, IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.3, March 2018.

[10] Tabaei, Bahman P., and William H. Herman. "A multivariate logistic regression equation to screen for diabetes: development and validation." Diabetes Care 25.11 (2002): 1999-2003.

[11] Yang, Jing, Mingyu Fan, Guangwei Wang, and Zhiyin Kong. "Simulation Study Based on Somewhat Homomorphic Encryption." Journal of Computer and Communications 2 (2014): 109.

[12] Tebaa, Maha, Saïd El Hajji, and Abdellatif El Ghazi. "Homomorphic encryption applied to the cloud computing security." In Proceedings of the World Congress on Engineering, vol. 1, pp. 4-6. 2012.

[13] Melchor, Carlos Aguilar, et al. "Improving Additive and Multiplicative Homomorphic Encryption Schemes Based on Worst-Case Hardness Assumptions}." IACR Cryptology ePrint Archive 2011 (2011): 607.

[14] Paillier, Pascal. "Public-key cryptosystems based on composite degree residuosity classes." In Advances in cryptology—EUROCRYPT'99, pp. 223-238. Springer Berlin Heidelberg, 1999.

[15] Sakurai, Kouichi, and Tsuyoshi Takagi. "On the security of a modified Paillier public-key primitive." Information Security and Privacy. Springer Berlin Heidelberg, 2002.

[16] El Gamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." In Advances in Cryptology, pp. 10-18. Springer Berlin Heidelberg, 1985.

[17] Taher elgamal, member, ―A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms‖, IEEE transactions on information theory, vol. it-31, no. 4, july 1985.

[18] Vaidehi, E. "Computing Aggregation Function Minimum/Maximum using Homomorphic Encryption Schemes in Wireless Sensor Networks (WSNs)." California State University, East Bay Hayward, CA, USA. (2007).

[19] Regev, Oded. "The learning with errors problem." In Blavatnik School of Computer Science, Tel Aviv University Invited survey in CCC (2010).

[20] Lyubashevsky, Vadim, Chris Peikert, and Oded Regev. "On ideal lattices and learning with errors over rings." Journal of the ACM (JACM) 60, no. 6 (2013): 43.

[21] Coron, Jean-Sébastien, Tancrede Lepoint, and Mehdi Tibouchi. "Practical multilinear maps over the integers." Advances in Cryptology–CRYPTO 2013. Springer Berlin Heidelberg, 2013. 476-493

[22] William, Stallings, and William Stallings. Cryptography and Network Security, 4/E. Pearson Education India, 2006.

[23] Lee, Hyungjick, Jim Alves-Foss, and Scott Harrison. "The use of encrypted functions for mobile agent security." In System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on, pp. 10pp. IEEE, 2004.

[24] Boneh, Dan, Eu-Jin Goh, and Kobbi Nissim. "Evaluating 2-DNF formulas on ciphertexts." In Theory of cryptography, pp. 325-341. Springer Berlin Heidelberg, 2005.

[25] Sigillito, V. I. N. C. E. N. T. "Pima indians diabetes database." UCI Machine Learning Repository, National Institute of Diabetes and Digestive and Kidney Diseases (1990).

[26] Joshi, Tejas & Pramila, M & Chawan, Pramila. (2018). LOGISTIC REGRESSION AND SVM BASED DIABETES PREDICTION SYSTEM. 5.

[27] Agarwal, Arushi, and Ankur Saxena. "Comparing Machine Learning Algorithms to Predict Diabetes in Women and Visualize Factors Affecting It." International Conference on Innovative Computing and Communications: Proceedings of ICICC 2019, Volume 1. Vol. 1087. Springer Nature, 2020.

[28] Alaya, Bechir, Lamri Laouamer, and Nihel Msilini. "Homomorphic encryption systems statement: Trends and challenges." Computer Science Review 36 (2020): 100235.

[29] B. Santhiya, K. Anitha Kumari, "Analysis on DGHV and NTRU Fully Homomorphic Encryption Schemes", Proceedings of International Conference on Artificial Intelligence, Smart Grid and Smart City Applications (AISGSC 2019), 669-678, 2020.

[30] Kocabas, Ovunc, and Tolga Soyata. "Towards privacy-preserving medical cloud computing using homomorphic encryption." Virtual and Mobile Healthcare: Breakthroughs in Research and Practice. IGI Global, 2020. 93-125.

BIOGRAPHY

Dr K Anitha Kumari is working as an Associate Professor in the Department of IT in PSG College of Technology, India. She is Highly Passionate and curious about Learning New stuff in Security Protocols. As an Independent Researcher, she had an Opportunity to present her UGC sponsored paper based on Quantum Cryptography in USA and visited a few Foreign Universities. To her credit, she had filed a PATENT and published around 55 Technical Papers in refereed and Impact Factored International/NationalJournals/Conferences published by Elsevier, Springer,T&F,Etc.,.Also, she's been an Active Reviewer for Prestigious Journals published by IEEE (IEEE Communications Surveys and Tutorials (IF: 20.230), IEEE Transactions on Industrial Informatics (IF: 5.43)), Springer, Wiley, etc.,and Technical Program Committee (TPC) for CECNet 2017, NGCT-2017 WICC-2018 and NCCI-2018 conferences. Her areas of interest include Cloud & IoT Security, Design and Analysis of Security Protocols, Attacks & Defense, Security in Computing, Bioinformatics, Cognitive Security, Quantum Cryptography, Web Service Security, Network Security and Analysis of Algorithms. Out of her research interest, she has contributed a Book chapter in T & F and delivered ample Guest Lectures. Her security project is sanctioned and granted by AICTE for a sum of Rs.11,80,000/-. She's been the mentor for Technovator Projects (2018 & 2014) and 'MEDROIDZ', an ICICI – Trinity 2014 funded project that was selected as one among the 6 projects in India. Academically, she has secured RANK-I and awarded Gold Medal in ME (SE) & in BE (CSE) from Anna University and from Avinashilingam University. She secured Elite+Gold Medal (Top 1%) in NPTEL – Cloud Computing course. She also won prizes in intra and inter institutional cultural events. As a Supervisor, she is currently guiding PhD scholars.