ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 10, March 2016

SCALABLE AND SECURE CERTIFICATELESS REMOTE AUTHENTICATION PROTOCOL FOR SHARING OF PHR USING WBAN

*N.Ramila
Sun college of engineering and technology ramilanatarajan@gmail.com

ABSTRACT-Wireless body area network (WBAN) has been recognized as one of the promising wireless sensor technologies for improving healthcare service. It is critical to secure the extra-body communication between the smart portable device held by the WBAN client and the application providers .Due to the lack of security users worry about the leakage of their private information, especially to those unauthenticated or even malicious adversaries .A certificate less encryption scheme and a certificate less signature scheme with efficient revocation against short-term key exposure for WBAN users to anonymously enjoy healthcare service. Our authentication protocols are used by certificate less signature (CLS) scheme, which is computational and more efficient. Also, our designs ensure that application or service providers have no privilege to disclose the real identities of users. Even the network manager, which serves as private key generator in the authentication protocols, is prevented from impersonating legitimate users. The performance of our designs is evaluated through both theoretic analysis and experimental simulations, and the comparative studies demonstrate that they outperform the existing schemes in terms of better trade-off between desirable security properties and computational overhead, nicely meeting the needs of WBANs.

KEYWORD: WBAN, Security, Signature, Authentication, KGC, Encryption, Decryption and Protocol.

I.INTRODUCTION

Wireless body area network:

The rapid advancement in intelligent physiological sensors and wireless communication technology has the potential to improve the quality of life significantly by allowing chronically ill, children and elderly to be monitored and treated continuously and remotely. With the tiny medical sensor nodes implanted inside or worn on human body and the smart portable device (SPD) held by the patient, a self-organized wireless body area network (WBANs) can be formed to monitor the health status and the surrounding environments of human bodies. Intra-body communications and extra-body communications are two basic communication modes in WBANs, which respectively allow sensors to communicate with each other and the SPD, and enable SPD to communicate with the remote application providers (APs) such as the hospital, physician or medical staff .Possible applications of WBANs range from long-term daily living monitoring to location tracking and medical status monitoring. Despite of the potential benefits, it is desirable and more prudent to secure WBANs due to the sensitive nature of the medical data collected by WBANs, one medium of the communication channel and the ad-hoc nature of the WBANs.

II. RELATED WORK

Mir HojjatSvyedi, BehailuKibret[7]. Intrabody communication (IBC) is an alternative wireless communication technology which uses the human body as the signal propagation medium. IBC has characteristics that could naturally address the issues with RF for BAN technology.JeongGilKo, Chenyang Lu [5].Different from the previous protocols in this field, our protocol not only provides mutual authentication, session key establishment, anonymity, unlink ability, and non-repudiation, but also achieves forward security, key escrow resilience, and scalability. Performance evaluation demonstrates that compared with the most efficient ID-based remote anonymous authentication protocol.

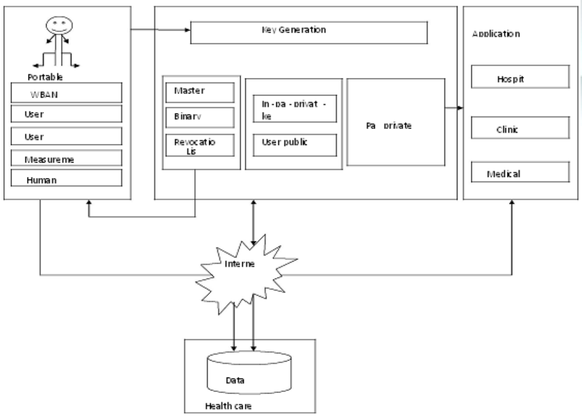
Daojing He, Sammy Chan[2] Personal health information (PHI) is collected by biosensors and delivered to the PWH before it is forwarded to the remote healthcare center for further processing. In a BSN, it is critical to only admit eligible biosensors and PWH into the network.Divya R &Sundararajan T.V.P[4] In Body Area Network, sensors are used to monitor the human's activities and their actions like health parameters so it is necessary to secure the privacy of the user and the necessary information are collected by the sensors from the body of the user.

Basavashri B, ManjulaM[1] Wireless body area network is one of the wireless sensor technologies for the health care service. the leakage of privacy is one of the main issue in WBAN especially to those unauthenticated or even malicious adversaries in order to provide the security to theWBAN users in this paper we are developing a new certificate less remote anonymous authentication protocol to give the strength to remote WBAN users to anonymously enjoy the health care service.

