FULLY HOMOMORPHIC ENCRYPTION WITH ACTIVITY SLEEP MONITORING OF HEALTH RECORDS WITH DATA ANALYTICS

Nandakumar K[1],
Assistant Professor, Department of IT
SNS College of Engineering, Coimbatore,India.
nan24.kumar@gmail.com

Dr. P Sumathi[2],
Head of Department, Department of IT
SNS College of Engineering, Coimbatore,India.
psumathi.it@gmail.com

Vinothkumar.S[3],
UG Scholar, Department of IT
SNS College of Engineering, Coimbatore,India.
vinothkumar.sk12@gmail.com

C.S.Baveesh[4],
UG Scholar, Department of IT
SNS College of Engineering, Coimbatore,India.
baveethala@gmail.com

Soorya.m[4],
UG Scholar, Department of IT
SNS College of Engineering, Coimbatore,India.
Sooryaa.j8754@gmail.com

Surya Narayanan.S[6],
UG Scholar, Department of IT
SNS College of Engineering, Coimbatore,India.
suryanarayanan125@gmail.com

ABSTRACT

Sleep inadequate is a factor that causes chronic diseases such as diabetes, hypertension and producing hormones that are associated with hunger. When it comes to sleep disorders, there is no period called sleep deep enough. Sleep apnea is to stop breath duration sleep, resulting in brain arousal and desaturation (decrease oxygen in blood). In addition, it introduces other high-risk factors for stroke, coronary heart disease, and risk for dementia . Insomnia is more common in the elderly or in middle-aged people, with 30 to 40 percent of non-sleep.

The sharing of medical data and the analysis of that data across the different providers and clinical sites becomes essential. Concern of privacy and security of the data shared across the healthcare providers is very difficult to maintain. The analysis on the shared data causes patient's data at stake because the clinical data of the patients will be revealed around the providers that causes insecurity and any intruder can breach into the data. To overcome this issue, Homomorphic Encryption scheme can be applied to the medical data. The encrypted medical data can be shared among the providers, thus ensuring privacy and security.. The computation and the analysis are made on the encrypted data without revealing the original data to the providers using these schemes

Key words - Homomorphic techniques, Gorti's, Carmichael's, Analysis time, AHI stages.

I.INTRODUCTION

Sleep disordered breathing a very common disorder with prevalence rates of up to 49% in large epidemiological studies on subjects older than 40 years. A recent study showed that patients with sleep disordered breathing recruited by their number of apnea and hypopnea events alone, does improve sleepiness but does not improve overall cardiovascular mortality. Based on older large studies however it is known that sleep disordered breathing is a cardiovascular risk and that treatment lowers mortality and morbidity. These results appear to be contradictory. However, they might be explained if patient populations investigated are carefully reviewed further, and if sleep apnea severity metrics are reconsidered. According to this, it appears that studies speak of different populations. Whereas epidemiological studies use sampled subjects willing to participate, earlier studies used patients contacting a sleep center with complaints and symptoms. In this paper two studies are presented with an assessment of anatomical metrics for upper airway morphology in

order to derive parameters for better prediction. Different phenotypes can explain why some people benefit from treatment and others do not benefit equally.

Homomorphic Encryption is the emerging cryptographic techniques that allow computation on the encrypted data without converting to the plain text that provides privacy and security of the data similar to conventional encryption schemes. Homomorphic Encryption scheme performs both additive and multiplicative property. The providers can perform the computation and searching on the encrypted data. In addition, encrypted queries also executed on the encrypted data. Homomorphic Encryption is used in Genomics, Healthcare, National Security and Education. In addition, it is used in cloud service when outsource the data for computations.

II. PROBLEM STATEMENT

Sleep related breathing disorders were reported to have a prevalence of 2-4% in the first epidemiological studies. When looking at this study carefully it was a striking result that the number of apnea and hypopnea events was high and according to diagnostic criteria was above 5 events per hour of sleep in 24% of male and 9% of female subjects. Excessive daytime sleepiness was considered in addition to result in a 'reasonable' percentage of patients suffering from obstructive sleep apnea (OSA). A recent epidemiological study in Switzerland in a population randomly selected among inhabitants older than 40 years, a prevalence of OSA based on a diagnostic threshold of 15 apnea and hypopnea events per hour of sleep was found in 49% of people . The population was not very obese and did not show much sleepiness. With this high prevalence it is unlikely that all these subjects need treatment in order to reduce risk for cardiovascular consequences. Many large studies did show that sleep disordered breathing is a risk for cardiovascular disorders. Risk had been proven for hypertension, cardiac arrhythmia, arthrosclerosis, myocardial infarction, and stroke.

Today's world of digitalization, sensitive and confidential medical records are stored in data centers by healthcare providers across the world. The computation on the medical records can be carried out by third-party service providers. This increases concerns about security and privacy of the sensitive information. The sensitive patient's record must be kept confidential in the healthcare sector. The privacy of the data can be guaranteed, if it is encrypted by the owner of the record before uploading in any clinical sites or in data centers. Only the owner of the record can able to decrypt the data using the private key. This ensures privacy and the security of the data. But, according to the encryption schemes the computation cannot be carried out on the encrypted data, it requires the private key to decrypt the data . Providing private keys to the third-party service provider again results in privacy and security concern. In all the standard encryption schemes, arbitrary computations such as addition or multiplication cannot be carried out on the encrypted data.

