Asian Journal of Applied Science and Technology (AJAST)
Volume 1, Issue 5, Pages 142-146, June 2017

Elliptic Curve Cryptography Based Security Enhancement for Wireless Body Area Network System

E.Pavithra[1], F.Anishya[2] and M.Nivetha Kumari[3]

[1]*Department of Information Technology, IFET College of Engineering, Villupuram, Tamilnadu, India.*
[2]*Department of Information Technology, IFET College of Engineering, Villupuram, Tamilnadu, India.*
[3]*Department of Information Technology, IFET College of Engineering, Villupuram, Tamilnadu, India.*

Article Received: 01 June 2017 *Article Accepted: 15 June 2017* *Article Published: 18 June 2017*

ABSTRACT

The aim is to provide the enhanced security mechanism and also it discusses the privacy issues in healthcare application using wireless medical sensor networks. The paper describes the basic idea of Elliptic Curve Cryptography and its implementation through the technique co-ordinate geometry for data encryption for the user. Elliptic curve cryptography is a process of the asymmetric key cryptography. It includes the two types the first consider that key (i) public key generation on the elliptic curve and its declaration for data encryption algorithm and (ii) private key generation and its use in data decryption depended on the points on two dimensional elliptical curve point. We also discuss the implementation of elliptic curve on two finite fields, first one is a prime field and another one is a binary field. In existing system they have using the universal key for the data which we are sending to the server. The major problem of this system server can decrypt the message to send by the user. In my proposed system the main server forward the message and receiver without decryption then applying the elliptic curve cryptography this algorithm every time generates the new key.

Keywords: Cryptography, Elliptic Curves, ECC, Keys, Field, Encryption, Decryption, Public and Private.

1. INTRODUCTION

Now a day's Elliptic Curve Cryptography is a newer approach, and considered as a marvelous technique and security enhancement with low key size encryption process for the user, and have a hard exponential time challenge for as talker to break into the wireless system. In ECC a 160-bit key encryption data to provide the same security as compared to the traditional crypto system or an enhancement system RSA with a 1024-bit key, thus lowers the computer power. Instead of being measured face-to-face, with WBANs patients health-related document parameters can be monitored remotely, continuously, and in real time, and then processed and transferred to wireless medical databases.

This medical information is shared among patient details and accessed by various users such as healthcare staff, researchers, government agencies, and insurance companies. An overview of elliptic curve implementation on two dimensional representations of plaintext coordinate systems and data encryption through the megamall processor Encryption technique has been discussed. such attention has been given here on the mathematics of elliptic curves starting with their beginnings and the proof of how to view the points upon them form an additive Aeolian group for the encryption procedure cryptographic purposes, specifically results for the group formed by an elliptic curve over finite field, E (Fop), E (F2m), and showing how this can form public key cryptographic systems for in both encryption and key exchange. Finally, we describe how to encrypt the data to the albetical table.

In wireless mobile communication technology and personal communication systems, also it open air is used as communication channel, the content of communication may be exposed to an eavesdropper processor or system services can be used duplicitously. So to provide security Enhancement over the wireless communication channel, security measures such as confidentiality, authenticity need to be provided. In general symmetric encryption algorithms are used to obtain high data rates on wireless channel data processor. These algorithms use identical keys for encryption and decryption. The key exchange problem is the major flaw of using symmetric algorithms. The key must be exchanged between the two communications parties ensure that key remains secret procedures.

