INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 06 ISSUE: 05 | MAY - 2022 IMPACT FACTOR: 7.185 ISSN: 2582-3930

An efficient and secure anonymous authentication framework with location privacy preservation for IoT-based WBANs

Neethu K.P [1,*] , Kalaiselvi R [2]
[1] ME Student, Department of CSE, Noorul Islam Centre for Higher Education, Kumaracoil
[2] Associate professor(Kalaiselvi R), Department of CSE, Noorul Islam Centre for Higher Education, Kumaracoil

Abstract— Advances in wireless communications, embedded systems, and integrated circuit technologies have enabled the wireless body area network (WBAN) to become a promising networking paradigm. Over the last decade, as an important part of the Internet of Things, we have witnessed WBANs playing an increasing role in modern medical systems because of its capabilities to collect real-time biomedical data through intelligent medical sensors in or around the patients' body and send the collected data to remote medical personnel for clinical diagnostics. WBANs not only bring us conveniences but also bring along the challenge of keeping data's confidentiality and preserving patients' privacy. In the previous, anonymous authentication (AA) schemes for WBANs were proposed to enhance security by protecting patients' identities and by encrypting medical data. However, many of these schemes are not secure enough. The AA scheme for WBANs and point out that it is not secure for medical applications by proposing an impersonation attack. In this project, propose a genetic-based algorithm (GBA) with secure anonymous authentication framework for WBANs and prove that it is provably secure. The comprehensive analysis section shows that the proposed scheme overcomes the security weaknesses in the existing schemes and also provides low computation cost during anonymous authentication.

Keywords—: *Cross-modality, contrast enhancement, 2D histogram specification (HS), SSIM gradient, tumor segmentation.*

I. INTRODUCTION

Technological advances in various fields have led to significant improvements in the lives of people all over the world resulting in their increased life expectancy. For example, the life expectancy in the United States has prolonged t 78.2 years from 69.8 years during the past 50 years. It is expected that about 81 million people will be 60 or older in 2050. The rapid growth in the number of aged people creates many economic and societal challenges as more aged people will suffer from chronic diseases and will not be able to take care of themselves. To take better care of aged people and reduce the burden on society, real-time monitoring of patients and remote medical clinical diagnostics are going to be a crucial part of the healthcare system.

The wireless body area network (WBAN), initially proposed by Zimmerman [2], is a promising networking paradigm, which uses wireless personal area network (WPAN) technology. In recent years, the WBAN has attracted a lot of attention from both the research community and industry as an important part of the Internet of Things (IoT). A WBAN consists of many low power intelligent sensors, which are placed in or around the human body. Through these sensors, real-time monitoring could be implemented remotely. The typical WBAN application scenario where the WBAN collects real time biomedical data such as heart rate, blood pressure, and pulse and then sends the data to a remote medical server through mobile devices such as a personal digital assistant (PDA) or a smart phone. Based on this data, doctors and other medical personnel could get a patient's status and provide the appropriate clinical diagnostics. Therefore, the use and deployment of WBANs could help us to take care of aged people and patients by providing a reliable and robust health-monitoring service in the IoT environment.

The data collected or transmitted in WBANs are very sensitive and important because these are the basis of clinical diagnostics. Besides, privacy is also an important issue from the patient's perspective because biomedical data are highly confidential and should be handled, transmitted, and stored with care to prevent information leakage to unauthorized users. Therefore, authentication, data confidentiality, integrity, nonrepudiation, and privacy preservation should be guaranteed during all communications within the WBAN environment. To generalize the applications based on WBANs, IEEE 802.15.6 has been proposed to provide an international standard for reliable wireless communication in WBANs and the standard could support data rates ranging from 75.9 kb/s to 15.6 Mb/s. The standard describes security requirements and various security levels in WBANs. The standard also recommends four elliptic curve-based security schemes to achieve those goals. However, recent works show that those four security protocols are vulnerable to several attacks. Therefore, the standard is not secure enough for some practical applications. To enhance security, anonymous authentication (AA) schemes for WBANs have been extensively studied to provide not only authentication and privacy preservation but also to ensure confidentiality, integrity, and nonrepudiation based on a shared key

Since the WBAN connects with more important and sensitive patient related information, it is necessary to provide security and privacy to this information. Moreover, privacy preservation is also an essential problem for a patient because biological information is considered to be highly confidential. Therefore, the biological information should be stored and transmitted secretly to prevent any information leakage to illegal users. Hence, it is very important to safeguard the patient-related information against security breaches and to ensure the patients privacy

The proposed framework is developed based on four security necessities:

(1) The privacy delivered by TA to WBAN users is a conditional privacy.