` III.RELATED WORK

A. XGBoost Algorithm:

In this type of algorithm the implementation of gradient boosted decision trees has been made for better speed and performance. XGBClassifier has been imported from XGBoost package. By the use of this algorithm the accuracy of 64.5% for apple watch data and 63.65% for FitBit data have been observed.

B. SVM Kernel Algorithm:

SVM kernel is used especially for pattern analysis and converting any linear pattern to a nonlinear one. From sklearn.svm package, SVC has been imported.

The accuracy of Apple watch data is 63.5% and FitBit data are 62.8% for SVM Kernel algorithm.

C. KNN Algorithm:

This algorithm is the simplest one and is used for classifying new data points on the basis of similarity. From sklearn.neighbors package KNeighborsClassifier has been imported in the program and implemented.

The accuracy by using this algorithm are 65.8 % and 61.7 % for Apple watch data and Fitbit data respectively.

D.Accuracy Comparison:

Algorithms used Accuracy	**Apple Watch Dataset**	**FitBit Dataset**
Random Forest	71.39%	62.5%
XGBoost Algorithm	64.5%	63.65%
SVM Kernel	63.5%	62.8%
KNN	65.8%	61.7%

Results for 112 bit various ECC based encryption scheme

	Results for 112 bit	
Encryption schemes	**Time(milliseconds)**	**Cost (kilobytes)**
EC-OU	158	1115
EC-NS	90	1762
EC-P	156	3962
EC-EG	110	2433

E.Encryption protection safeguarding plan

The Encryption protection safeguarding plan for secure multiparty calculation utilizing ECC. Secure multiparty expansion have been actualized for protection safeguarding information mining utilizing Secret sharing and holomorphic encryption .Yet in this methodology traditional public key encryption plot is utilized with the goal that it is computationally costly.

Further numerous figure task at each site expanded the calculation cost .The secret S sharing based methodology proposed in is effective as far as computational expense yet here correspondence cost is high because of message trade .we center around holomorphic encryption based ECC approach . We accept correspondence between gatherings in ring topology where each gathering can speak with the following party in a ring. Consider the three party situation with gatherings A, B and C and its private value m1,m2 and m3 individually and need to perform joint calculation. Gatherings need to register m1+m2+m3 safely. The convention begins with the gathering appointed as initiator party in the ring. In actuality any gathering go about as an initiator party .here we accept that the main party as an initiator .The Initiator initially encodes its private value utilizing ECC based encryption calculation .The resultant figure is sent to the following party in the ring .Next Gathering does not play out any figure activity but rather simply include its very own mapped esteem or its private esteem which is mapped on elliptic curve with the received cipher text .this process repeated until all the values are not received by initiator means (E(m1)+m2+m3).After getting the message from each party initiator decrypt the message and compue (m1+m2+m3).Now the initiator sends the result or broadcast the result to all related parties.

IV.IMPLEMENTATION AND RESULTS

A.HOMO-MORPHIC SCHEME

The Gorti's Enhanced Homomorphic Cryptosystem(ECH) is a encryption scheme that allows to perform on the encrypted data as the operations are performed on the plaintext format,and then the results are fetched that will be decrypted using the gorti's enhanced decryption algorithm. The scheme mainly focuses on addition ,multiplication and mixed operations The scheme is strong as the secret keys are used which is difficult to find ,this scheme is very faster and requires less memory.Gorti's scheme is more secure to perform,increased security due to medical data privacy concerns.

The carmichael's function is vital performing in cryptography system, it's a security performance algorithm, due to its use in the RSA encryption algorithm. The scheme is used for security of the data transmission. The encryption key is the public key and the decryption key is the secret key which is kept private. The key is secretly published by any two prime numbers along with the values. This can be regenerated only by someone who known as the prime secret key.(FIG 3.1)

B. ElGamal algorithm

ElGamal: ElGamal algorithm was introduced in 1985 by Taher ElGamal . ElGamal is an asymmetric key encryption algorithm that is based on the Diffie-Helman key exchange as an alternative to RSA for public key encryption. ElGamal is also used in digital signature generation algorithm called ElGamal signature scheme. A homomorphic algorithm named paillier used for its semantic security.

