INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

WBAN CLIENT VERIFICATION USING REMOTE ANONYMOUS AUTHENTICATION SCHEMES WITHOUT CERTIFICATES

Madhusudhan U R[1,] Keerthana B[2], Poonam Tijare[3]

M.TECH[1], Assistant Professor[2], Assistant Professor[3]
Dept. Of Computer Science and Engineering, CMRIT, Bangalore, India
Visvesvaraya Technological University, Belgaum, India
madhu10ugane@gmail.com[1] , keerthana.b@cmrit.ac.in[2] , poonam.v@cmrit.ac.in[3]

ABSTRACT: - In this paper, communication between Client and Application provider should be authentic; so two protocols are used for authentication which is trivial and coherent performed through Network manager (NM). The authentication success between WBAN client and Application provider (AP) is used to activate users of WBAN in distant to access services such as healthcare, medical applications, military application etc, unknowingly. To design this authentication protocols a novel certificate less scheme with signature (CLS) is developed. Its computed, coherent, verified and secured. Service providers or Application providers do not have any advantage to reveal the private information of users. Private Key generator (PKG) served by Network manager cannot imitate legal users. Theoretic analysis, experimental simulations and comparative studies are conducted and evaluated. Computation cost, implementation & security gives better tradeoffs between two authenticated protocols. Comparison of running time gives better performance and results.

Keywords: WBAN, Authentication, Signature schemes, Client, Application provider, Network Manager, PKG

I. INTRODUCTION

Wireless personal area network (WPAN) technologies are used for communications on, near, and around the human body. WBAN named as Wireless body area network was first proposed by Zimmerman in 1996. Immediately the work was drew much attention from both academia and industry. For example, a family of short distance communication standards was developed by IEEE802.15. In particular, 802.15.6 was formally standardized in 2012 after five years effort of engineers from 60 companies. Wireless body area network (WBAN) is one of the wireless sensor technologies for improving different types of services such as healthcare services. WBAN has the capability to continuously exchange medical information in real time.

In a system such as WBAN, the information is shared to physicians and care takers based on detection of risks and also it prevents the health conditions of patients by continuously monitoring. WBAN contains two various types : one is body surface which gets operated by wearable body area network & second one is on inside the human body which gets operated by implantable body area network categorized based on the operating environments.

Implementation of real-time wearable health monitoring for patients using wireless sensor nodes is utilized as a forthcoming technology known as Wireless Body Area Networks (WBAN). Multiple bio-parameters (such as heart activity, blood pressure and blood oxygen saturation) of multiple patients in the hospital at a central location can be monitored by using sensor nodes that can be worn externally or implanted inside the body.

In daily activities patient can live normally and patients' health status can be monitored anytime and anywhere without restricting his/her mobility because It is a radio frequency based wireless networking technology.

The biomedical information gathered by Low-power wireless sensor nodes used in WBAN is used for different applications in residential, and work environments and hospitals. Primarily WBAN applications are divided in to two categories i.e., medical and nonmedical ones. Medical applications need to collect vital information of a patient continuously and forward it to a remote monitoring station for further analysis. This huge amount of data can be used to treat various diseases such as cancer, gastrointestinal tract, neurological disorder and asthma, and also occurrence of myocardial infarction can be prevented.

Data file transfer, monitoring forgotten things, social networking and gaming applications is included in nonmedical applications. For example, in gaming, coordinate movements of different parts of the body can be collected by using sensors in WBAN and movement of a character in the game can be made subsequently. For example, moving soccer player or the intensity of a ball in table tennis can be captured. Allowing people to exchange digital profile or business card by shaking hands in social networking shows the use of WBAN.

When the authorised user wants to access and share any services such as healthcare, military etc he should access through Application provider from client through network manager which acts as a private key generator .the doctors who are application providers need to know the bio information of the patients where as all personal information such as name and ID nos. must be kept unknown. In different words legal users must be allowed to preserve the privacy to maximum extent. Therefore one of the solutions i.e. effective to achieve this is Remote anonymous Authentication schemes.