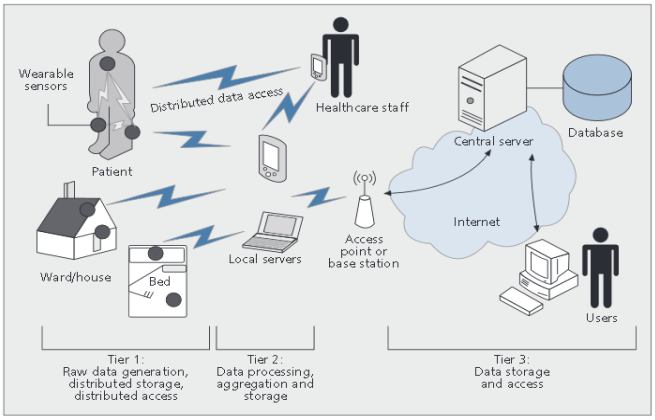

Fig.1. WBAN model

2. TRADITION SYSTEM

In existing system they have used the universal key for the data which we are sending to the server side. The major problem of this system was that the server can decrypt the message sent by the user If anyone hacked the main server means the whole privacy information's of the patients will went on the vain. in existing system we are using the three tiers first one is an raw data generation, distributed storage, distributed access second one is an data processing aggregation and storage. Third tier is an data storage and access point to using the wearable sensor in the patient body and to collect the information to the patient detail to store the control server to an local server and then send by the access point or a base station via internet to the user.

© 2017 AJAST All rights reserved.

3. ENHANCED SYSTEM

In our proposed system we are improving the security using our new enhanced encryption algorithm. In our proposed system the main server used to forward the packet to the receiver without decryption. Here we are applying the Elliptic curve encryption algorithm for the encryption. Every time we are generating the new key for encryption, so that we are enhancing the security of the WBAN.my project to using the elliptic curve for the new enhancement security in existing system server can decrypt the message and send by the user and they are using the universal key but proposed system user can decrypt the message sent by the server. The receiver without decryption to forward the packet.

4. PROPOSED SYSTEM ARCHITECTURE

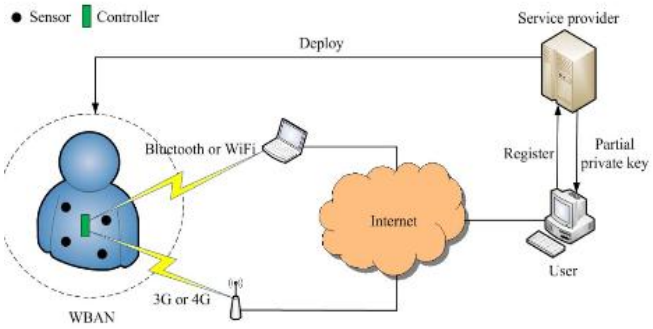

Fig. 1. Network model.

Fig.2. Network model

5. RELATED WORKS

We proposed a security enhancement algorithm technique can be authenticated key agreement data protocol that offers mutual authentication and secured way of deriving an encryption and decryption shared secret key where both the entities contribute information for universal key agreement.

A. Wired Equivalent Privacy (WEP)

Anyone can a radio receiver on audio and video can eavesdrop on a wireless local area network, and therefore widely acknowledged that a WLAN needs a mechanism to counter this encryption technique threat. The IEEE 802.11 standard defines a data confidentiality mechanism known as Wired Equivalent Privacy.

This technique can use the security goal of equivalent privacy and issues on health care security procedure are data confidentiality equivalent procedure on the security algorithm to that of a wired local area network. When active in wireless local and personal area network is took place, packet is encrypted separately with RC4 cipher stream generated by a 64-bit RC4 key. The 64-bit key consists of a 24-bit starts vector and a 40-bit wired equivalent privacy encryption key. The encrypted packet is generated with a bit wise exclusive OR of the original packet and RC4 stream generation.

The initialization vector chosen by the sender should be used in the plaintext and the hypertext changed so that every packet won't be encrypted the data without decryption the packet with the same cipher stream. A 4-byte integrity check value is computed on the original packet using CRC32 checksum algorithm processor.

B. Elliptic Curve Cryptography (ECC)

What makes ECC Important? The Discrete Logarithm. The security due to elliptic curve relies on the difficulty of Elliptic Curve Discrete Logarithm technique Problem. They have using the two point first point is an P point and second point is an Q point Let P and Q be two points on an elliptic curve such that KP = Q, where k is a scalar point. Given P and Q, it is computationally infeasible data to obtain k. If k is sufficiently large, k is the discrete logarithm of Q to the base P. Hence the main server operation involved in elliptic curve is related to the point multiplication i.e. multiplication of a scalar k with any point P on the curve to obtain another point Q on the curve procedure technique.

