European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 07, 2020

Secure Privacy Preserving Schema Using ECC By Holomorphic Algorithm for BAN and Data Storage in Cloud

G Prasanna[1], Dr.K.Ramesh Reddy[2], Y. Sreevaishnavi[3]

[1,3]Research Scholar, [2]Assistant Professor

[1,2]Department of Computer Science, 3Department of ECE

[1,2]VikramaSimhapuri University, Nellore, 3SV University, Triupati

Abstract--We can simply define the wireless networks as 'the system networks which are not interlinked by any cables'. Wireless network is a dynamic one both in the growth of productivity and be supportive in data transferring. The health status of a patient is submitted to a remote medical server via a portable digital assistance or cell phone may be tracked remotely by doctors. WBAN will help users to store their gathered information on their PDA (Personal Digital Assistant) or any other mobile computers and then pass that information to an appropriate server/computer. Medical data protection is a major subject in contemporary world. We proposed a new algorithm for encrypting and decrypting the ECG data using Holomorpic Algorithm through cloud services. ECC algorithm is used to generate the key for encryption process.

Key words— ECG data, Holomorpic and ECC algorithm, WBAN, Wireless Network.

1. INTRODUCTION

Mostly with the development of wireless communications and semi-conductor innovations, the field of sensor networks has expanded substantially to serve a variety of applications, particularly in medical and healthcare systems. A Wireless Body Area Network (WBAN) is a specially modified area network aims to enable different medical devices and sensors within and outside a human body autonomously. Compared to the existing electronic healthcare tracking systems, a WBAN may deliver two substantial benefits. The first benefit is patient mobility due to the use of portable surveillance unit. The second benefit is the independent location tracking service. As an autonomous computer, a WBAN node can check for and find an appropriate communication network to transfer data for processing to a remote database server. A WBAN can also access internet to transfer data in a nondestructive way. WBAN will help users to store their gathered information on their PDA (Personal Digital Assistant) or any other mobile computers and then pass that information to an appropriate server/computer. A WBAN is made up of multiple small sensor nodes and Gateway nodes to connect the remote database system. The sensor node could be connected to a variety of telecommunication networks by the Gateway node. Those contact networks may be either a

regular telecommunications network, a cell telephone network, a specialized emergency center / hospital network or a public Wi-Fi hotspot.

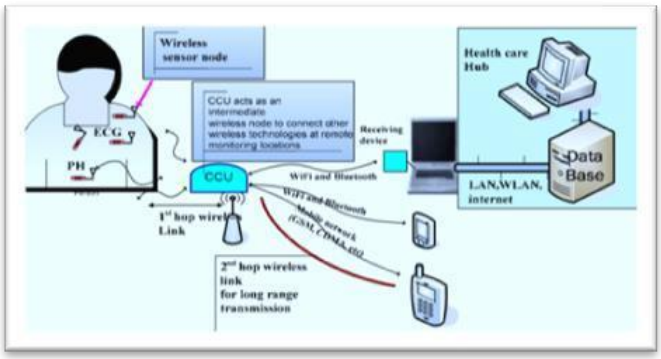

Fig. 1. A communication architecture of a typical WBAN health monitoring structure

The above WBAN system, Collection and tracking of data through the Gateway from individual wireless senor nodes from a single human body.WBAN includes different challenges like energy needs, WBAN stability, accessibility support, quality of service, connectivity problems. Hence, here we used holomorphic encryption algorithm. Holomorphic encryption can be used to maintain external storage and resources for protection.

2. RELATED WORKS

Author, Cheon et al [1] presented the very first aggregate signature based on identity in 2004. Other certificate less aggregate signature (CL-AS) schemes were suggested shortly afterwards. Because of the resistance of Certificate less Public Key Cryptosystem (CL-PKC) to the key escrow issue in ID-based Public Key Cryptosystem (ID-PKC). Authors, H. Liu, M. Liang, and H. Sun suggested [2] a CL-AS method that needs just four aggregate authentication matching algorithms and two signature size group items, but it declines to provide unforgettable details. Later some authors proposed an effective CL-AS scheme with enhanced efficiency than the previous approaches. Based on an improved/effective CL-AS algorithm, Author [3] put together an efficient verifiable data aggregation system for IoT situations, called VDAS, which essentially decreases the computing overlap in IoT data center. Under dynamically selected messages, the device is proven safe from universal forgery.