A client is a software or hardware of computer that accesses services for service providers or Server and Application providers provide services of computer based to clients or users (customers) over a network. The network i.e. managed during the communication between two systems or wireless networks is called Network manager. Ensuring and confirmation of users identity is called Authentication.

II. RELATED WORK

Theoretically , anonymous authentication scheme can be implemented in Threshold ring signature scheme[2] presented a scheme for privacy preserve communication.Threshold ring signature scheme is used that allow a group of ‘t’ members to jointly sign a message anonymously in a ring of ‘n’ members as threshold ring signature scheme generation and verification is quite inefficient. But Efficient Threshold Ring signature (t,n) scheme is used through a system of t linear eqns and n variables can achieve unconditional signer ambiguity and is existentially unforgivable against adaptively chosen message attack and has much lower computational complexity.[3] has presented a survey paper on wireless body area networks where in these networks various sensors are attached on clothing or on the body or even implanted under the skin and also using a WBAN, the patient experiences a greater physical mobility and is no longer compelled to stay in the hospital. A paper on communications with wireless by using a scheme called authentication with improved and enhanced security anonymously is implemented in [4] where authentication used by user can withstand many attacks and provide user friendliness environment. And also based on bilinear pairings used in this paper is used in novel remote user authentication scheme [5]. For low power communications in mobile a secure and fast elliptic curve protocol (ECC)with authentication and with key agreement” is used implemented in [6].A concept of RFID known as radio frequency authentication schemes is used for privacy and security i.e. presented in [7]. And the project is implemented in java where the information of java card standards is presented in paper [9]. It has been shown that Cryptosystems with identity based schemes with signatures is enhanced over ECC-based schemes (Elliptic curve cryptosystems) in [10]. To avoid the limitation of ID-based cryptography, public key signature without certificates i.e. easy and systematic was introduced in [11] as this scheme does not need certificates for authentication. And D.Y. Long, C.J. Wang, , and Y. Tang[12], proposed bilinear pairings by an signature scheme with an efficiency called CLS where pairing can be computed, as by claiming efficiency is improved, that are used as parameters of the system.

III .OVERVIEW OF EXISTING SYSTEM

The information i.e. biological in WBAN are gathered by the sensors like heartbeat rate and blood pressure in and around the body and it gets transmitted to body area network controller nodes(BAN) i.e. outside , such as smart phones and PDA, that acts as a gateway for anonymous access to the services of servers and external networks .The cryptosystems with public key i.e. traditional implemented remote user authentication Extra computation is needed for the users to validate others certificates. For better performance different method authentication has been presented depending on cryptosystem called as elliptic curve (ECC) The disadvantages are leakage of private information is one of the major concerns of potential users.Main issue is WBAN's unique characteristics and there are threats and many new vulnerabilities which is secure because of signal noise, mobile terminals, open medium channel and flexible infrastructure. Traditional public-key cryptosystems (PKC)-consume more computational resource. Elliptic curve cryptosystem (ECC)- require a certification authority (CA), need extra computation.

VI. PROPOSED SYSTEM

To provably secure against existential forgery in the random oracle model for adaptively chosen message attack, and to be cost effective and efficient, the cryptographic primitive such as new CLS scheme is developed. The design basis for two remote anonymous authentication protocols is served by the proposed CLS scheme, suitable for resource-constrained mobile clients.Example: Healthcare services, Anonymously accessing and sharing medical services by authorized patients in applications such as remote healthcare services, information such as name and ID number must be kept private where the doctors only should know the bio-information of the patient. Therefore Remote anonymous authentication schemes are one of the most effective solutions to achieve privacy. To preserve the privacy to the maximum extent, legitimate users are one of the legal users allowed to preserve the private information. The Advantages are summarised as follows:

- Its computed, coherent, verified and secured against forgery i.e. existent
- Network manager and application provider private information cannot be leaked and it is prevented.
- Soundness and performance of the similar designs is examined.
- Anonymous account index records is used instead of WBAN client real identity, to access the WBAN services,

V. PUBLIC KEY SYSTEM WITHOUT CERTIFICATES (CLS)

Public key systems without certificates is introduced in contrast to public key system with traditional , here cryptography with cetificateless does not require certificates to ensure the public key authentication and it depends on the existence of third party called network manager (NM) who will be having a master key.