What is Elliptic Curve? It's Derivation and Use

Note that elliptic curve cryptography enhancement security for data process is not ellipses. They are so named algorithm because of the fact that ellipses are formed by quadratic curvatures. Elliptic curves are always cubic and elliptic form has a relationship to elliptic integrals in mathematics analysis where the elliptic integral can be used to determine the encryption procedures arc length of an ellipse. An elliptic curve in its standard form is described by $y2 = x3 + ax + b$. For the polynomial algebraic algorithm can be used them following equations , $x3 + ax + b$, the discriminated can be given as $D = - (4a3 + 27b2)$ This discriminate must not become zero for an elliptic curve polynomial algorithm $x3 + ax + b$ to possess three distinct roots. If the discriminate is zero point processor, that would imply that two or more roots have coalesced, giving the curves in singular form. It is not safe to use singular curves for cryptography as they are easy to crack process. Due to this reason we generally take non-singular curves for data encryption.

C. Elliptic Curve Arithmetic

An Algebraic Expression for Adding *Two Points on an Elliptic Curve over Fp.* Let FP, where *p* an odd prime number, be a prime finite field given two points used on the first point is an Q = (x1, y1) and another point is an R = (x2, y2) on an elliptic curve E (a,b), we have to compute the point Q + R.

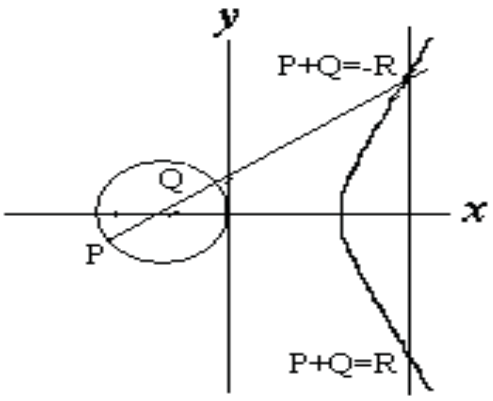

Fig.3. Elliptic curve

We first draw a straight line processor through the two point P and Q. Next, we find the third coming together of this line with the

© 2017 AJAST All rights reserved.

Elliptic curve denote this point of intersection by R. Then P + Q is Equal to the mirror reflection of R about the x-axis. In other words, if the points P, Q and -R are the three intersections of the straight line with the elliptic curve processor Curve, then

$$P + Q = - R$$

D. Encryption Algorithm

Step 1.First algorithm can be taking the message to be encrypted from the sender.

Step 2.Convert it to its 7bits binary element form using the ASCII code of the message.

Step 3.Convert the binary form of each word of the Message into an x 7 binary matrix where n is a Number of letters in each word of the message.

Step 4.To get the compressed decimal matrix of size n x 1, we will multiply the n x 7 matrix with the masked matrix process of size 7 x 1.

Step 5.We will get n values of „x‟ and to get the value of an data can Corresponding „y‟ values we will use the formula Y^2=x (i) ^3+j Where, i = 1 to n SS (and n is the no. of rows in the resultant Matrix) j is the variable which will keep on incrementing every time we get a y for a particular x value. The initial value of j = 1.

Step 6. Using the formula we will get (x, y) points.

Step 7.Algorithm for plotting the values of x, y:

Step 7.1: Get the values of x and y and truncate the Decimal values of y as well.

Step 7.2: Create a matrix consisting of the decimal values of y.

Step 7.3: Now find the x, y coordinates in the image.

Step 7.4: inverse the bit values of the image (i.e.: if bit value=01 then make it 10) on the particular coordinates of (x, y). That will produce the steno image as well.

Step 8.We will generate a prime matrix of size n x7 and using the „x‟ values we will generate an equation which will resemble the decimal matrix.

Step 9. Public Keys: The generated equation from the step7, prime matrix, will be send to the receiver.

Step 10.Private key: the original image, the steno image, the matrix containing numbers after decimal point of the values of „Y‟ and our formula (mentioned above).

E. Decryption Algorithm

Step 1.The receiver will get the x and y values after Comparing two images and finally get the values of y with the help of the matrix containing the values of y (after decimal points).

Step 2.The required matrix will be generated using the “x” values and the prime matrix which is public.

Step 3.We will multiply the „x‟ values with the prime elements and will check the result of the co-efficient with the generated public equation.