(2) The construction of our anonymous authentication framework is based on the use of bilinear pairing.

(3) In this proposed framework, TA is not required to keep the anonymous certificates of patients and medical experts. Instead, the patients and medical experts can make their own anonymous certificates to guard their privacy.

(4) In the case of any problem, TA has the facility to efficiently revoke the privacy of a misbehaving medical expert to discover its actual identity. Then, TA keeps actual identity of the revoked medical expert in its revocation list.

secret from the unauthorized entities

II. LITERATURE SURVEY

Security is currently one of the most important concerns for telecommunications due to the widespread of deployed wireless networks. One of the key problems in the field of ensuring the wireless exchange of information is the initially shared awareness between source and destination. So, various encryption techniques are used in literature to secure the data. Author Anwar et al. proposed safe hashing algorithms along with encryption techniques that are used to make data transmission more efficient and powerful. Digital signatures are created by a hash procedure to transport patient data more safely and authentically. This proposed algorithm used the Asymmetric key generation approach that requires pairs of public and private keys, making the algorithms slower and highly complex [1].

Advances in medical science and technology have brought together modern Patient Monitoring System (PMS) activated by the wireless body area network which provides a simple, effective, and unparalleled revolution health facilities. WBAN used nano sensors to collect patient's data and transmit it on the way to the hospital server through a wireless network. Privacy and protection of data is an important concern for the patients and doctor. Consequently, the author Fahim Shahriar Chowdhury et all used data encryption to secure from eavesdropper and authenticate to ensure the legitimate user [2].

The literature technique used end to end secured monitoring transportation system and encrypt data with lightweight version AES (Advanced Encryption Standards). Then encrypted data is transported over MQTT protocol in the direction of the hospital server. This scenario resulted into a simple and effective system. Various protocols were used in the literature for the transmission of data. The author Shahwar et al. used LEACH protocol in the proposed study and lightweight encryption algorithm which transfers data on wireless sensor networks efficiently [3] and Savita Sindhu et al. used CSMA/CA and TDMA protocol for routing [10]

Author Marva BOUMAIZ et al. intends to investigate the impact of an adjacent BAN 's existence, when it transmits power differs, on a reference BAN's output through simulation. Both the CM3A path loss model, defined in the IEEE 802.15.6 standard for the 2.4 GHz on-body medium, and the temporal variation phenomenon, are being considered. Evaluation of output is performed in terms of the rate of packet loss (PLR) [6]. The author Saiyma Fatima Raza et al. suggests a new approach to data protection especially during emergencies in a wireless network

WBAN uses passive Encryption Standard-128 (AES-128) cipher requiring considerable time for encryption which can be fatal in emergencies. Due to the region and resource constraints, the sensor node protection mechanism should be lightweight. The suggested approach uses chaos-based scrambling in emergencies, which is Lightweight concerning AES, and much less processing time is needed in emergencies [7]. Many security standards are inevitable in WBAN, such as data confidentiality, data quality, data accessibility, data authentication, accessibility, access control, transparency, non-repudiation, etc. [8]. Two security suits are presented in the proposed study in the study of Agha et al. [9]. The first security suit focused on KBS key management with Hashing and the second called KAISC suit for communication between sensors as key management scheme.

The requirement to have two separate procedures, one for transmission of data to the base station and one for intersensory communication, is to improve safety. WBAN is an advanced technology that employed nano sensors into the human body and accumulates health-related data. The transportation of data needs security schemes to avoids attackers. Such cryptographic mechanisms are based on the use of wellmanaged cryptographic keys (generation and distribution) to make security robust enough [11]. The author Marko Kompara et al. used efficient mutual authentication and key agreement technique for security in the proposed study of WBAN [12]. Two new protocols have been proposed by author Peyman Dodangeh to exchange the key between the sensor nodes with the watch and the mobile node in a two-tier WBAN topology and to achieve mutual authentication. The proposed protocols for inter and intra BAN sections require secure authentication of other nodes by one node, biosensors, the watch, the mobile node, and the medical server.