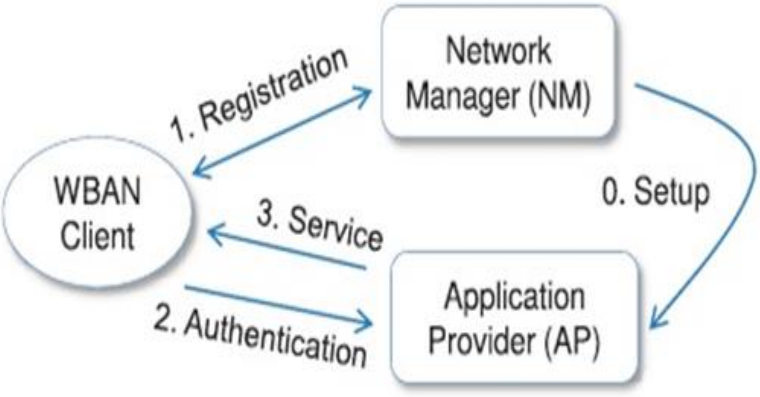


Fig 1.Working flow in Anonymous Authentication protocol

VI. ANALYSIS OF SYSTEM

For a problem to find out a best solution, Analysis is one of the processes. The project is run or started with the good software environment; this is done for the complete performance of the work of project. Primarily the operating system is Windows XP/7, and the main aim of this project is to authenticate the communication between client and application provider through Network manager (NM) .By using two protocols called as preliminary version and enhanced version the project works on. Running of above protocols and Comparison of time shows the performance analysis

A. *Study Of Feasibility*

The feasibility study depends on the primary investigation of the results. According to meet the needs with ability and resources with effective use, organization impact, and workability, feasibility study is a test of proposal of the system.

B. *Economic Feasibility*

The proposed system that provides the organization a positive economic advantage determined by assessment of economic feasibility is the main purpose. The benefits or cost analysis is involved by assessment. The products with customization are purchased.

- We need 3 PCs or systems with recently updated configuration, good performance, and Windows XP/7 OS to run the project
- Physical devices are not used in this project for connection, therefore it is feasible economically.

C. *Technical Feasibility*

The technical feasibility is checked for this system by studying about the technical requirements needed for this project or system. When any of the system is developed technical resources available should not be in high demand and when demands are high, it is placed on client. The system when developed, it should have modest requirements so when system is implemented only null or minimal changes are required. Some points are used regarding technical analysis which focuses on:

- **Some Changes should be done in the system:** The efficiency level will get increased and service for the customer should be better and in positive direction the changes should be done.
- **Skills Required:** Programming language, tools and platforms are widely used in this project used in this project and in the industry manpower with skillness in the industry are available.
- **Acceptance:** From the users view the problem should not be there so that the systems structure is feasibly enough.

VII. DESIGN OF A SYSTEM

1) *Design Objective*

The main aim is the communication between WBAN client and AP (Application provider) should be authentic through network manager (NM) and it depends on an existence of third party called Network manager that serves as a private key generator in the authentication protocols. AP can offer services to the client when authentication is success using primary version protocol and security enhanced protocol by developing certificate less signature scheme.

2) *CLS Scheme(Certificateless Signature Scheme)*

This scheme consists of six algorithms:

a) ***Setup*:** System parameters are generated with $(l,G_{1,}\ G_{2,}q,P,e,H,h,Q_{PKG})$ where l is the security parameter, G1 and G2 indicate the cyclic groups of prime order $q>2^{l,}$ P is the generator of G1, The pairing operator $e : G_1{*}G_1 \rightarrow G_2$ satisfies the properties of bilinear and non-degenerate. Two secure hash functions are $:H:\{0,1\}^* \text{ x } G_1 \rightarrow G_1$ and $h:\{0,1\}^* \text{ x } G_2 \rightarrow Z^*q$ .The random integer is picked $s_{PKG} \in Z^*q$ as the master key-private key and $Q_{PKG} = s_{PKG}P$ as the public key is computed, as s_{PKG} is kept secret.

b) ***Partial private key is set*:** $s_1 \in Z^*q$ is set as partial secret key.