Step 4. In this way the receiver will generate the required matrix which will contain the binary form of the ASCII codes of the same hash algorithm and then uses the signature verification algorithm to verify the signature. If the message is verified successfully receiver authenticates the sender. In the following, H denotes a cryptographic hash function whose outputs have bit length no more than that of n.

F. Modules

They are three types of modules can be used in the proposed system.

- WABN Sensor Module
- Personal Server Module
- Medical Server Module

G. WABN Sensor Module

Wireless body area sensor network consists of a number of intelligent nodes, each capable of sensing, sampling, processing, and communicating of physiological signals. The architecture of a sensor network intended for medical applications must be carefully designed in order to have a long life time. Examples of such medical sensors are ECG(electrocardiogram) which can be used for monitoring hart activity, an EMG (electroencephalography) which is used for monitoring muscle a cavity, EEG (electroencephalography) sensor that monitor brain electricity and there is a movement sensor used to estimate user's activity.This module represent the process of an module of tis patient body networks.

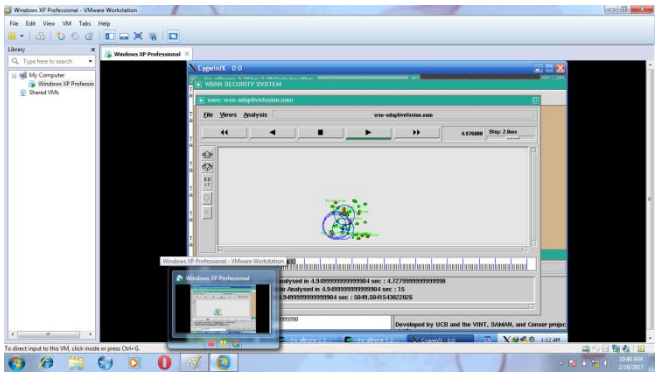

Fig.4.WABN model

H. Personal Server Module

The personal server interface the WBAN sensor nodes through Zigbee or Bluetooth connectivity and communicate with services at the medical server through mobile telephone networks (2G, GPRS, 3G) or WLANs to reach an internet access point .It is typically implemented on cell phone, but alternatively can run on home personal computer. The interface to the WBAN includes the network configuration and management. The network configuration and management. The network configuration encompasses the following tasks: sensor node registration (type and number of sensor), initialization (e.g., specify sampling frequency and made mode of operation), customization (e.g., run user specific calibration or user –specific signal processing procedure upload), and setup of secure communication (key exchange).he personal server can be using the sensor nodes

© 2017 AJAST All rights reserved.

on using the Bluetooth and connectivity to the data can be transfer the patient details on the server via a mobile and telephone networks that is an personal server model to the sensor nodes of the design on wireless networks .that can be represent the organization of the encryption procedure of this algorithm data can be viewed process.

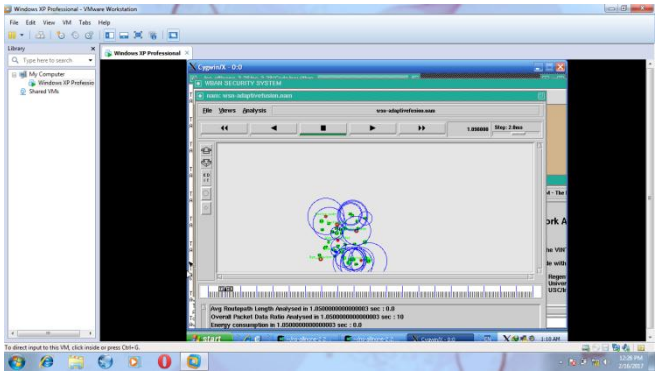

Fig.5. personal server model

I. Medical Server Module

The function of the medical server is to authenticate users, accept health monitoring session uploads, format and insert this session data into corresponding medical records. Analyse the data patterns, recognize serious health cases in order to contact emergency care givers, and forward new instruction to user such as physician prescribed exercises. Finally the medical server module can be represented the procedure like organization processor data element process data challenges in various requirement on this model this module doing the server side can be server send the authentication for the user.