DivyashikhaSethia, Huzur Saran [3] i) Secure Medical Tags for reducing medical errors and ii) Secure Healthcare for storing Electronic Health Record (EHR) based on Secure NFC Tags, mobile device using NFC P2P Mode or Card Emulation Mode.Wei Gao, Guilin Wang[9]The round-complexity of the threshold signing protocol is optimal since each party pays no other communication cost except broadcasting one single message.ZhoaoyangZang, HonggangWarg[10].The improved Jules Sudan (IJS) algorithm is proposed to set up the key agreement for the message authentication. The proposed ECG-IJS key agreement can secure data communications over BANs in a plug-n-play manner without any key distribution overheads.

Ming Li ,Wenjing Lou[6]. WBAN has shown great potential in improving healthcare quality, and thus has found a wide range of applications from ubiquitous health monitoring and computer assisted rehabilitation to emergency medical response systems.Qiaoyan Wen &Hua Zhang[8]. WBAN technology gives the main advantage of mobility to the user and at the same time the health of the user is monitored. The main research challenges in BAN design is personal health security, also transmitting amounts of valuable and confidential data between WBAN nodes through wireless channel puts the data at serious risk of theft, sabotage, exploitation and manipulation.

III. PROPOSED METHODOLOGY



By examining the characteristics of WBAN and considering the existing remote authentication schemes here we develop a new certificate less signature (CLS) scheme which is cost effective, efficient and secure. This CLS scheme then serves as a design basis for two remote anonymous authentication protocols. Here the protocol use anonymous account index instead of WBAN clients real identity to access WBAN service.

The system architecture of WBAN in order to get a treatment from the physicians, emergency center primary care provider initially WBAN client has to attach the sensors to their body the information that is collected in the sensors is transferred the computer, mobile phones or pda the collected information is then transferred to the physician's tele medicine services in order to provide the secure communication between the client and the physicians here proposing two remote anonymous authentication protocol. Initially the WBAN client has to send the registration request to the network manager.

(Step 1)Network manager reply's to client by giving a ticket to get the treatment from the application provider (step 2).once the client gets the permission from network manager then he will authenticate with application provider (step 3) here the application providers are the physicians, emergency centers. If the authentication request received by the client is valid then application provider replies to client whether the authentication is successful or not to (step 4).

WBAN SETUP

The WBAN technology is the consequence of the existing WSN technology. A number of tiny wireless sensors, strategically placed on the human body, create a wireless body area network that can monitor various vital signs, providing real-time feedback to the user and medical personnel. In a WBAN, each medical sensor monitors differential signs such as temperature, blood pressure, or ECG. The system consists of multiple sensor nodes that monitor body motion and heart activity, a network coordinator, and a personal server running on a personal digital assistant or a personal computer.

Data collected by the medical sensors is transmitted to the coordinator. The sensors are always activated and continuously transmit data to the coordinator. This configuration causes high energy consumption in all medical sensors and reduces their operational time. The WBAN architecture presented in several key Components. Different types of medical sensors can be used for monitoring various vital parameters. Figure represents the other form of WBAN in which data from the multiple nodes transmitted through the internet to multiple clients.

KGC Update key

KGC center provide key updating for clients .its receives the input public key from WBAN sensors and generate Ini-pri-partial key .KGC generate new key both combination of public key and random generation encryption code and update for the application provider

CERTIFICATELESSIGNATURE SCHEME

It provide the security for wireless body area network we use our new certificate less signature scheme to design a remote anonymous authentication protocol. The authentication protocol preserves the anonymity for WBAN client. A certificate less signature scheme consists of six algorithms:

Setup: This algorithm is done by network manager so he will acts as a private key generator (PKG).

- G1 and G2 be a pairing operator
- Let l be a security parameter.
- PKG picks a random integer SPKGЄZq* as its private key
- Then he computes QPKG=SPKGP as its public key
- Then he publishes system parameter where SPKG is kept secret.

Set partial private key: Here the signer is client he selects a random integer s1Єzq as his partial secret key.

Set partial public key: Here the client computes Q1=s1P has its partial public key.