Lightweight Encryption Algorithm (LEA) is the most appropriate for WBAN settings were the devices used (sensors and mobile devices) have limited memory space and low processing power is very low compared to traditional algorithms for encryption [19]. The scheme adopts the concept of hybrid encryption to reduce data encryption's computational overhead, that is, to use the symmetric key to encrypt data to ensure performance, and to use the CP-ABE method to encrypt the symmetric key for protection. [20]

III SYSTEM OVERVIEW

A typical system model [3] of the proposed WBAN system is depicted in Fig. 1. The four most important entities of the WBAN system are trusted authority (TA), Sensors (wearable and implanted), data sink (a mobile device like a smart phone or the BAN data controller), and users such as doctors, medical experts and patients

Trusted authority (TA):

The TA is used to do system initialization, public parameters generation, user registration and secret keys generation for every user. The generated secret keys should be unique in nature to avoid collusion attacks. At first, all users are required to register in the TA through its website by providing the necessary information, which includes personal information, original identities and so on. A secure socket layer (SSL) encryption is performed between user and T A during the registration process. After completion of the registration process, TA issue credentials to the users. By getting the credentials from T A only, the users are considered as the WBAN users.

Sensors:

Generally, a WBAN consists of wireless wearable and implanted sensors. The wearable sensors are equipped on/near the surface human body through wearable devices and the implanted sensors are implanted inside the tissue of the human body. These sensors are mainly used to provide life support by monitoring vital biological body parameters such as blood pressure, body temperature and so on. The main resource constraint of the implanted sensors is battery power compared to wearable sensors. Since the wearable devices are commonly battery-powered, the batteries can be easily changed and recharged. These wearable and implanted sensors collect the information about the biological parameters of the human body and send it to the data sink. In turn, the data sink of the particular patient sends the biological information to an authorized medical expert or an authorized doctor periodically.

Data Sink:

A data sink is a mobile device such as a smartphone or a BAN controller which is used to collect the patient's biological information from the implanted and wearable sensors. The data sink has communication and computation capabilities to send the biological information to the authorized doctors. The data sink has the storage capability to store the collected biological information and to store the secret keys which are given by T A during the time of user's initial registration process. The data sink can authenticate the medical experts or doctors in an anonymous manner to understand their legitimacy with T A before sending the biological information to them. On the other hand, protecting the information in the data sink is also essential to avoid various categories of security attacks in WBANs. In order to overcome this limitation, in our framework, the information is stored in an encrypted manner and hence the attacker has no way to access the original information. Therefore, the main functionally of the data sink is to keep the information in an encrypted form and to disseminate the information to the authorized doctors or medical experts also in an encrypted form. Thus, the information kept in the data sink is protected and it is not easily compromised by attackers.

Users:

The authorized patients, doctors or other medical experts are considered as the users in the WBAN system. T A can generate a set of unique secret keys for every registered user. These keys are used to anonymously authenticate the sender of the patient-related information and to avoid the malicious injection of information from the outside.

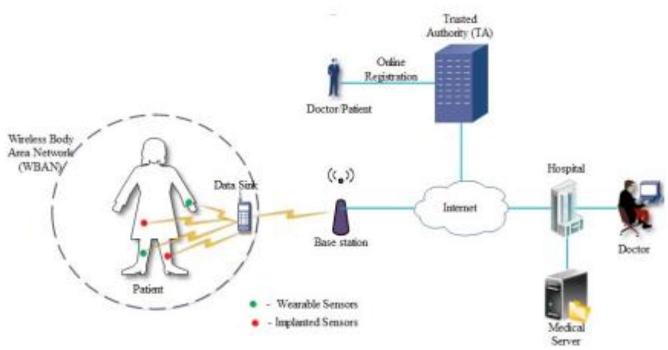

Fig 1 System Architecture

IV PROPOSED SCHEMES

In this section, propose a computationally efficient anonymous authentication scheme based on bilinear pairing to avoid communication with malicious users in the WBAN system. In anonymous authentication, the patients can effectively authenticate the doctors without knowing their actual credentials or identity information. Hence, the privacy of the doctor is preserved from information leakage. In the same manner, doctors can anonymously authenticate the patients to avoid communication with the malicious patients. To achieve perfect anonymous authentication, the user's real credentials and secret keys must be protected. Our scheme has six important stages namely TA's initialization, user registration, patient's anonymous authentication process, doctor's anonymous authentication process, confidentiality and revocation.

A) Initialization:

TA picks the random numbers $t \in Z^*q$ as its master key and $a \in Z^*q$ as its private key. Then, T A computes its public key as $X_1 = g^{a\,1}$ and an authentication parameter as $A_1 = g_1\,2^{a+t\,1}$.

B) User Registration

In the registration process, the WBAN users (patient or doctor or other medical expert) directly access the TA's website and provides their personal details like name, address, mobile number and email id, etc.

