ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

A Novel Group Digital Signature Authentication Protocol for Wireless Body Area Networks

[1] C. Rameshkumar, [2] A. Hemalathadhevi,[3]Dr .R.Viswanathan
[1][3] Assistant Professor, [2] Associate Professor
[1][3] School of Computer Science and Engg,Galgotias University, Uttar Pradesh, India
[2] Department of Computer Science and Engg, Meenakshi College of Engineering, Tamil Nadu, India

Abstract: Wireless body area networks (WBANs) are a key eHealthcare technology that allows patient's essential data to be together from the carrier or implantable biosensors. However, the protection and privacy of collected data is a major unresolved issue, as challenges stem from stringent resource constraints on biosensors and the high demand for security/privacy and practicality. Authentication protocol using a digital signature algorithm with a challenge response protocol that offers effective WBAN authentication. Based on public key infrastructure, In this paper group biosensor nodes (BNs) first, generate their public-private keys. The Designed Authorized Registrar (AR) generates the identifier code (gID) of the group biosensor identifier, the group identification tag, and the group secret key. Each group biosensor node (BN) retains its private key with signing ID. These parameters can only be provided by members who can sign and provide data authentication and non-retrieval for data transmission between biosensors. The signing protocol for the response identification signal with overlapping logical swap operation is proposed to guarantee that the signer receives a key group that is secure and prevents the making of false statements in the eHealthcare system.

Keywords- Wireless Body Area network; Group digital signatures; challenge response; public-private keys.

I. INTRODUCTION

The wireless network was introduced by TG Zimmerman for the first time in 1996. Such networks are initially set up since the Wireless Local Area Network (WPAN). The name of the physical network was reset, such as WBAN, instead of WPAN, or as far as about 3 meters [1].

In a Wireless Body Area Network (WBAN), miniature, low-power sensing element node area unit placed around a patient's deceased for watching their body functions and also the neighboring [2].With the assistance of a WBAN, a patient's healthiness connected info, together with their temperature, respiration, heart rate, pulse measuring device, pressure level, blood sugar, and pH are often remotely monitored [3]. To attain the most profit, this info should be incessantly processed in real time. The medical info should be shared and accessed by varied levels of users like tending employees, researchers, government agencies, and insurance corporations to create vital choices like clinical diagnoses and emergency medical responses for the patients.

The bio-sensors are to be found on a patient's body to convey sensing knowledge throughout a secure channel toward a small body space network gateway. The gateway then regionally processes the info and resends it throughout a protected channel toward the exterior network router with subsequently on to the medical server at the hospital. The results square measure then determined and analyzed by the medical staff/doctors charged with observance patients.A centralized management device is employed to transmit knowledge in and out of the network. This power device may moreover be used as an entryway between the interior network and also the establishment station.

The base location connects to the exterior network. The communication of health connected info between sensors lying on a patient's body in an exceedingly WBAN over the web to medical servers should be strictly personal and confidential. Authenticated medical knowledge transmissions are a unit essential need for a WBAN since an answer of false or unauthenticated medical info might result in incorrect treatments or diagnoses for patients[4]. Therefore, the transmitted info must be encrypted toward safeguard patient privacy. Additionally, the medical workers of the hospital that collect the information should be assured that the information area unit in-situ and so originate from the required patient. The most important challenge in an exceedingly WBAN area unit security, robustness, and quantifiability.The scale and supply constraint of the bio-sensors conjointly play a critical role in the success and responsibleness of a WBAN [5]. Healthiness care employees will directly access

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

knowledge of the body area network of an enduring when self-made authentication

User right to use control is crucial to the victorious operation and intensive approval of wireless body area network services.The protection framework designed for a WBAN ought to encompass user authentication (identity verification), user authorization (access provided to the user) and user responsibleness (monitoring activity and dominant access) to handle user access with forestalling differing kinds of attacks [6]. User access management will determine and impose completely different access privileges for various forms of users.During a typical WBAN, completely different health center, healthiness care workers, and medical nondepository financial institution agents area unit the foremost users, but access toward a few or the entire medical info of a specific patient might not be needed for every kind of users. For instance, an involved doctor will retrieve his/her patient information, however no different patient info.

This paper structured in four sections. Section I provide a transitory introduction happening WBAN and highlights. Section II describes the connected work of the projected techniques and the composition of the planned group digital signature system is explained in section III attracts general design of this technology.Section IV discusses implementing projected cluster signature subject in WBAN and also the conclusion of this paper is conferred within the section V.