Partial private key extract:

- This algorithm is performed by network manager. When a client request the secret key to his identity (ID) network manager computes the other secret key to client. Where ID is the other partial public key of the client.
- Secret key of the identity is given as S2=SPKG Q2 where Q2=H (ID,Q1).Both secret key and public key is given to the signer in a secret channel.
- For a signer <ID, Q1> is public key and <S1, S2> is private key

CL-SIGN:

- To sign message the signer chooses random integer k € Zq and computes as:
  r=e (Q2, QPKG) K

  v=h (m‖r,p)
  U=KS2- vs1Q2
  The pair (v, U)є(ZQ*,G1) is considered as signature

CL-VERIFY: This algorithm is computed by the application provider and he will acts as a verifier. On receiving the message m and signature <v,U> the verifier computes:

Q2=H (ID, Q1)
Accepts the signature if and only if:

V=h (m ‖r, p)

AUTHENTICATION PROTOCOLS FOR WIRELESS BODY AREA NETWORK:

Preliminary version authentication protocol:

The protocol takes a new certificate less signature scheme as a design basis .Network manager initially generates an account index for each requesting WBAN client and uses it for signature generation and verification. If client wants to login he needs to send the signature of the message issued by the network manager along with the account index to the corresponding application provider. Application provider then verifies the client's signature using the account index and the Network manager (NM) signature by NM public key. It is obvious that the role of AP is only to verify the generated signature, and the information in hand does not allow it to recover the real identity of the client

Initialization Phase: This is the initial step in the preliminary version authentication protocol takes place by network manager which generates key and establishes the system parameter. By considering the security parameter l NM determines its public, private pair(QNM,SNM).Where QNM=SNM P and gives the system parameter as <l, G1,G2, q, P, e,H, h,QNM> as defined in the certificate less signature algorithm. Application provider also as a key pair as<QAP,SAP>where QAP=SAPP.

Registration phase: This step is performed by the WBAN client with network manager to access an application provider. The following step should be performed in the registration phase. In this step WBAN client chooses his own partial private key while obtain another partial private key using an algorithm partial-private-key-extract. Network manager then issues a ticket=<m,σ> to client where m=rightand σ is the corresponding signature on m.in the same way the WBAN client store a group of QAP for different application provider.

Authentication phase: The WBAN client performs the following steps to anonymously authenticate by himself to the application provider.

- Selects a random K, t Є Z q* and compute T=tPandT'= tQAP
- Pick up the current time tc of the requesting WBAN terminal. then calculates v=h(σ| | tc| | r,T)
- Computes U=KS2-vs1Q2.
- Computes the session key=h (v,T).
- Send the request message as(v, U, m, σ, tc, T')
- When the AP receives Req(v, U, m, σ,tc, T') it Checks the validity of <M, σ> and tc.
- Then AP rejects the request if m and tc are not valid. Otherwise, the AP does the following:

- Verifies v=h(σ||tc||r,T)
- Computes the session key=h(v,T)
- Compute MAC key(V) as the reply. On receiving the reply from application provider WBAN client checks the integrity of MAC key(V) with session key WBAN client quits the current session if it produces negative result otherwise WBAN client authenticates with the application provider.

SECURITY ENHANCED AUTHENTICATION PROTOCOL:

In the preliminary version, all the requested authentication information, including the account index and the corresponding right of the client, is carried in the request message. This may allow one sophisticated adversary to determine whether two different sessions are initiated by the same client, and may also allow NM to trace the client's real identity from the session information to avoid this here we are proposing security enhanced authentication protocol. This protocol also consists of three phases like initialization, registration, and authentication phase.

Initialization phase: Initialization phase is same as like preliminary version authentication protocol.

Registration phase: This process is as the same as preliminary version but NM issues <I, indcv, right> to AP, where I =indcvP, instead of sending a ticket<m, σ> to client

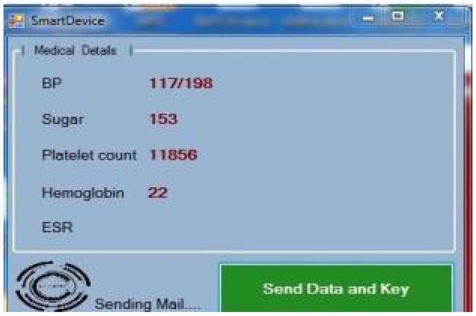
Authentication phase: The WBAN client performs the following steps to anonymously authenticate him/herself to the requested AP