In [4] author proposes an effective and interactive search method that not only promotes effective multi-keyword search, but also automatic elimination and integration of records and proposed a "Greedy Depth-first Search" method to improve greater effectiveness. In addition, the parallel search process may be carried out more to minimize the time factor. The protection of the device is secured by two threat models against using KNN stable method. The system administrator is responsible for building and submitting information to the cloud server to be updated. The system administrator must then store the un-encrypted index tree and the information required for the IDF parameters to be recalculated.

In this article [5], author addressed the challenging multi-keyword fuzzy search issue over the encrypted files. We implemented and incorporated many groundbreaking concepts to

address the multiple keywords search and the fuzzy search problems concurrently with high performance. The above-mentioned works takes more execution time, gives more throughput and packet delivery ratio. To get more details refer section III to get information about implementation, section IV for results and discussions, section V for conclusion and section VI for references.

3. IMPLEMENTATION

The implementation procedure of this model is shown in figure 2. The block diagram consists of two inputs which are called as input 1 and input 2. One is conversion of signals like EEG/ECG into values of integers and other is generation of 128 bit key from ECC.

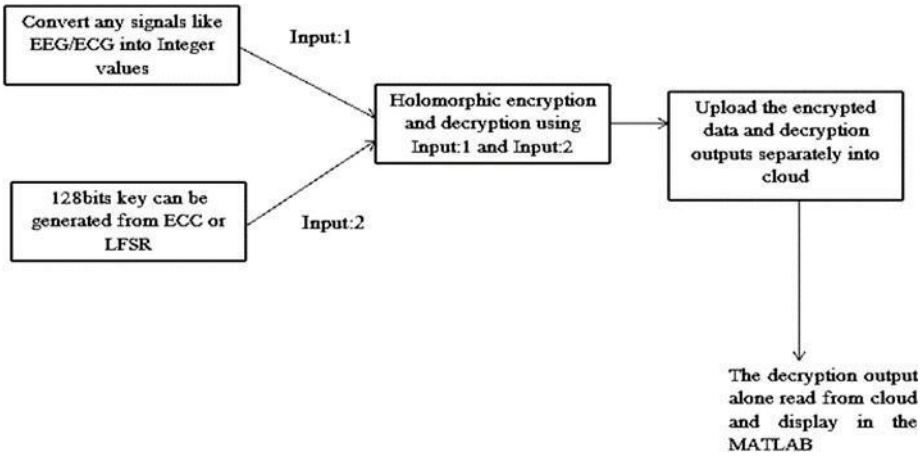

Fig 2. Block diagram of our system

The algorithm of Homomorphic for encryption and decryption of data is applied on both of inputs 1 and 2. and then we need to upload the outcome of previous block into cloud server. The above process of decryption, we need to download the data from cloud server and decryption method is performed in reverse process. The key goal of the proposed approach is to use Homomorphic algorithms to maintain secure encryption and decryption. The detailed description of our proposed methodology is given below:

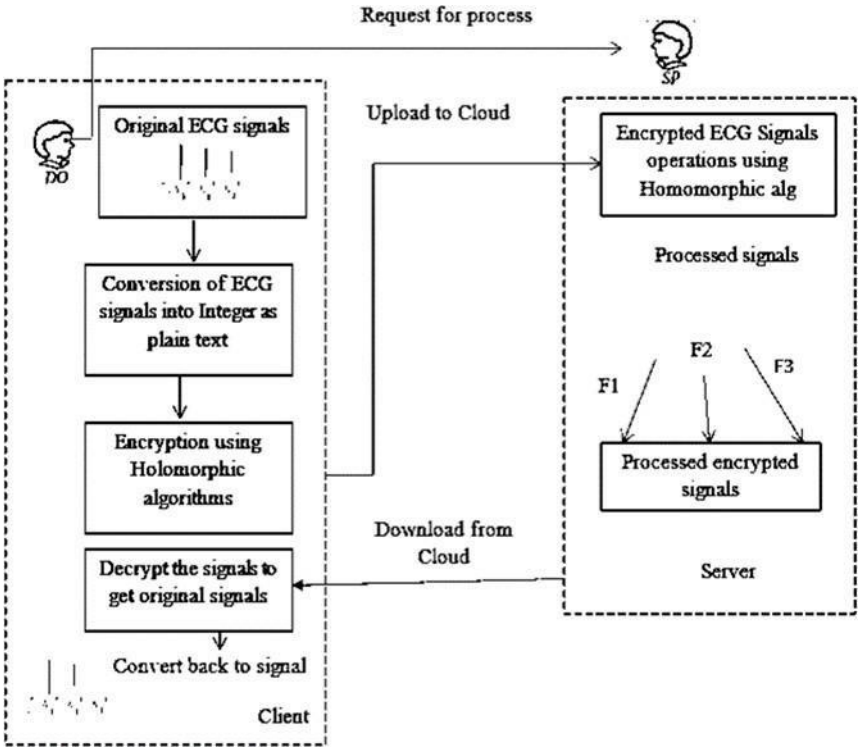

Fig 3. Structure of proposed model in detail.

It has multiple process stages, those are: first we need to build an account in a cloud using personally identifiable information including the hidden key. Mostly with help of IDs and credentials, the data is stored in the cloud through various channels. The ECG signal or text is extracted in this operation then the data is translated to ordinary integer data. With the help of Holomorphic operations, these data/values are encrypted.

In the article [5], Rivest, Adleman and Dertouzos first suggested the definition of homomorphism in 1978.Homomorphic encryption is the encryption method that enables the encryption key to be used without the decryption function being identified. There are typically four algorithms in a homomorphic encryption scheme: KeyGen, Encrypt, Decrypt, and Evaluate. We can conceptually define the four functions as obeys, according to the concept of homomorphic encryption:

KeyGen, this includes a security factor s and creates a private key pk and a public key bk
KeyGen(s) → (pk, bk).

Encrypt, it uses as inputs public key pk and a plain-text t, and generates a cipher text ci of t
Encrypt (t, pk) → ci

In things peak server, the encrypted chipper data is inserted/uploaded. The things peak server stuff is the cloud ecosystem in which we can build new channels where we can insert

the data of our choosing. Then the data is retrieved from the things peak channel at the receiving end and data is decrypted through using procedure as described in the following:

Decrypt, it takes as inputs the private key pk and ci, and generates the plaintext t of ci.
Decrypt (ci, pk) → t

Evaluate, it uses the inputs public key b_k, circuit C and a cipher text sequence (t1, t2, · · · t_n) and generates the encrypted output ci.
Decrypt (pk, ci1, ci2, ci3…cin) = f (t1, t2...t_n) Here, f is the feature/functionality that we want to execute.

In order to have the same degree of cryptographic stability, ECC needs one sixth of the computation complexity. The key is generated using the methods point addition and point doubling and considered those points are in Elliptic curve. The standard/normal form of elliptic curve can be expressed as:

2
$$b = a^3 - za - yb \quad \ldots (1)$$

For certain constant values for y and z parameters. This model is often referred to as the typical equation of Weierstrass 0. Parameters y and z have to fulfill the condition:

2
$$4z^3 + 27y \neq 0$$

Assume that we have a set of points on a plane (ai, bi). The set is indeed very large, although it's finite. We are going to represent this set by F.

Point Addition:

The group operator would enable us tomeasure the third point $C\ (a_r, b_r)$, also in set F, for the two points $A\ (a_p, b_p)$, $B\ (a_q, b_q)(A \neq \pm B)$ in set F, so that (adding).The following interactions are then valid.

$$A + B = C$$
$$b - b_p = t\,(a - a_p) \ldots (2)$$

2 3

$$b_p = a_p - za - y \quad \ldots (3)$$

$$b_q\ 2 = a_r^3 - za - y \quad \ldots (4)$$

$$b_r\ 2 = a_r^2 - za - y \quad \ldots (4)$$

The slope of the line between A and B is t. From equation (3) and (4), we get:

( )(b_p+b_q)=(- q_x)(b_q^2+ q+ ^{2})$a_{\overline{p}}$ $zd\left(a_p a_{\overline{p}}\ a_q a_p\right) a\quad a_q$ (6)

From equations (3) and (5), we get:

$$b_r - b_p)\,(b_r + b_p) = (a_r - a_p)\,(a_r^2 + a_r a_p + a_p^2) - z\,(a_r - a_p) \ldots (7)$$

Divide equation (6) and (7) by (ap-aq) & (ar-ap) respectively. The above equation (6) and & (7) will get:

$$t\,(b_p + b_q) = (a_p - a_q)^2 - a_p a_q - z \ldots (8)$$

$$t\,(b_r + b_p) = (a_r - a_p)^2 - a_r a_p - z \ldots (9)$$

Subtracting the equations (8) – (9), we get:

$$t\,(b_q - b_r) = (2a_p + a_p + a_q)\,(a_q - a_r) - a_p\,(a_q - a_r) \ldots (10)$$

Dividing the equation (10)by $(a_q - a_r)$; we get:

$$t^2 = 2a_p + a_q + a_r - a_q \ldots (11)$$

With the help of equation (11), we will find:

$$a_r = t^2 - a_p - a_q \ldots (12)$$

Here, C ∈ straight line(AB)then

$t = (b_r - b_p) / (a_r - a_p)$, then we will get:

$$b_r = b_p + t\,(b_r - b_p) \ldots (13)$$

The coordinates of point C are equations (12) and (13).

Point Doubling:

The group operator willhelp to measure the third point $C\,(a_r, b_r)$for the given point $A\,(a_p, b_p)$in set F, sothat

. $A + A = 2A = C$

Dividing the equation (6) with $(a_r - a_p)$,we get:

$$t\,(b_r + b_q) = a_r^2 + a_r a_p + a_p^2 - z \ldots (14)$$

Weknow that$t = b'(a_p)$&$b' = (3a^2 - z) / 2\sqrt{(a^3 - za - y)}$then

$$b'(a_p) = \frac{3a_p^2 - z}{2b_p} \ldots (15)$$

As weknowthat then $t = \frac{3a_p^2 - z}{2b_p} \ldots (16)$We can findthat:

$$t = b'(a_p)$$

$$\&\frac{b_r - b_p}{a_r - a_p} = t \ldots (17) \quad -z = 2tb_p - 3a_p^2$$

From the above equation, we can get:

$$b_r = b_p + t(a_r - a_p) \ldots (18)$$

Substituting equations (17) and (18) in equation (14), we get:

$$t(2b_p) + t(a_r - a_p)) = a_r^2 + a_r a_p + a_p^2 + 2tb_p - 3a_p^2 \ldots (19)$$

From these equations, we can obtain quadratic equation:

$$E = (3a_p - t^2)^2$$

$$a_r^2 + (a_p - t^2)a_r + t^2 a_p - 2a_p^2 = 0 \ldots (20)$$

Its discriminate is:

Then the solutions are:

$$\& \quad a_r = t^2 - 2a_p \quad a_r = a_p(that\ rejects) \ldots (21)$$

From equations (13) & (21), wecan b_r

$$C = A + A$$

The principle is that when the calculations are performed in modulo p, above mentioned formulas remain the same. Thus, we will find elliptic curves over the finite field I_p, where p is odd prime p.

4. RESULTS AND DISCUSSIONS

When it comes to execution part, the inputs are of two types. One is in the form of text and another is in the form of a signal. Let's discuss about one by one. For the ECG signal, the input is given as 1 and for text as 2. The input is selected from our selection. Let us take the input as 2: Then the outcomes will be derived as described in the following:

Input text: INDIA IS MY COUNTRY Encrypted Output: 6

Here, the input is a text which shown in Input text phase. Basically, encryption means transformation of data into an interpreted format from a compact form that could only be translated or analyzed after it has been decrypted. Here, encrypted data is shown in Encrypted output phase. As follows, the encrypted information is converted into integer values.