c) ***Partial public key is set*** **:** $Q_{1 =} s_1P$ is set as partial public key

d) ***Extract of partial private key*:** it is performed by PKG when a requests comes from signer parallel to his identity. Suppose the identity of signer is given by string id,i.e. the other partial public key. So the partial secret key is then given by
$S_2= s_{PKG}Q_{2,}$ where $Q_2= H(id, Q_1)$, PKG computes the value of Q_2 and in a secret key it is sent to the signer.
For a signer, (id, Q_1) is public key and (s_1,S_2) is private key. The above step of extraction is done once for each identity

e) ***CL sign*:** The signer selects a integer randomly $k \in Z^*q$ to get a message m. The following is computed as follows:

1. $r = e(Q_2,Q_{PKG})^K$-------------1
2. $v = h(m||r, P)$--------------2
3. $U = kS_2 - vs_1Q_2$--------------3

The pair $(v,U) \in (Z^*q, G_1)$ is taken as signature.

f) ***CL verify*** **:** when the message m is received and (v,U) signature, the following way is performed:

1. $Q_2= H(id, Q_1)$, is computed-------------4
2. Signature is accepted iff $v = h\ (m||\ e(U,P)\ .\ e(Q_2,Q_1)^v\ ,\ P)$----------5
3. The proposed CLS scheme assures completeness by checking the verification eqn that supports a valid signature.

$v = h(m \| e(U,P)\ \ .\ e(Q_2,Q_1)^v,P)$
$= h(m \| e(kS_2 – vs_1Q_2,P)\ .\ e(Q_2,vs_1P),P)$
$= h(m \| e(ks_{PKG}Q_2, P),P)$
$= h(m||\ r, P)$--6

This section presents our new architecture for a system choosing waterfall model as a development model.

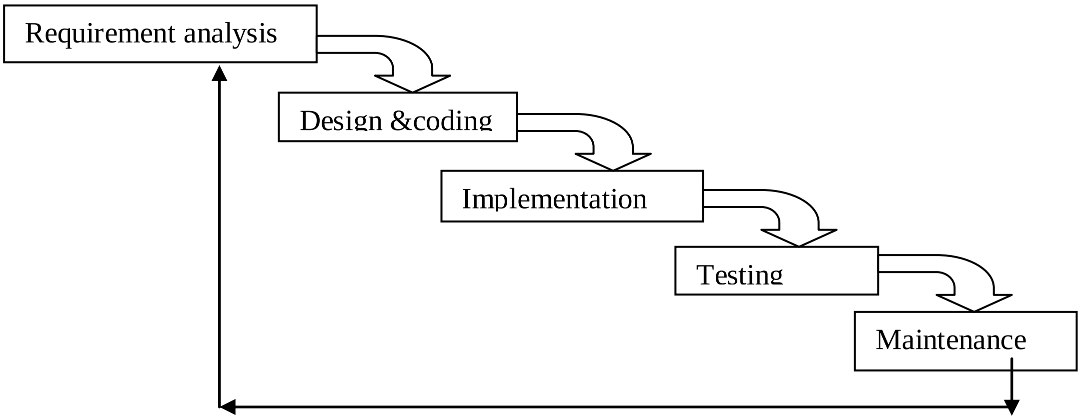


Fig 2. Waterfall Model

3) *Architecture Of The System*

To define the structure and system behaviour a design i.e. conceptual is called system architecture, a system with formal specification is the architecture specification.i.e organised in a manner that supports the structural system properties by reasoning

The System architecture is shown below.