II. RELATED WORK

Several analysis teams are developing the implantable or wearable devices for health observation in WBAN communications. However, these researchers primarily specialize in building system design and to the lesser extent in developing networking protocols. Besides, it's tough to find solutions, providing security for WBAN and security has typically been lined on an individual basis.

Liu, Bin, et al[7]. Mentioned varied sensible problems needed to meet the safety and privacy necessities in WBANs. They explored the relevant security solutions in sensing element networks and WBANs whereas analyzing varied applications. They planned Associate in nursing attribute-based encoding for achieving fine-grained access management. This can be a one-to-many encoding technique wherever the ciphertext is just decipherable by a bunch of users that satisfy an explicit access policy.

Mahmud and Morogan[8]. Projected an identity-based user authentication and access management protocol supported an identity-based signature (IBS) theme. They used ECC code primarily based digital signature algorithmic program (DSA) for language and confirmatory a message. At data formatting, sensing element nodes and users were registered to a base station and cluster identity and user access rights were additionally provided by the bottom station. User revocation was enforced through the expiration of user time interval as allotted by the bottom station at the time of registration. Each user wasn't allowed to achieve access while not the right access rights. Although their theme was secure against node capture and denial-of-service (DoS) attacks, the password amendment method wasn't supported. for brand new user additions, the base station required to send user parameters like user ID, cluster ID and system time stamp, therefore acquisition additional communication overhead within the network.

Mishra, Dheerendra et al[9]. Projected Associate in ECC-based user access Control scheme. During this method, the client should register through the key delivery center (KDC) used for access authorization before verification. The KDC control and maintain a client entrée list group through the individual user's right of entry freedom. They give access privilege consists of user ID, cluster ID and a user access privilege mask; multiple users at intervals identical cluster ought to have identical access privilege.Supported elliptic curve cryptography, the KDC generates the common public key, the personal input of the user and also the access list certificate, supported the user's request. The user requests the detector node by causing the certificate; the detector node then selects one random variable as a session key. During this theme, the user authenticates a detector node and a detector node additionally authenticates the user; mutual authentication is therefore provided between the user and also the detector node.

J. Liu, Z. Zhang, et a[10].Projected associate energy-efficient right of entry Control system supported ECC that improved on Wang et al. Their theme was a private key in cryptography based mostly access management theme wherever the user should settle for access permissions from a key delivery center (KDC). The KDC maintains an associate access Control list (ACL) team and related client identifications. The user's right of entry privileges square measure outlined within the ACL supported the user's access privilege mask. The general private keys between the KDC with also the detector nodes square measure reciprocally changed throughout the pre-

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

deployment section. Once registered, the user gains a public and personal key.One signed certificate of the access management list is additionally issued via the KDC with sent to the user. The user should then be genuine by the detector node for future communications.

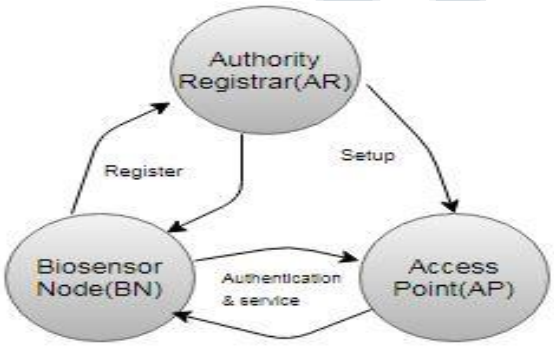
In the history decade, some grouping signature technique contains be proposed.Chaum with van Heyst [11] first propose four cluster signature schemes that area unit supported resolution resolving and distinct index issues.However, 2 drawbacks exist: (1) the cluster manager should collaborate with cluster members within the case of dispute; (2) connexion new members or deleting previous members has to modification key sizes of the cluster. 2 economical cluster signature schemes [12] [13] are also supported resolution distinct index mathematical issues. However, they need identical problem: the sizes of secret keys of the cluster member can increase with the number of signatures.Two economical cluster signature techniques for big teams [14-15] area unit projected to resolve this downside. L. Chen and T. Pedersen [16] propose another information-theoretic cluster signature theme. However, this system permits the cluster manager to sign messages within the name of any members of a cluster.Moreover, some offensive the prevailing cluster signature works area unit tired [17.]