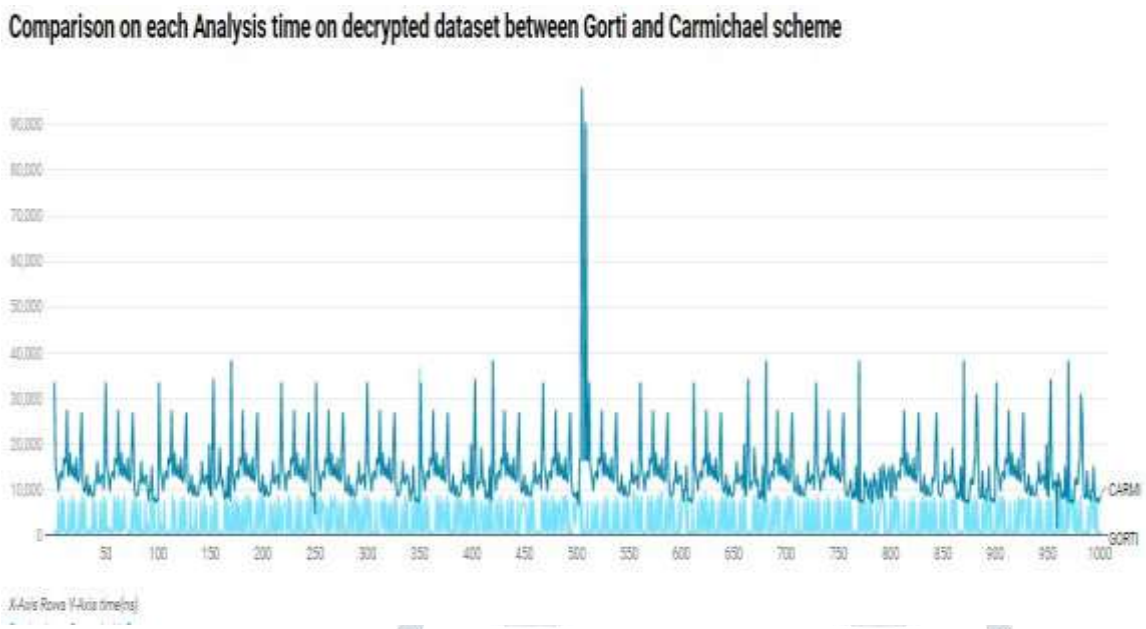

Fig. 1: comparison analysis of decryption schemes

The computational time comparison, taken in nanoseconds, of each row analysis time on the encrypted dataset of Gorti's scheme

VI. CONCLUSION

In the work the user security serves as a major threat during data processing and analysis. Adoption of homomorphic encryption schemes such as the Gorti encryption scheme and Carmichael's encryption scheme eliminates this threat, by processing data and computation in encrypted values. Client's security stays a significant test, as the specialist organization can without much of stretch access the client's information. It has been indicated that completely homomorphic encryption plans may be the ideal arrangement, as it permits one gathering to process the client's information homomorphically, without the need of knowing the corresponding mystery keys. The encryption conspire is made sure against assaults, for example, plaintext recuperation assault like picked plaintext assault and known-plaintext.

REFERENCE

[1] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Advances in Cryptology (EUROCRYPT '99), vol. 1592 of Lecture Notes in Computer Science, pp. 223–238, Springer, New York, NY, USA, 1999."

[2] C. Gentry, "Fully homomorphic encryption using ideal lattices",Symposium on the Theory of Computing (STOC), 2009, pp. 169-178

[3] Craig Gentry and ShaiHalevi, "Implementing Gentry's fullyhomomorphic encryption scheme," Advances in Cryptology–EUROCRYPT 2011, pp. 129– 148, 2011.

[4] Van Dijk, Marten, Craig Gentry, ShaiHalevi, and VinodVaikuntanathan. "Fully homomorphic encryption over the Integers". Advances in Cryptology EUROCRYPT 2010 (2010):24-4

[5] Yu Yu, JussipekkaLeiwo, Benjamin Premkumar, "A Study on the Security of Privacy Homomorphism", Nanyangchnological University, School of Computer Engineering, Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06), IEEE 200

[6] J. Marcos, R. Hornero, D. Alvarez, F. Campo and Miguel Lopez, "Applying Neural Network Classifiers in the Diagnosis of the Obstructive Sleep Apnea Syndrome from Nocturnal Pulse Oximetric Recordings," in Proceedings of the 29th IEEE International Conference on Engineering in Medicine and Biology Society (EMBS 2007), pp. 5174-5177, Aug. 2007.

[7] Khandoker A.H., Gubbi J., Palaniswami M. "Automated Scoring of Obstructive Sleep Apnea and Hypopnea Events Using Short-Term Electrocardiogram Recordings". IEEE Trans. Inf. Technol. Biomed. 2009;13:1057–1067. doi: 10.1109/TITB.2009.2031639.Page(s): 1057 – 1067,INSPEC Accession Number: 10957723.

[8] L. Almazaydeh, M. Faezipour, and K. Elleithy, "A Neural Network System For Detection Of Obstructive Sleep Apnea Through SpO_2 Signal Features", (IJACSA) *International Journal of Advanced Computer Science and Applications*, vol. 3, no. 5, pp. 7-11, Jun. 2012.

[9] L. Almazaydeh, K. Elleithy, and M. Faezipour, "Detection of obstructive sleep apnea through ECG signal features", in *Proceedings of the IEEE International Conference on Electro Information Technology (IEEE eit2012), pp. 1*-6, May. 2012.

[10] M. Canosa, E. Hernandez, and V. More, "Intelligent Diagnosis of Sleep Apnea Syndrome," In IEEE Engineering in Medicine and Biology Magazine., vol. 23, no. 2, pp. 72–81, 2004.