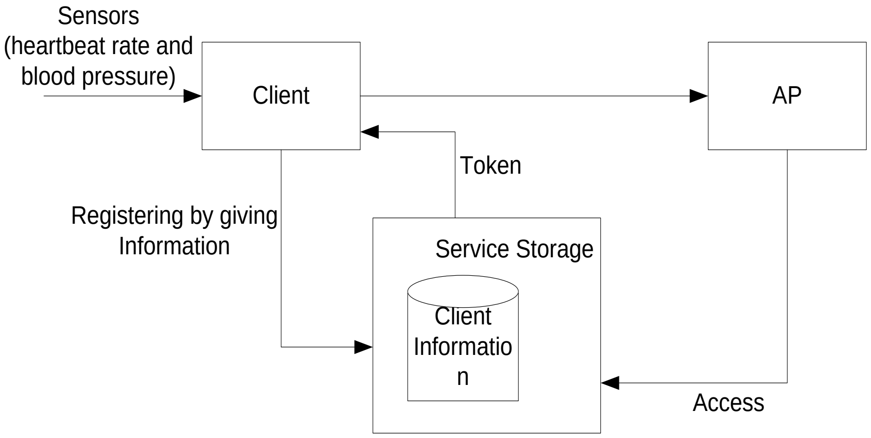


Fig 3: Architecture Design

The client receives information from the sensor which is wireless body area network for instance like heartbeat rate and blood pressure. This biomedical information which is gathered from the sensors is transmitted to the service storage for instance patient register in the reception. After registration, the reception list will provide tokens to the patient. Meanwhile, the Application provider for example nurse, physician will access the service storage patient information and calls the patient for check up with the doctor. The application provider will not reveal the true identity of users even given all the session information. The certificateless signature scheme has a potential to achieve more desirable security properties with less computational cost than the existing schemes.

4) *Primary version Authentication protocol*

This protocol uses the CLS scheme proposed in section 2; an account index is generated by NM for WBAN client request used for generation of signature and verification. The signature is generated using the account index for the client's request. When client wants to login , it needs to send the signature given by NM with the account index to the corresponding AP as it verifies the signature of client using account index and NMs signature by NMs public key. Here the role of AP is to verify the generated signature and it does not reveal the real identities of user. It consists of initialization, registration and authentication. So the protocol is described in reference paper [1] presented in 2014

5) *Security Enhanced Authentication Protocol*

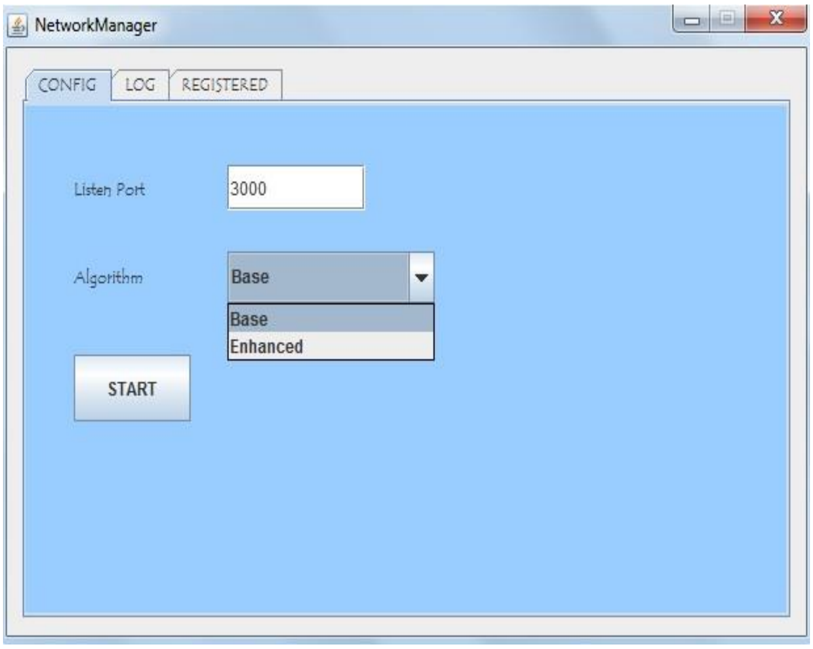
In primary version , the authenticated information requested that includes the account index and corresponding features of client is carried out in message request. So this allows adversary to determine whether two various sessions are initiated by same client and also NM can find the clients real identity from the session information .To avoid this vulnerability, security enhanced protocol is used that consists of Initialization, registration and anonymous authentication. The above named protocol is described in reference paper [1] presented in 2014.