III. PROPOSED GROUP DIGITAL SIGNATURE SCHEME

The sensors around the body gather the biological information and transmit it to the BAN controller nodes, such as PDA and smartphones, and the controller node serves as the gateway for anonymously accessing the services provided by external networks. In general, we assume that the authentication protocols are deployed in distributed WBAN application environments equipped with public key cryptographic primitives. This allows the existence of some authority mechanism, such as the authority registrar (AR) that can generate and certify cryptographic keys for different purposes. The registered Node can be authenticated by various APs.

The sensors around the body gather the biological information and transmit it to the BAN controller nodes, such like PDA and smartphone, and the controller node serves like the gateway for secretly access the services provided by exterior networks.In general, we suppose that the verification protocols be deployed in distributed WBAN application environments equipped with public key cryptographic primitives. This allows the survival of some authority mechanism, such as the authority registrar (AR) that can generate and certify cryptographic keys for different purposes. The registered join can be authentic by various APs.

The Node sends his or else her signature on the signature issued by AR and the account index to the AP to log in illustrated in Figure 1. The AP then verifies the client's signature by the account index and the AR's signature by AR's public key. Since the signature is generated in a way that only the AP preserve verify and complete the protocol, it cannot recover the real identity of the WBAN client from the information that it can obtain. We believe to the AP and the clients are synchronous in time with our protocol.

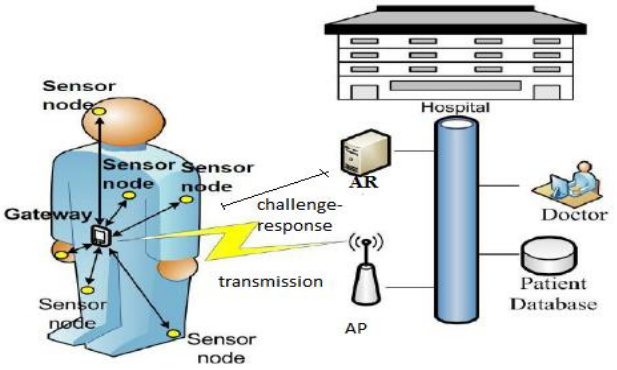


Associate in Authority registrar (AR) and group biosensor Nodes (BNs) is illustrated in Figure 2. The communication among the authority registrar (AR) and group biosensor nodes (BNs) relies on a challenge-response detection scheme. The challenge-response detection theme supports information privacy on transmission and unsigned signature created by the particular node. The AR related to the challenge-response detection scheme ensures that only nodes will build the signature, information legitimacy, along with non-repudiation used for several signers within the cluster.

Figure 2. The structure of the proposed group digital signature technique

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018



The digital signature algorithm [10] supported finding quadratic harmony, resolving and distinct log issues is employed to properly determine the signer within the group. The group biosensor nodes (BNs) initial apply this digital signature formula to produce their public-private key pairs respectively and register their identities within the AR. Consistent with listed group node's identities, the AR then generate a group set of a secret key in the database for further transmission. Five processes are enclosed. They are:

(1) Public-private key making through group biosensor nodes
(2) Group gID mark and element identity code making on behalf of group nodes
(3) The challenge-response detection
(4) Signing Process
(5) Verification Process

A. Public-private key making through group biosensor nodes (BNs)

Step1: Let p, q, r, with s are four prime facts with the aim of satisfying n1=2*p*q + 1 along with n2=2*r*s + 1, wherever n1 along with n2 also are prime numbers. Let N = n1*n2, as a result, Φ (N) = (n1–1) (n2 - 1) = 4*p*q*r*s, wherever Φ (N) is the Euler phi-function that's the number of positive integers not exceeding N, that is comparatively prime to N. condition N is prime, Φ (N) is capable N-1.

Step2: Choose an odd variety t that satisfies following equations:

$$X_1 \equiv t^2 mod\big(\Phi(N)\big)$$
$$X_1 * d \equiv 1 mod\big(\Phi(N)\big)$$
$$X_2 \equiv t^{(t+1)^2} mod\ N \equiv t^{x,+2r+1}\ mod\ N$$

Step3: Publish the wide-ranging public keys (X1, X2, and N) to the AR.

Step4: Keep the personal keys (t and d) firmly.