Encrypted Cipher as integer:

14237 31800 17599 11561 19295 28819 7118 1151522372

The information is then submitted to the cloud server, as seenbelow:

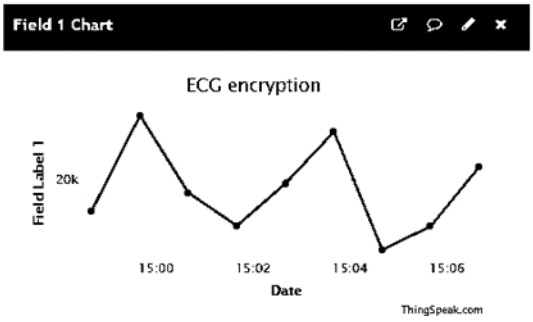

Fig 4. Encryption of text data into Thing Speak Server

Up-to now the encryption process is completed. When we want to decrypt the data, first we need to download the data from Thing Speak Server through our credentials. The decryption process are as follows:

Decrypted Output: INDIA IS MY COUNTRY

The Throughput is an exact indicator of how much data is transmitted efficiently from origin to destination. The Throughput of our suggested approach for single text data is given below:

Throughput rate (in Gbps): 3.1600

The strength that is calculated when a normal test signal is tested at a given point in a telecommunications device is known as Transmission Level. Generally, the transmission level is specified in dBm. The general mathematical sense of accuracy measurement applies to the closeness of computations or calculations to the exact or accurate values.

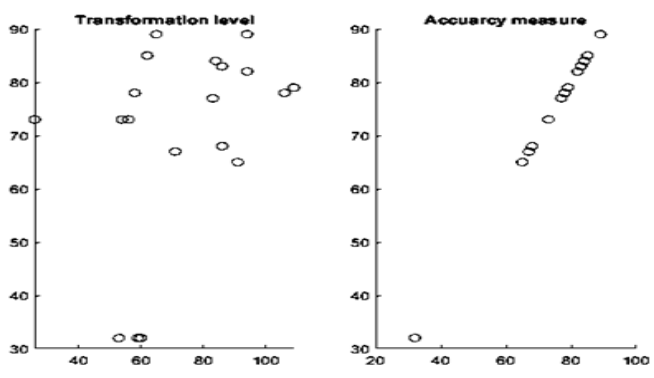

Fig 5. Measurements of Transmission levels & Accuracy

If the user selects input as 1, then the input for our model is treated as signal. The below shown figure is the selectors signal input.

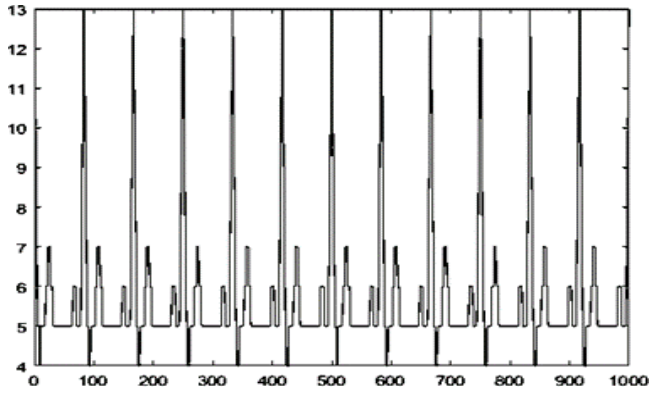

Fig 6. ECG signal is given as input

For the above input signal, the encrypted cipher text will be as: Encrypted Output: mW▫hE_▫▫

```
Encrypted Cipher text
楊帴▫丁
     1     1     0     0
     1     0     1     0
     1     0     0     1
     0     1     1     1
     0     1     1     0
```

Encrypted Cipher as integer:

27101 24121 9825 29805

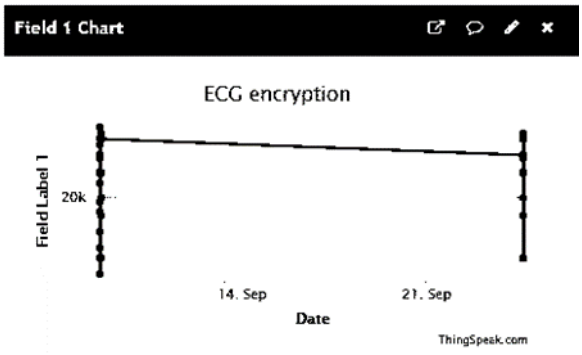

Fig 7. Encryption of ECG signal into Thing Speak Server

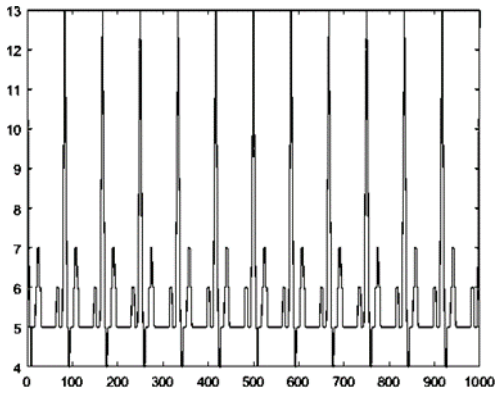

Fig 8. Decrypted Output

The Throughput of our suggested approach for single text data is given below:

Throughput rate (in Gbps): 0.3401

Table 1: Comparison between Existing and Proposed Models

Parameter	Proposed	Existing
Execution time	230ms	424ms
Throughput	0.2866 GHz	0.193 GHz
Packet Delivery Ratio (PDR)	451MHz	492MHz

The proposed system compared with the parameters like Execution time, Throughput and PDR. All the above parameters it gives the remarkable results. The resulted parameter values are Execution time is 230 ms instead of 424 ms, the Throughput is 0.2866 GHz instead of 0.193 GHz and the PDR is 451 MHz instead of 492 MHz.

5. CONCLUSION

For improved security protection, the proposed approach using Holomorphic encryption and decryption systems. This approach uses the ECC encryption framework for key generation and scalable data sharing, where we used cloud integration using Thing Speak server material. Compared to state-of-the-art approaches, this approach produces decent performance. The proposed system compares with the existing system all parameters like Execution Time, Throughput and PDR are efficient. The proposed system is better than the available system.

6. REFERENCES

[1] J. Cheon, Y. Kim and H. Yoon, "A New ID-Based Signature with Batch Verification", Report 2004/131, 2004

[2] H. Liu, M. Liang, and H. Sun, "A secure and efficient certificateless aggregate signature scheme", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E97-A, no.4, pp. 45-56, 2014

[3] Jingwei Liu, Jinping Han, Longfei Wu, Rong Sun and Xiaojiang Du, "VDAS: Verifiable Data Aggregation Scheme for Internet of Things", 2017 IEEE International Conference on Communications (ICC), 978-1-4673-8999- 0

[4] Xia, Z.et al.: A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. IEEE Trans. Parallel Distrib. Syst. 27, 340–352 (2016)

[5] R. Rivest, L. Adleman, and M Dertouzos, "On data banks and privacy homomorphisms", in Foundations of Secure Computation, pp. 169–177, Academic Press, 1978.

[6] Jamil. Y. Khan and Mehmet R. Yuce, "Wireless Body Area Network (WBAN) for Medical Applications", New Developments in Biomedical Engineering. https://cdn.intechopen.com/pdfs/9103/InTech-Wireless_body_area_network_wban_for_medical_applications.pdf

[7] Dragan Vidakovic2, Dusko Parezanovic2 and Jelena Kaljevic, "Addition and doubling of points", Journal of Theoretical Physics and Cryptography.

[8] Roger A. Hallman, Mamadou H. Diallo, Michael A. August and Christopher T. Graves, "Homomorphic Encryption for Secure Computation on Big Data", 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), pages 340-347

[9] TianyingXieandYantao Li, "Efficient Integer Vector Homomorphic Encryption Using Deep Learning for Neural Networks", Springer Nature Switzerland AG 2018

[10] Pan Yang, XiaolinGui, Jian An, and Feng Tian, "An Efficient Secret Key Homomorphic Encryption Used in Image Processing Service", Hindawi Security and Communication Networks Volume 2017, Article ID 7695751