1). If the user is the patient P_i , then T A gets the personal details from P_i and stores them in its database in a secure manner. Next, T A picks a random number $ui \in Z^*q$ and computes the private key as $P\,{}^{r}P_i = g_1{}^{ui+a}$

2) Then, T A generates an anonymous identity for each P_i such that $FP_i = g^{a+t-ui\ 1}$ to protect the real identity of P_i from unauthorized users during the time of communications. Instead of using the real credentials of P_i , the anonymous identity FP_i is used for communications in WBANs. Here, FP_i is mapped with the user's real credentials only in TA. Therefore, by capturing this anonymous identity, it will give zero knowledge about the real credentials of Pi to attackers.

3) Besides, T A generates the tracking parameter TP_i such that $TP_i = g^{t+ui\ 1}$ for each Pi and keeps (PkP_i ,PrP_i, FP_i ,TaP_i) in its tracking list. In case of patient's misbehaviouring, T A can revoke him/her from the WBANs using TP_i .

4) Then, T A sends P rP_i through SSL to P_i and P_i stores P rP_i in its data sink in a secure manner. Finally, T A sends Ω = ((FP_i k P kP_i k TP_i) $\oplus$ P rP_i) to P_i . By receiving this, Pi performs $\Omega \oplus$ P rP_i and gets (FP_i , P kP_i , TP_i).

5) Similarly, for a D_i , T A picks a random number $d_i \in Z^*q$ and computes the private key as P rD_i = g 1 d_i+a 1 and its corresponding public key as P kD_i = g d_i 1 .

6) Then, T A computes an anonymous identity FD_i such that FD_i = g a+d_i 1 for D_i .

7) Moreover, the doctors are required to register their working medical institution in the TA. Then, T A generates an anonymous identity for the working institution of Di such that $F_{Mi} = g^{a-di+t\ 1}$. Next, T A can generate this identity only if the corresponding medical institution is registered in the TA. The doctors of the non-registered institutions are not considered to be the part of the WBAN system. Hence, the medical institution is also anonymously authenticated by the patient.

8) For each Di , T A generates a tracking parameter $TD_i = g^{t+di\ 1}$ and keeps (FD_i , F_{Mi} , T a D_i) in its tracking list to revoke the misbehaving doctors from the WBANs.

9) In addition, T A selects two secret keys (DSK) K_{i1}, $K_{i2} \in Z^*q$ for a doctor D_i , where K_{i1}, K_{i2} > 18000.

10) Next, T A sends P rDi through SSL to Di and the Di stores P rDi in a secure manner. Finally, T A sends Ω 0 = ((F$_{Di}$ || P k$_{Di}$ || F_{Mi} || K_{i1} || K_{i2}) $\oplus$ P rDi) to the Di . By receiving this, the Di performs Ω ' $\oplus$ P rD_i and gets (FD_i , P kD_i , FM_i , K_{i1}, K_{i2}).

After the completion of registration process, a patient and a doctor can perform anonymous authentication process.

C) Patient's Anonymous Authentication Process

In anonymous mutual authentication process, the patients and doctors are required to anonymously authenticate each other before starting their communications. In patient's anonymous authentication process, the credentials of the patients are verified anonymously by the doctors or the medical experts.

Anonymous authentication certificate generation To prove the legitimacy to the doctors or medical experts anonymously, the patient's data sink first generates the anonymous authentication certificate (AAC) as per the following steps:

Anonymous signature generation:

To maintain the integrity of the communication messages, the data sink is required to generate the anonymous signature.

Anonymous signature verification:

By receiving {AS k $_m$ k δ1}, Di first verifies the integrity of m by checking whether e(δ1 × g b 1 , AS) = e(g1, g2). If this condition is satisfied, then Di accepts m, otherwise rejects it.

$$\begin{aligned} & e(\delta_1 \times g_1^b, AS) \\ &= e(g_1^k \times g_1^b, g_2^{\frac{1}{k+b}}) \\ &= e(g_1^{k+b}, g_2^{\frac{1}{k+b}}) = e(g_1, g_2) \end{aligned}$$

Anonymous authentication certificate verification:

Next, D_i checks the timestamp T S_i such that |T $_{Sj}$ − T S_i | < ΔT to avoid the replay attack where ΔT is the mutually agreed time delay between the Di and P_i .

$$\begin{aligned} \gamma_2' &= \mathcal{O}_2 \times \mathcal{O}_3 \times \mathcal{O}_4 \\ &= g_1^{-l} \times g_1^{-\beta+l} \times g_1^{\alpha+l} \\ &= g_1^{-l-\beta+l+\alpha+l} \\ &= g_1^{-\beta+\alpha+l} = \gamma_2 \end{aligned}$$

$$\begin{aligned} \gamma_1' &= \delta_1 \times \mathcal{O}_1 \times \mathcal{O}_2 \\ &= g_1^k \times g_1^{l+\beta} \times g_1^{-l} \\ &= g_1^{k+l+\beta-l} \\ &= g_1^{k+\beta} = \gamma_1 \end{aligned}$$

After verifying the anonymous signature and anonymous authentication certificate only the doctor Di can analyze the biological information (BI). If any one of the verification processes fails, then Pi is considered as the illegal user of WBAN system.