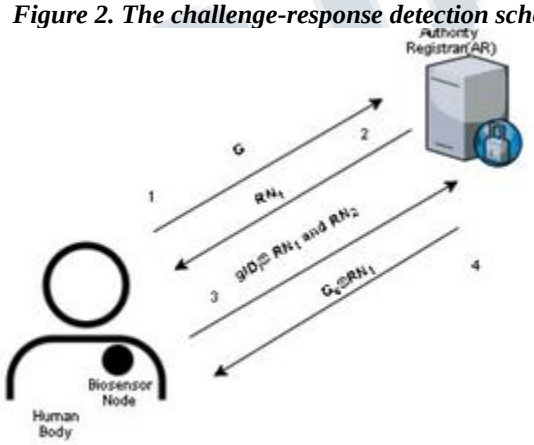
B. Group gID mark and element identification code generation on behalf of group nodes

Let G and gIDi be present the group individuality mark, ith identity code of a grouping member, where i = 1, 2, … , n. These two parameters are set by the AR securely.

C. The challenge-response detection Process

The challenge-response detection process is given away in Figure 2, where RN1 and RN2 are arbitrary numbers as challenges.

Figure 2. The challenge-response detection scheme



Let Gs be present the group secret key to generates through AR associated with the challenge-response protocol. In this process, the overlapping-shifting among EXOR logical function symbolize because E is used to guarantee information transmit securely. The mathematical appearance is described as follows.

Assume $A = [a_m, a_{m-1}, a_{m-2}, \dots, a_2, a_1]$

$B = [b_n, b_{n-1}, b_{n-2}, \dots, b_2, b_1]$

Then, $E = A©B = [e_m, e_{m-1}, e_{m-2}, \dots, e_2, e_1]$

Where,

$$E_k \equiv \begin{cases} a_k \oplus b_{n-(m-k)} \oplus b_{n-(m-k+1)} \oplus \dots . \oplus b_k, when\ n \geq \\ a_k \oplus b_n \oplus b_{n-1} \oplus \dots . \oplus b_{n-(m-k)}, when\ n < m, and\ k > n \\ a_k \oplus b_1 \oplus b_2 \oplus \dots . \oplus b_k, w\square ere\ n < m, and\ k \leq m - \end{cases}$$

In classify to take the Gs, four steps be included.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Step 1: The biosensor node send the group identity mark G toward the AR

Step 2: The AR sends the random number RN1 to the user if the received G is identified correctly.

Step 3: The biosensor sends gIDi©RN1 and the random number RN2 to the AR. The AR would take the received gIDi©RN1 through the decrypting process. If the RN1 be able to be presently decrypted by gIDi, the node is then identified.

Step 4: After the node is identified, the AR would response an acknowledgment and send Gs©RN2 to the biosensor. The user would take the received Gs©RN2 through the decrypting method to discover the group secret key Gs for further signing process.

Signing Process

If Node B wants to sign a message m to A, four steps are integrated inside the signing process.

Step1: B gets the grouping secret key in Gs from the AR by the challenge-response protocol.

Step2: B uses his private keys (t and d) to sign the message such as

$$S(m) = (m^{d} * t^{d+2t^{-1}+1} \bmod N)$$

Step 3: B computes two parameters: XS and P, by following equations:

XS = Gs e gIDic S (m), P=G e XS

Step 4: B sends the (P, XS, S(m), m) to the A.

Verification Process

Two steps are integrated into the verification process.

Step 1: After A receives the signature information (P, XS, S(m), m) from B, A uses P and XS to verify the received data by calculating Pc XS. If the consequence is equal because the group identity mark G, after that the received message be ensured with signed through the group.

Step 2: In the casing of disagreement, the AR will check the equation XSe S(m) = Gsc gIDi. If it is accurate, the AR after that check the public key authentication table to discover the ith public key toward decrypt S(m). Such as

$$m' = V(S) \equiv S(m)^{X_1} * X_2^{-1} \bmod N$$

If m = m', the signer is identified.

Proof:

$$\begin{aligned} V(S) = m' &\equiv X_2^{-1} * S^{X_1} (mod\ N) \\ &\equiv X_1^{-1} * \left(m^{d} * t^{d+2t^{-1}+1}\right)^{X_1} mod\ N \\ &\equiv X_2^{-1} * m^{d-X_1} * t^{t^2+2t+1} \bmod N \\ &\equiv m * X_2 * X_2^{-1} mod\ N \\ &\equiv m\ mod\ N \end{aligned}$$

F. Security Analysis:

The authentication protection ability would be provided via the challenge-response detection scheme as well as the digital signature algorithm. They are analyzed as follows.