6. CONCLUSION

This Project discussed the security and privacy issues in healthcare applications using medical sensor networks. In this respect, we have found many important challenges in implementing a secure healthcare monitoring system using medical sensors, which reflects the fact that if a technology is safe, then people will trust it. Our proposed system will overcome all the security issues obtained from the previous research schemes. This project fully based on the encryption and decryption data for the user and then server to existing system using the universal key in my proposed system using the generating the key for an elliptic curve cryptography.

REFERENCES

[1] Kio, B.J.G.; Lu, C.; Srivastava, M.B.; Stankovic, J.A.; Teri's, A.; Welsh, M. Wireless Sensor Network for Healthcare. *Proc. IEEE 2010, 98, 1947–1960. [Google Scholar]*.

[2] *http://www.census.gov/prod/2009pubs/p95-09-1.pdf*

[3] Alzheimer's Disease. Available online: *http://www.nia.nih.gov/NR/rdonlyres/7DCA00DB-1362-4755-9E87-96DF669EAE20/18196/ADFACTSHEET.pdf*

[4] Aging Heart and Arteries, A scientific Quest. Available online:*http://www.nia.nih.gov/NR/rdonlyres/0BBF820F-27D0-48EA-9820-736B7E9F08BB/0/HAFinal_0601.pdf*

[5] Gad dam, A.; MukhopadhyayS, S.C.; Gupta, G.S. Elder Care Based on Cognitive Sensor Network. *IEEE Sensors J 2011, 11, 574–581.*

[6] Kibitz N., Mentees A.J., and Vanstone S.A. The state of elliptic curve cryptography. Design, Codes, and Cryptography. Vol 19, Issue 2-3, 2000, 173-193.

[7] Lustra A., and Overhauls E. Selecting cryptographic key sizes. *Third International Workshop on Practice and Theory in Public Key Cryptography-PKC 2000. LNCS 1751, 2000.*

[8] *Silverman, The Arithmetic of Elliptic curves, Springer-Verlag, New york, 1986.*

[9] Tate, Jute arithmetic of elliptic curves. *Invent. Math*. 23 (1974), 171-206.

[10] S. Bajracharya, C. Shun, K. GA, and T. El-Ghazis, Implementation of Elliptic Curve Cryptosystems over GF(2n) in *Optimal Normal Basis on a Reconfigurable Computer.*

[11] Mentees A.J., Take E., and Went A. Weak fields for *ECC.CORR 2003-15*, Technical Report, University of Waterloo, 2003.

[12] Rivets R., Schemer A. and Alderman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21, 1978, 120-126.

[13] C. Shun, S. Kwon, and K. GA, Reconfigurable Computing Approach for Tate Pairing Cryptosystems over Binary Fields submitted to *IEEE Transactions on Computers.*

[14] Certicom. Information on the Certicom ECC challenge, *www.certicom.com/research/ecchallenge.html*

[15] Megamall, T., A public key cryptosystem and a signature scheme based on discrete logarithm, *IEEE Trans. Inform, Theory*, IT-31, no.4, pp469-472, July 1985.
.

[16] Hankerson, D.,Hernandez, L. J., and Mentees A. Software implementation of elliptic curve cryptography over binary fields, CHESS 2000,LNCS 1965, 1- M. M Amin, M. Salah, S.Ibrahim, M.R.K taming, and M.Z.I.Shamsuddin, Information Hiding using Steganography, *National Conference on Telecommunication Technology Proceedings, Shah Alarm, Malaysia, 2003 IEEE.*

[17] S Shell , G A Sathish Kumar, K Boopathybagan, A Secure Triple Level Encryption Method Using Cryptography and Steganography, *20 II International Conference on Computer Science and Network Technology, 978-1-4577-1587- 7/111$26.00 ©20111EEE, December 24-26,* 2011.

[18] Zhang and S. Wang, Steganography using multiple-base notational system and human vision sensitivity, *IEEE Signal Process. Lett.* vol.12, no. I, pp. 67-70.

[19] William Stallings, Cryptography and Network Security, *Pearson Prentice Hall.*

© 2017 AJAST All rights reserved.

[20] An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication, *2nd International Workshop on Discrete Algorithms and methods for Mobile Computing and Communications*, Oregon State University, October 30, 1998.
[21] Kevin Anderson, *MWSU, Elliptic Curve Cryptography*.

© 2017 AJAST All rights reserved.