D) Doctor's Anonymous Authentication Process

Before sending the biological information and getting the medical advises or instructions from the doctor, it is necessary for the patient to check the legitimacy of the doctors or medical experts in an anonymous manner.

Doctor's anonymous authentication certificate generation:

D_i generates his authentication certificate DAAC as follows:

(a) Di computes an arbitrary parameter θ1 as θ1 = FMi × FDi .

(b) After computing θ1, Di computes a challenger value (DCV) as DCV = H(e(g1, g2)kFDi kP kDi).

(c) Then, Di sets its anonymous certificate as DAAC = {θ1, FDi , P kDi } and sends it to the data sink of Pi along with the timestamp T Si+1.

(d) By receiving this, Pi first verifies the current timestamp and then verifies whether e(θ1, A1) = e(g1, g2) to check the legitimacy of Di .

$$\begin{aligned} & h_1 \\ &= e(\theta_1, A_1) \\ &= e(F_{M_i} \times F_{D_i}, A_1) \\ &= e(g_1^{a-d_i+t} \times g_1^{a+d_i}, g_2^{\frac{1}{2a+t}}) \\ &= e(g_1^{a-d_i+t+a+d_i}, g_2^{\frac{1}{2a+t}}) \\ &= e(g_1^{2a+t}, g_2^{\frac{1}{2a+t}}) = e(g_1, g_2) \end{aligned}$$

(e) Then, the data sink calculates its own challenger value as DCV 0 = H(h1 k FDi k P kDi) and compares whether DCV 0 = DCV . If these two values are equal, then the data sink considers that Di is an authenticated user of WBAN, otherwise, it simply avoids the future communications with Di During the anonymous authentication process as well as the communication of messages, the doctor does not know about the real location of the patient. The real location of the patient is preserved from the other entities of WBAN by the TA. However, in the case of emergency, the doctor is required to monitor the patient directly. In the case, the doctor can only get the location of the patient from T A using CRT-based location privacy preservation process.

E) Confidentiality

After successful mutual authentication, the data sink of Pi sends the biological information (BI) to Di . To maintain confidentiality, the BI of Pi is encrypted by the data sink using any one of the genetic-based encryption algorithm.

A lightweight genetic-based encryption algorithm is presented to secure the patient's data over WBAN. After sensing the patient's health data, the proposed encryption algorithm is implemented to convert the data into ciphertext over sensor devices. Encrypted data transmits towards the collector through Bluetooth, and the collector will further transfer it over the network towards the medical server. This encryption scheme uses fewer steps which makes the algorithm simple and efficient. The key generation algorithm is also using very simple mathematical operations that generate 8 bits of a key which later used in the genetic encryption algorithm. Then encrypted data is transferred in the direction of the cloud server through a message queuing telemetry transfer protocol. The genetic-based algorithm takes 8 bits of plaintext as patients' data is in the form of decimal numbers and then convert this text into binary numbers. After the conversion of binary performs exclusive or (XOR) with the key generated by a simple step. Key generation is performed by taking a random integer and convert that integer into the binary. Then perform 1's complement over the generated binary bits. After this step do circular two shifts right and now the generated binaries will act as a key in the genetic algorithm.

This key performs XOR with the 8-bit binaries of the patient's data, then mutation T replacement is carried out on index values of an array to make data in an incomprehensible form from table 1. Now, 8 bits of data are divided into four bits each for crossover operation. In crossover exchange of right side of four bits into the left side and left side of four bits into the right side is positioned. The generated data will perform the next step of S-box values that took the first two bits of the left side as rows and first two bits of the right side as columns respectively from table 2. Then the generated alphabets values from the s-box will obtain their substitution code from amino acid table 3 and the produced code performs string mapping like '0' mapped with 'A' and '1' mapped with 'B'. The obtained combination of 'As' and 'String is calculated ciphertext from a genetic algorithm.

Table 1 shows the mutation T values that are used in the genetic-based encryption algorithm for swapping binaries of temporarily generated ciphertext. These values used an array index of '0' to '7' for 8-bits of values to swap according to the assigned values on that index. All the 8-bits binaries are shuffled with their corresponding index values. E.g. binary value at index 1 will shuffle the binary value of index 7 while decrypting the binary data at index 7 will replace with the binary of index 1 value.