- Select at random k,t Є Zq* and computes T= t p,T'=tQAP and I'=I+T
- Pick up the current time tc of the WBAN client and computes v=h(tc||r,T)
  ComputesU=KS2-vs1Q2
  Computes the session key=h(v,T)
- Send a service request message Req = (v, U, tc, T', I ')

When the application provider receives the request it checks the current time of the requesting WBAN client and also computes the session key. If the current time tc of the requesting WBAN terminal is valid then AP accepts the request or else rejects the request. Then application provider computes MAC key(V) as the reply to respective WBAN client. When WBAN client receives the reply message from the application provider it checks the integrity of MAC key(V) with session key if the integrity is not valid then WBAN client will not authenticate.

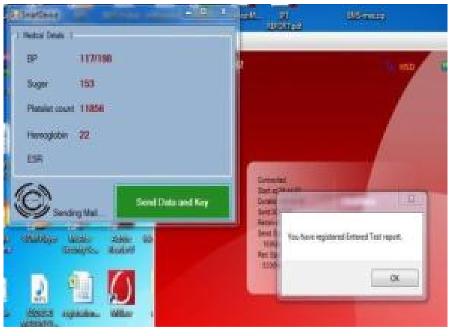
IV.EXPERIMENTAL RESULTS

The protocol takes a new certificate less signature scheme as a design basis .Network manager initially generates an account index for each requesting WBAN client and uses it for signature generation and verification. If client wants to login he needs to send the signature of the message issued by the network manager along with the account index to the corresponding application provider. Application provider then verifies the client's signature using the account index and the Network manager (NM) signature by NM public key. It is obvious that the role of AP is only to verify the generated signature, and the information in hand does not allow it to recover the real identity of the client.In the preliminary version, all the requested authentication information, including the account index and the corresponding right of the client, is carried in the request message. This may allow one sophisticated adversary to determine whether two different sessions are initiated by the same client, and may also allow NM to trace the client's real identity from the session information to avoid this here we are proposing security enhanced authentication protocol. This protocol also consists of three phases like initialization, registration, and authentication phase.



BP	117/198
Sugar	153
Platelet count	11856
Hemoglobin	22
ESR	

Sending Mail....



Medical Details

BP 117/180

Sugar 153

Platelet count 11856

Hemoglobin 22

ESR

Sending Mail...

You have registered Entered Test report.

V.CONCLUSION

Thus discussed various security approaches to secure Body Area Network. We have discussed many user public key, Ini-pri key and hybrid key security mechanisms in BAN. The detail comparison among these approaches is also done . Various approaches are also used to secure BAN. Further work has to be done to make it more secure and efficient network. In future there is a requirement of a protocol which is more efficient and more secure than existing protocols for Body Area Network.

REFERENCES

[1] Basavashri B, Manjula M, Vol-2, Pg-1981(IORJET), Jun-2015, “Ensuring Certificate less Remote Anonymity and Authenticity wireless Body Area Network”.

[2] Daojing He, Sammy Chan, Vol- 17, Pg-664, May- 2013, "Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks ".

[3] DivyashikhaSethia, Huzur Saran, Vol 1, Pg-978, (IRJET), 2014, “NFC Based Secure Mobile Healthcare System”.

[4] Divya R &Sundararajan T.V.P, Vol -3, Pg-1502 (IJA RECE), Nov 2014, “Security Mechanism in Body Area Network”.

[5] JeongGilKo, Chenyang Lu, Vol. 98, Pg- 11, Nov 2010 “Cost-Effective Scalable and Anonymous Certificateless Remote Authentication Protocol”.

[6] Ming Li &Wenjing Lou, Vol 2, Pg- 51, Feb 2010“Data Security and privacy in wireless body area network”.

[7] Mir.HojjatSvyedi&BehailuKibret,Vol- 60, Pg-2067, Aug 2013.”A Survey on Intra body Communications for BodyArea Network Applications”.

[8] Qiaoyan Wen &Hua Zhang, “Cryptanalysis and improvement of two certificate less three-party authenticated key agreement protocols”, Jan 2013.

[9] Wei Gao, Guilin Wang , Feb 2012, vol. 2595., “Efficient identity-based threshold signature scheme from bilinear pairings in the standard mode”.

[10] ZhoaoyangZang, HonggangWarg, Vol-17,Pg- 1070, Nov-2012 “ECG-Cryptography and Authentication in BodyArea Networks”.