VIII. SYSTEM IMPLEMENTATION

The design which is theoretical i.e. turned into system in working is called implementation, which is the projects main stage. In this section to evaluate the computation overhead of proposed schemes, the hardware and software requirements are setup. They are listed as follows : Processor: Pentium 4, Speed of processor: 2.50 GHz , Ram: 512MB , Storage: 40GB, Monitor: 15", Programming Language : Java , Platform for programming : Jdk, Name of tool: Netbeans IDE 7.2 Operating system: Windows XP/7, Interface for front end: Swings

IX PERFORMNACE AND RESULTS

Fig 4 shows the Network manager module by displaying to select base or enhanced version for registration of client and AP. And fig 5 shows the generation of system parameters by NM.Fig 6 shows the NM module after registration, fig 7 and 8 compare the run time of base and enhanced version protocols. The results demonstrate that the two authentication protocols outperforms the other protocols by offering a better comparison time between two versions where this ensure thar security enhanced protocol takes less running time when compared to preliminary version.

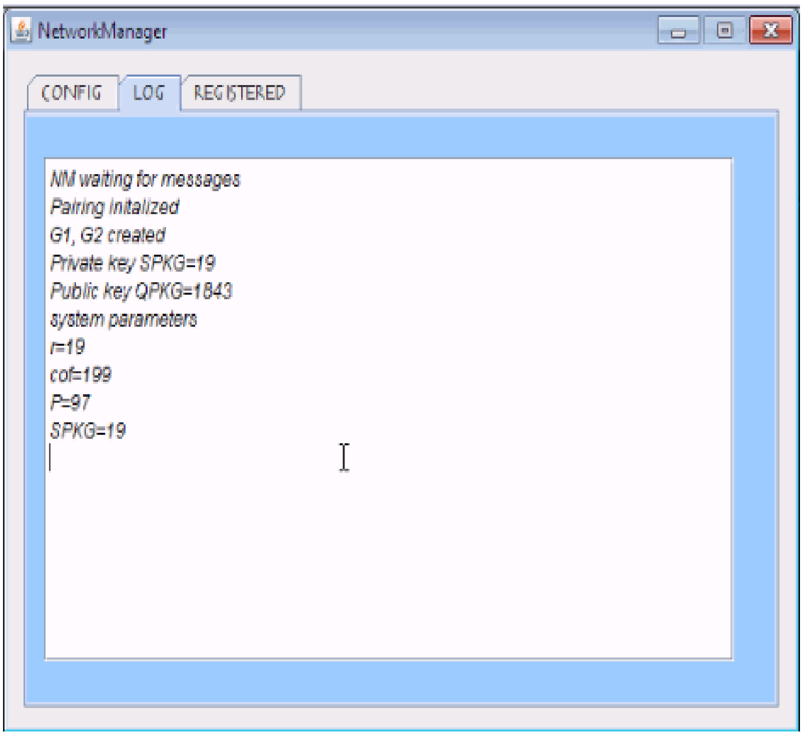


Listen Port 3000

Algorithm Base

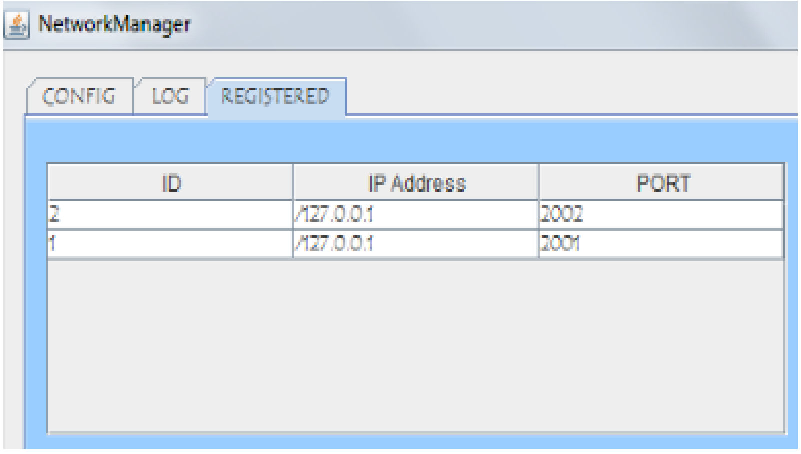
Base
Enhanced

Fig 4: Network manager module for registration



```
NM waiting for messages
Pairing intialized
G1, G2 created
Private key SPKG=19
Public key QPKG=1843
system parameters
r=19
cof=199
P=97
SPKG=19
```