TABLE 1. Mutation t exchange values in array index.

Mutation T							
0	1	2	3	4	5	6	7
5	7	1	4	6	0	3	2

Table 2 presents substitution values for resultant binary generated data after performing crossover which gives two subsets (4-bits each) of 8-bits data used s-box. The values of the s-box are substituted by the following pair of first 2-bits as rows and second 2-bits as columns of the first subset.

TABLE 2. S-box values for replacing data

S-box	00	10	11	01
00	T	E	Y	A
10	N	U	H	C
11	I	S	R	B
01	G	K	F	M

TABLE 3. Amino acid code values for substitution

Amino Acid	Code
T	0000
E	0001
Y	0010
A	0011
N	0100
U	0101
H	0110
I	0111
S	1000
R	1001
C	1010
B	1011
G	1100
K	1101
F	1110
M	1111

The same process is for the second subset of data. S-box contains rows and columns of binary pairs and the value that are being substituted from the table are in alphabetic form to make temporary cipher. S-box generating 1 resultant alphabets against one subset of 4-bits. Likewise, 1 alphabet resultant of second 4-bits. Therefore, the s-box provides a temporary cipher of two alphabets.

Table 3 contains amino acid codes for the S-box generated alphabets. Amino acid table assigned some specific codes of binaries to the specific alphabets which are near to ciphertext. Every alphabet assigned 4-bits of binaries, so the s-box resultant two alphabets replaced with the Amino acid 4-bits binary to make 8-bits data again.

(F) Revocation

Sometimes, even the authenticated doctors may give wrong medical advise or improper medical treatments to the patients so that they may suffer from harmful side effects. In case of such misbehavior, T A can revoke the misbehaving doctors from the WBAN system. For that, T A first decrypts the ciphertext C_0 of D_i using the private key of Pi who is affected by Di's wrong medical advise. Then, TA computes T_aD_i and matches this parameter with the original identity of Di through its tracking list. After identifying D_i, TA revokes her/him from the WBAN system and hence the patients cannot make further communications with Di .

V RESULT AND DISCUSSION

The following metrics are used to evaluate the performance of the protocols:

Computation Cost

In proposed scheme, the multiplicative cyclic groups G1, G2 and GT are generated based on a Type-A elliptic curve, which is defined in the PBC library with default parameters. Let us consider some major cryptographic operations to determine the computation cost as follows: Tp, Th, Ts and Tm denote the time required to perform the bilinear operation, hash operation, symmetric and point multiplication operation in a group, respectively. The experiment is performed on a intel core i3 2-GHz processor featured with 4-GB RAM, running with C#.net [. The execution time for each time parameter Tp, Th, Ts and Tm are derived after repeated simulations and the average of all simulation results is taken as final values. The execution times of each cryptographic operations Tp, Th, Ts and Tm are calculated to be equal to 1.7 ms, 2.6 ms, 0.4 ms and 0.7 ms, respectively.

Fig. 5.1 shows the comparison of computational cost of patient's anonymous authentication with various schemes. From Fig. 5.1, it is very clear to observe that our scheme takes only around 550 ms for verifying 100 patients where as the other existing schemes take more than 1500 ms for verifying 100 patients.

Comparison Table of Computation cost of certificate and signature verification

No. of Patients	Verification time in ms		
	AA	AAC+ECC	AAC+GBA
20	400	150	145
40	750	300	290
60	1200	450	440
80	1500	550	530
100	2000	700	680

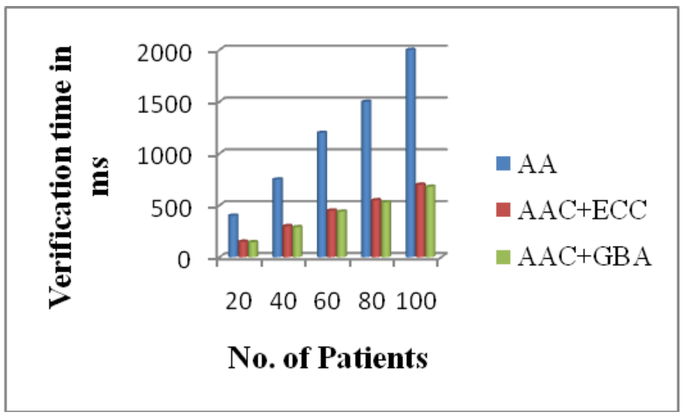

Figure 2 Computation cost of certificate and signature verification

Communication overhead

In this section, the communicational overhead of our scheme is analyzed with the existing schemes. The Type-A elliptic curve y 2 mod q ≡ x 3 + ax + b mod q, which is defined in the PBC library is used, where q is the 160-bit prime number and the size of each term in G1, G2 and GT are 20 bytes. Let us consider the size of the timestamp, element in Z ∗ q and the output of hash function are 4 bytes, 20 bytes and 20 bytes, respectively.