(1) The challenge-response detection scheme

by random numbers since challenges with E function because the cipher ensures dynamic messages transmit going on WBAN every process. These challenges are able to avoid the node from denying their communication and any entry from forgery or making false claims. Therefore, the non-repudiation is provided inside WBAN.

(2) The digital signature algorithm

The difficulties of the planned digital signature algorithm are base resting on solve three mathematical problems: discrete logarithm, factorization, and quadratic correspondence. hence, the sufficient complexity of the planned technique is provided.

IV. IMPLEMENTATION METHODS

The implementing proposed group signature system consists of four measures: setup, sign, verify and open. They are described in the following and an example is shown.

Setup

An interactive detection procedure among the AR and the group biosensor's builds. a few parameters such as the group individuality mark, the Node ID, and the Node's public-private keys are as well position.

Sign

A signature generates algorithm applies to produce a signature used for a communication.

Verify

An algorithm is conventional toward verifying the validity of a group signature through deference to a few interrelated parameters.

Open

An algorithm allows the AR or else the group administrator to decide the identity of the group node's

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

who issue the signature, as well as provide a verification of this information.

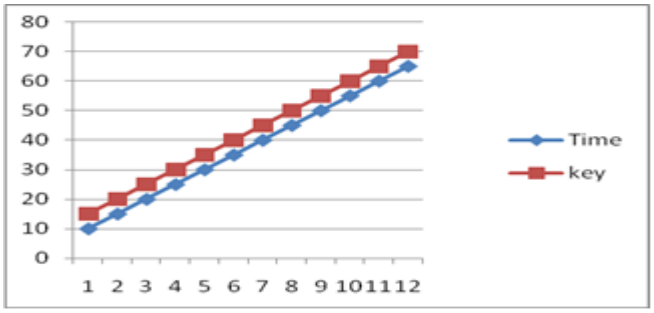


Fig-3

The planned method provides two improvements is illustrated into Figure 3: faster processing time and the key size of the group member determination do not enlarge among the number of signatures.

Faster processing time:

Because the parameters of G, gIDi, and GS are independent of the group members' signatures, signing, verification, change of integrity new member otherwise delete previous members could be performed with adding or erasing the connected public parameters while not dynamic any keys of alternate members. Therefore, the statistics of calculation are attenuate. Furthermore, the planned methodology uses only one public-private key combine rather than two pairs of existing works. This reduces the occasion for generating keys and computing the connection parameters.

The sizes of keys of the group element could not enlarge among the number of signatures:

Because key generation is independent of different group members, therefore, the key size of the group element won't enlarge the number of signatures. what is more, the utilization of the challenge-response detection protocol and E perform rather than uses of mathematical calculation to extend the quality of the scheme, the key sizes don't appear to be completely required moreover time-consuming toward extending system protection inside WBAN.

An example:

Setup

The interactive challenge-response detection protocol is located as given away in Figure 2. presumptuous the group uniqueness mark G is 372, the user's gID is 965, user's public keys (X1, X2, N) equals (3259, 3096, 4757) and its private keys (d, t) equals (2689, 113).

Sign

Let the group undisclosed key GS be 1453 set by the AR. The user can obtain the GS by the challenge-response detection protocol. If the message m = 813, then the signer's signature can be generated by

$S(m) = (m^d * t^{d+2t^{-1}+1} \bmod N) = 813^{2689} * 113^{564} \bmod 4757 = 464$

XS = SG e ID e S(m) = 1453 c 965 c 464 = 1234,

P = G e XS = 372 c 1234 = 251

Therefore, the related parameters are generated such as:

(P, XS, S(m), m) = (251, 1234, 464, 813)

Verify

By checking Pc XS = G, the legality of a group signature is identified

Open

By checking Is XSc S(m) equal to SGc IDi? If the answer is yes, the AI after that check the public key confirmation table to discover the ith public key toward decrypt S(m). Such as

$m' = V(S) \equiv S(m)^{X_1} * X_2^{-1} \bmod N$

If m=m', the signer is identified.