Fig 5: NM generated system Parameters



ID	IP Address	PORT
2	/127.0.0.1	2002
1	/127.0.0.1	2001

Fig 6: NM module after Registration

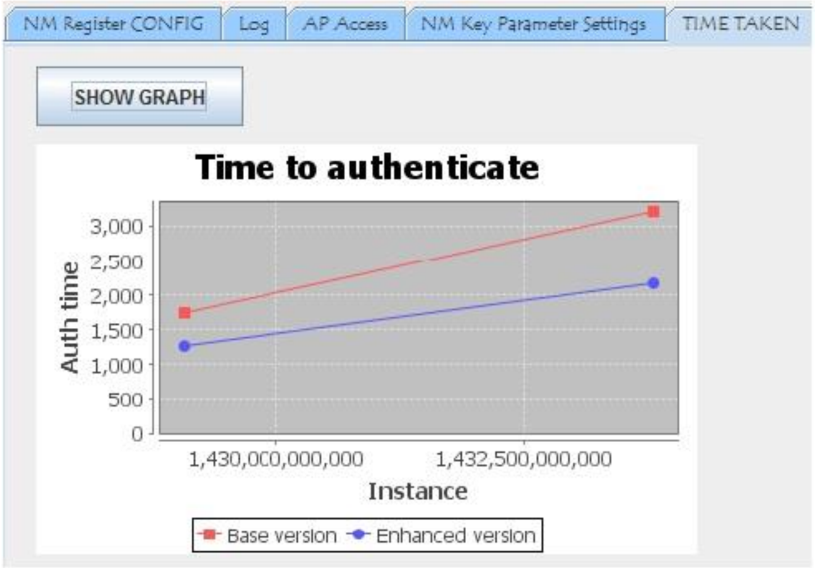


Fig 7: Comparison time graph between primary and security enhanced protocol in WBAN client terminal

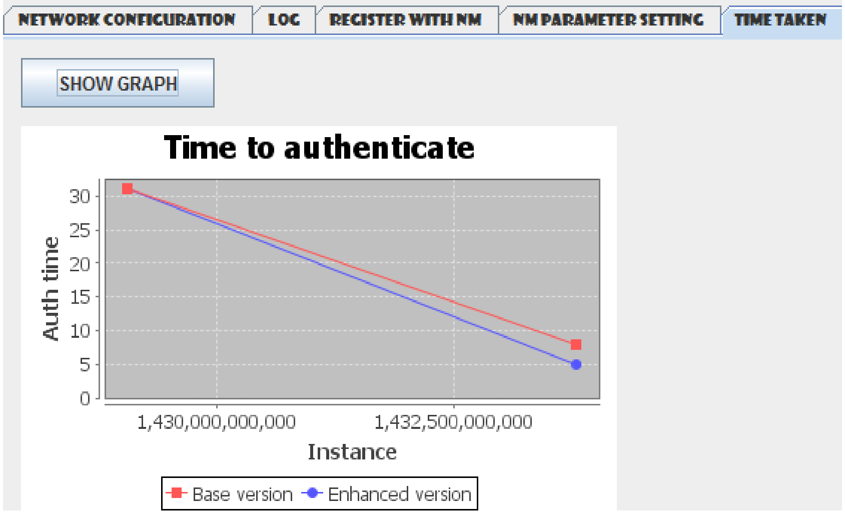


Fig 8: Comparison time graph between primary and security enhanced protocol in AP

X. FINAL OUTCOME AND FUTURE SCOPE

Here two protocols are used authentically in distant to keep the privacy of potential users in wban while they access network medical service through WBANs terminals. To design the protocols, we developed a novel certificate less signature scheme as a cryptographic primitive by carefully exploring the special characteristics of WBANs. We formally proved that our certificate less signature scheme has a potential to achieve more desirable security properties with less computational cost than the existing schemes. One salient feature of our protocols is that service or medical application providers do not have advantage to reveal the private information of users even when all the session information given. Private Key generator (PKG) served by Network manager cannot imitate legal users. Theoretic analysis, experimental simulations and comparative studies are conducted and evaluated for the proposed protocols, which outperformed most of the existing authentication schemes, where Implementation, running time, security and estimation cost shows better balancing between two authenticated protocols. Here in this project 3 systems or PCs are configured with software and communication goes on between them authentically using the particular systems IP address, where AP can offer services according to clients request when authentication is successful.