Comparison Table of Communication Overhead

Message Type	Communication Overhead		
	AA	AAC+ECC	AAC+GBA

Single message (bytes)	320	180	170
n messages (bytes)-=2	640	360	350

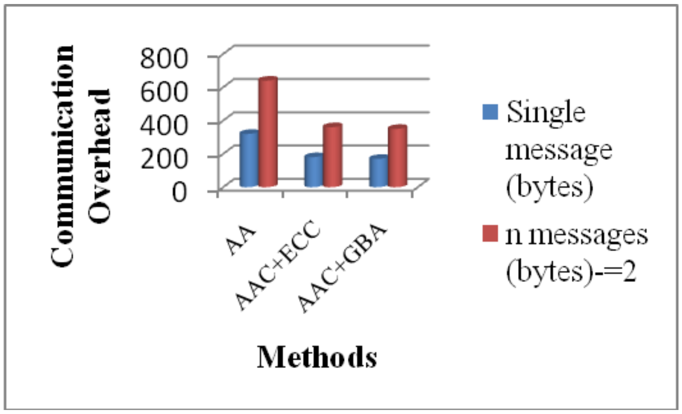

Figure 3 Communication Overhead

V1 CONCLUTION AND FUTURE WORK

In this project, proposed a new AA scheme with GBA for WBANs with provable security. In our scheme, first the doctor anonymously authenticate the patient to check the patient's legitimacy and then the patient anonymously authenticate the doctor to check the legitimacy of the doctor. Moreover, the location privacy of both the patient and the doctor is preserved by T A and it is exposed to the authorized doctors or patients based on the use of CRT. The security analysis shows that our scheme can provide resistance against impersonation attack, message modification attack, replay attack, eavesdropping attack and man-in-the-middle attack. The performance analysis shows that our scheme is efficient in terms of computational cost and hence it is more appropriate for practical IoT-based WBAN applications. The future extension of this work is to provide the batch authentication to the communicating users in an efficient manner.

V11 REFERENCES

[1] T. Wang, M. Z. A. Bhuiyan, G. Wang, M. A. Rahaman, J. Wu, and J. Cao, "Big data reduction for a smart city's critical infrastructural health monitoring," IEEE Communications Magazine, vol. 56, no. 3, pp. 128–133, 2018.

[2] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "Privacyprotector: Privacy-protected patient data collection in iot-based healthcare systems," IEEE Communications Magazine, vol. 56, no. 2, pp. 163–168, 2018.

[3] H. Zhao, P. Bai, Y. Peng, and R. Xu, "Efficient key management scheme for health blockchain," CAAI Transactions on Intelligence Technology, vol. 3, no. 2, pp. 114–118, 2016.

[4] F. Wu, T. Wu, and M. R. Yuce, ''An Internet-of-Things (IoT) network system for connected safety and health monitoring applications,'' MDPI Sensors, vol. 19, no. 1, pp. 1–21, Dec. 2018.

[5] A. Bashir and A. H. Mir, ''Securing communication in MQTT enabled Internet of Things with lightweight security protocol,'' EAI Endorsed Trans. Internet Things, vol. 3, no. 12, pp. 1–6, Apr. 2018.

[6] M. Boumaiz, M. El Ghazi, A. Bouayad, M. Fattah, M. El Bekkali, and S. Mazer, ''The impact of transmission power on the performance of a WBAN prone to mutual interference,'' in Proc. Int. Conf. Syst. Collaboration Big Data, Internet Things Secur. (SysCoBIoTS), Casablanca, Morocco, Dec. 2019, pp. 1–4.

[7] S. F. Raza, C. Naveen, V. R. Satpute, and A. G. Keskar, ''A proficient chaos based security algorithm for emergency response in WBAN system,'' in Proc. IEEE Students' Technol. Symp. (TechSym), Nagpur, India, Sep. 2016, pp. 18–23.

[8] I. A. Sawaneh, I. Sankoh, and D. K. Koroma, ''A survey on security issues and wearable sensors in wireless body area network for healthcare system,'' in Proc. 14th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. (ICCWAMTIP), Dec. 2017, pp. 1–5.