V. CONCLUSION

A novel group digital signature method by way of a challenge-response detection protocol and a digital signature scheme is planned in the direction of wireless body area network and allow only group nodes to make signatures, remain actual node that made signatures anonymous, along with grant data accuracy and non-repudiation designed for whichever signer in the group. The proposed method provides two improvements: Because the parameters of G, gIDi, and GS are independent of the group Nodes' signatures, signing, verification, change of integrity new node's or deleting previous nodes could be performed by adding or erasing the connected public parameters while not dynamic any keys of alternative node's. Therefore, the statistics of computation are attenuate. Furthermore, the planned methodology uses only one public-private key combine rather than two pairs of existing works. This reduces the moment in time for generating keys and computing the connection parameters. Because key generation is independent of different group node's, therefore, the key size of the grouping node won't enhance with the number of signatures, the key sizes don't appear toward be

completely required as well lengthy to extend system protection in WBAN.

REFERENCE

[1]. He, Debiao, Sherali Zeadally, Neeraj Kumar, and Jong-Hyouk Lee. "Anonymous authentication for wireless body area networks with provable security." IEEE Systems Journal 11, no. 4 (2017): 2590-2601.
[2]. Latré, Benoît, Bart Braem, Ingrid Moerman, Chris Blondia, and Piet Demeester. "A survey on wireless body area networks." Wireless Networks 17, no. 1 (2011): 1-18.
[3]. Ullah, Sana, Henry Higgins, Bart Braem, Benoit Latre, Chris Blondia, Ingrid Moerman, Shahnaz Saleem, Ziaur Rahman, and Kyung Sup Kwak. "A comprehensive survey of wireless body area networks." Journal of medical systems 36, no. 3 (2012): 1065-1094.
[4]. Chen, Min, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, and Victor CM Leung. "Body area networks: A survey." Mobile networks and applications 16, no. 2 (2011): 171-193.
[5]. Yuce, Mehmet R. "Implementation of wireless body area networks for healthcare systems." Sensors and Actuators A: Physical 162, no. 1 (2010): 116-129.
[6]. Kumar, Ramesh, and Rajeswari Mukesh. "State of the art: Security in wireless body area networks." International Journal of Computer Science & Engineering Technology (IJCSET) Vol4, no. 5 (2013): 622-630.
[7]. Liu, Bin, Zhisheng Yan, and Chang Wen Chen. "Medium access control for wireless body area networks with QoS provisioning and energy efficient design." IEEE transactions on mobile computing 16, no. 2 (2017): 422-434.
[8]. Al-Mahmud, Abdullah, and Matei Ciobanu Morogan. "Identity-based authentication and access control in wireless sensor networks." International Journal of Computer Applications 41, no. 13 (2012).
[9]. Mishra, Dheerendra, Ashok Kumar Das, and Sourav Mukhopadhyay. "A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using the smart card." Peer-to-peer networking and applications 9, no. 1 (2016): 171-192.
[10]. J. Liu, Z. Zhang, X. Chen, and K. S. Kwak, "Certificateless remote anonymous authentication schemes for wireless body area networks,"IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 332–342, Feb. 2014.
[11]. D. Chaum and E. van Heyst, "Group signatures," In Andances in Cryptology – EUROCRYPT'91, vol. 547, pp. 257-265, 1991.
[12]. L. Chen and T. P. Pedersen, "New group signature schemes," In Advances in Cryptology – EUROCRYPT'94, vol. 950, pp.171-181, 1995.
[13]. J. Camenisch, "Efficient and generalized group signatures," In Advances in Cryptology – EUROCRYPT'97, vol. 1233, pp.465-479, 1997.
[14]. W. B. Lee and C. C. Chang, "Efficient group signature based on discrete logarithm," IEE Proc. Comput. Digit. Tech., vol. 145(1), pp. 15-18, 1998.
[15]. J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," In Advances in Cryptology –CRYPTO'97, vol. 1296, pp. 410-424, 1997.
[16]. L. Chen and T. Pedersen, "On the efficiency of group signatures providing information theoretic anonymity," In Advances in Cryptology- Eurocrypt'95, vol. 921, pp.39-49, 1995.
[17]. Y. M. Tseng and J.K. Jan, "Improved group signature scheme based on discrete logarithm problem," IEE Proc. Electronic Letters, pp. 1324-1325, 1999.