A set of many experimental scenarios in realistic can be developed to test this project as it is an added advantage for research community of WBAN.

Acknowledgement

Madhusudhan U R, thanks to Mrs. Keerthana B , Assistant professor and Mrs.Poonam Tijare, Assitant Professor , Dept of CSE, CMRIT, Bangalore, who is always encouraging and motivating me to do research activities, I am also very thankful my families and friends

REFERENCES

[1] Jingwei liu , Zonghua Zhang, Xiaofeng Chen and Kyung Sup Kwak ," Certificateless Remote Anonymous Schemes For wireless Body Area Networks" IEEE Transactions, vol 25, no.2, pp.332-342,Feb-2014.

[2] J. Ren and L. Harn, "An Efficient Threshold AnonymousAuthentication Scheme for Privacy-Preserving Communications,"IEEE Trans. Wireless Comm., vol. 12, no. 3, pp. 1018-1025, Mar.2013.

[3] M. Seyedi, B. Kibret, D.T.H. Lai, and M. Faulkner, "A Survey on Intrabody Communications for Body Area Network Applications," IEEE Trans. Biomedical Eng., vol. 60, no. 8, pp. 2067-2079, Aug. 2013.

[4] Cong Liu, Fu-shan Wei , Chuan-gui Ma," Improved Anonymous Authentication Scheme with Enhanced Security for Wireless Communications" Advances in information Sciences and Service Sciences(AISS) Volume4, Number13, July 2012 doi: 10.4156/AISS.vol4.issue13.34

[5] C. Yang, W. Ma, and X. Wang, "Novel Remote User Authentication Scheme Using Bilinear Pairings," Proc. Fourth Int'l Conf. (ATC '07), pp. 306-312, 2007.

[6] P. Abichar, A. Mhamed, and B. Elhassan, "A Fast and Secure Elliptic Curve Based Authenticated Key Agreement Protocol for Low Power Mobile Communications," Proc. Int'l Conf. Next Generation Mobile Applications, Services and Technologies, pp. 235- 240, 2007

[7] Ari Juels "RFID Security and Privacy: A Research Survey" RSA Laboratories, 28 September 2005

[8] F. Armknecht, L. Chen, and A. Sadeghi, "Anonymous Authentication for RFID Systems," Proc. Sixth Int'l Conf. Radio Frequency Identification: Security and Privacy Issues (RFIDSec '10), pp. 158-175, 2010.

[9] P. Bichsel, J. Camenisch, T. Gro_, V. Shoup, "Anonymous Credentials on a Standard Java Card," Proc. 11th ACM Conf. Computer Comm. Security, pp. 600-610, 2009.

[10] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (Crypto '84), pp. 47-53,1984.

[11] Z. Zhang, D. Wong, J. Xu, and D. Feng, "Certificateless Public-Key Signature: Security Model and Efficient Construction," Proc. Fourth Int'l Conf. Applied Cryptography and Network Security (ACNS '06), pp. 293-308, 2006.

[12] C.J. Wang, D.Y. Long, and Y. Tang, "An Efficient Certificateless Signature from Pairings," Int'l J. Network Security, vol. 8, no. 1, pp. 96-100, 2009.

.

Author Profile

Madhusudhan U R received the B.E degree in Computer Science and Engineering from NMIT, Bangalore in 2011 and M.tech degree in Computer Science and Engineering Pursing in CMR Institute of technology, Bangalore in 2015, respectively.

Mrs. Keerthana B is working as a Assistant professor of CSE Department in CMR Institute of Technology, Bangalore.

Mrs. Poonam Tijare is working as a Assistant professor of CSE Department in CMR Institute of Technology, Bangalore.