[9] D. S. Agha, F. H. Khan, and R. Shams, ''A secure crypto base authentication and communication suite in wireless body area network (WBAN) for IoT applications,'' Wireless Pers. Commun., vol. 103, pp. 2877–2890, Sep. 2018.

[10] S. Sindhu, S. Vashisth, and S. K. Chakarvarti, ''A review on wireless body area network (WBAN) for health monitoring system: Implantation protocol,'' Commun. Appl. Electron., vol. 4, no. 7, pp. 1–5, 2016.

[11] A. Sammoud, M. A. Chalouf, O. Hamdi, A. Bouallegue, and N. Montavont, ''A new biometrics-based key establishment protocol in WBAN: Energy efficiency and security robustness analysis,'' Comput. Secur., vol. 96, Sep. 2020, Art. no. 101838.

[12] M. Kompara, S. H. Islam, and M. Hölbl, ''A robust and efficient mutual authentication and key agreement scheme with untraceability for WBANs,'' Comput. Netw., vol. 148, pp. 196–213, Jan. 2019.

[13] P. Dodangeh and A. H. Jahangir, ‘‘A biometric security scheme for wireless body area networks,’’ J. Inf. Secur. Appl., vol. 41, pp. 62–74, Aug. 2018.

[14] P. K. D. Pramanik, A. Nayyar, and G. Pareek, ‘‘WBAN: Driving ehealthcare beyond telemedicine to remote health monitoring: Architecture and protocols,’’ in Telemedicine Technologies: Big Data, Deep Learning, Robotics, Mobile and Remote Applications for Global Healthcare. Amsterdam, The Netherlands: Elsevier, 2019, pp. 89–119.

[15] J. Wang, K. Han, S. Fan, Y. Zhang, H. Tan, G. Jeon, Y. Pang, and J. Lin, ‘‘A logistic mapping-based encryption scheme for wireless body area networks,’’ Future Gener. Comput. Syst., vol. 110, pp. 57–67, Sep. 2020.

[16] M. Gowtham and S. S. Ahila, ‘‘Privacy enhanced data communication protocol for wireless body area network,’’ in Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS), Coimbatore, India, Jan. 2017, pp. 6–7.

[17] A. M. Koya and P. P. Deepthi, ‘‘Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network,’’ Comput. Netw., vol. 140, pp. 138–151, Jul. 2018.

[18] M. M. Dhanvijay and S. C. Patil, ‘‘Internet of Things: A survey of enabling technologies in healthcare and its applications,’’ Comput. Netw., vol. 153, pp. 113–131, Apr. 2019.

[19] A. Z. Alshamsi and E. S. Barka, ‘‘Implementation of energy efficient/lightweight encryption algorithm for wireless body area networks,’’ in Proc. Int. Conf. Informat., Health Technol. (ICIHT), Riyadh, Saudi Arabia, Feb. 2017, pp. 21–23.

[20] M. Xiao and X. Hu, ‘‘Multi-authority attribute-based encryption access control scheme in wireless body area network,’’ in Proc. 3rd Int. Conf. Inf. Syst. Eng. (ICISE), Shanghai, China, May 2018, pp. 4–6.

[21] S. Soderi, L. Mucchi, M. Hamalainen, A. Piva, and J. Iinatti, ‘‘Physical layer security based on spread-spectrum watermarking and jamming receiver,’’ Trans. Emerg. Telecommun. Technol., vol. 28, no. 7, pp. 1–13, Jul. 2017.

[22] L. Mucchi, L. S. Ronga, and L. Cipriani, ‘‘A new modulation for intrinsically secure radio channel in wireless systems,’’ Wireless Pers. Commun., vol. 51, no. 1, pp. 67–80, Oct. 2009.

[23] M. A. Shayokh, A. Abeshu, G. B. Satrya, and M. A. Nugroho, ‘‘Efficient and secure data delivery in software defined WBAN for virtual hospital,’’ in Proc. Int. Conf. Control, Electron., Renew. Energy Commun. (ICCEREC), Bandung, Indonesia, Sep. 2016, pp. 12–16.

[24] J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, ‘‘BHEEM: A blockchain-based framework for securing electronic health records,’’ in Proc. IEEE Globecom Workshops (GC Wkshps), Abu Dhabi, United Arab Emirates, Dec. 2018, pp. 9–13.

[25] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, ‘‘Blockchain-based remote patient monitoring in healthcare 4.0,’’ in Proc. IEEE 9th Int. Conf. Adv. Comput. (IACC), Tiruchirappalli, India, Dec. 2019, pp. 13–14.