Research Journal of Applied Sciences, Engineering and Technology 13(1): 48-56, 2016
DOI:10.19026/rjaset.13.2889
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: December 13, 2015 Accepted: March 1, 2016 Published: July 05, 2016

Research Article

Security Analysis in Body Area Networks using Attribute-based Ring Signcryption Scheme

A. Arul Jothi and Dr. B. Srinivasan
Department of Computer Science, Gobi Arts and Science College, Gobichettipalayam, Tamil Nadu-638453, India

Abstract: At present, Body Area Networks (BANs) are budding as one of the major research interests, predominantly in the field of personal health monitoring. In view of the fact that health data are extremely private and includes sensitive details, the security of data transmission inside a BAN turns out to be a critical issue that needs instant attention. In this study, Attribute-based Ring Signcryption Scheme (ARSS) is proposed for body area network security. The initial process of proposed system is preprocessed the patient's dataset using Independent Component Analysis (ICA). Then interoperability is defined by semantics and the semantic interoperability among body area sensor networks is used Ant Colony Optimization based Fuzzy Ontology (ACO-FO). The ACO-FO is used to improve the interoperability of BAN system. Then the proposed ARSS is simultaneously providing the characteristics of message confidentiality, authentication, integrity, remembrance, non-repudiation, verifiability in public and forward secrecy of message confidentiality. ARSS can make use of any speedy and safe symmetric algorithm for the encryption of messages, it offers huge benefits in order to be employed in establishments involving security in the fields of health monitoring and while managing with resource constrained devices. Theoretically it proves that ARSS is efficient and feasible. And also its security level is analyzed and compared to existing Elliptic Curve Cryptography with Fuzzy Ontology (ECC with FO) signcryption and Fuzzy Attribute-Based Signcryption Schemes.

Keywords: Attribute-based ring signcryption scheme, ant colony optimization, body area networks, fuzzy ontology, independent component analysis, interoperability, security

INTRODUCTION

Body Area Networks (BANs) can be used to continuously or remotely monitor patients' health, which have the tremendous capability for revolutionizing the acquisition, processing and the communication of significant data for e-healthcare systems. As we know, the modern e-healthcare systems can provide new ways of hospitalization with quality health care. Wirelessly connected medical sensor nodes placed in, on and around the body form a BAN for continuous, automated and remote monitoring of physiological signs to support medical applications (Patel and Wang, 2010; Lorincz *et al*., 2004). In addition, a Patient Controller (PC) is needed to perform a multitude of functions in BANs. A PC (such as a PDA or smart phone) can sense and fuse data from sensors across the body, serve as a user interface and bridge BANs to higher-level infrastructures. The primary applications of BANs are seen in the domain of healthcare, especially for continuous monitoring and logging vital parameters of patients suffering from chronic diseases such as diabetes, asthma and heart attacks. Moreover, BAN technology is able to support other personalized applications, such as sports, gaming, entertainment, military and so on (Hanson *et al*., 2009; Li *et al*., 2010; Jovanov *et al*., 2005). A wide range of applications make BANs have a promising future.

A continuous development of wireless sensor network application is observed in BANs. Every BAN instrument is connected to the body of a human and observes the condition of that corresponding body. In the field of health care, application of BAN gives constant monitoring regarding the patient's critical signs, permitting for quicker medical help with no difficulty of being made to physically reside in the hospital stringed with wired monitoring devices and in-person supervision. In addition, BAN can make possible a better experience with respect to exercise by means of providing feedback and measurements regarding the body's response to physical activities. In comparison with traditional sensor networks, the most important difference of BANs is that a BAN needs to deal with more important medical information. Data

Corresponding Author: A. Arul Jothi, Department of Computer Science, Gobi Arts and Science College, Gobichettipalayam, Tamil Nadu-638453, India

confidentiality and integrity are the most important requirements in BANs, since wireless medium is susceptible to lots of security attacks. In this research work, the security provided by a BAN in opposition to an outsider is majorly concentrated. In view of the fact that a BAN comprises of all entities in touch with the body, the aim is securing the communication of these devices opposed to outsider devices which do not make physical contact with the body.

In BANs, sensor association that is secure is a not a small issue, because a healthcare worker must check whether a set of sensors are securely and correctly in association with a patient intended prior to any data communication. Lots of previous works focus only on group key agreement in sensor nodes (Tan *et al*., 2009; Morchon *et al*., 2006; O'Donovan *et al*., 2009; Malasri and Wang, 2007). BANs output the same data bits that are independent of the application domain, though the purpose of this data can be different in different domains. For instance, heartbeat can indicate about health in the care domain or it can be synonymous with performance ability in the sports or entertainment domains. This example exhibits that semantic interoperability needs sharing of data and concepts, along with placing them for the particular application purpose for the sake of for their suitable usage. Ontologies have been accepted in the literature as a way for achieving interoperability at semantic level between systems (Ouksel and Sheth, 1999). Ontology is a conceptualization of real-world phenomena (Guizzardi, 2005), hence there is a necessity to examine which concepts has to be also included in ontology for the achievement of semantic interoperability between the sensor networks and sensor applications and what is needed for directing towards their usage that will be appropriate for them.

In this study, Attribute-based Ring Signcryption Scheme (ARSS) is proposed for body area network security. The initial process of proposed system is preprocessed the patient's dataset using Independent Component Analysis (ICA). Then interoperability is defined by semantics and the semantic interoperability among body area sensor networks is used Ant Colony Optimization based Fuzzy Ontology (ACO-FO). The ACO-FO is used to improve the interoperability of BAN system. If the interpretability of communication failure is occurs means BAN interaction does not progress as the external users. Once the problem has been identified and fixed, communication is then resumed using the updated ontologies. Then the proposed ARSS is simultaneously provides the attributes of message confidentiality, authentication, integrity, unforgetability, non-repudiation, public verifiability and forward secrecy of message confidentiality. As it is on the basis of ARSS, it can employ any speedy and safe symmetric algorithm for the encryption of messages; it offers huge benefits in order to be employed in establishments involving security in the fields of health monitoring and while managing with resource constrained devices.

BACKGROUND STUDY AND SYSTEM MODEL

In this section, the most related research that still exists is summarized. And system model of proposed system is explained. A certificate less remote anonymous (Liu *et al*., 2012) authentication protocol proposed. Even doctors do not have the authority of disclosing the private information regarding the patient. This approach makes use of an account index that is anonymous. Three resources that are employed in this protocol are the network manager, WBAN client and Application Provider (AP). The WBAN client makes the request for service from the application provider, then the network manager takes the responsibility of managing the network and authenticity and the application provider offers the services in the network. This protocol is in accordance with the CL-PKC means Certificate less Public key cryptography. The three steps involved in this protocol are initialization, registration and remote anonymous authentication. The impersonation of the client cannot be done by the network as it is capable of generating only a part of the key.

The physiological value could be heart rate, pulse rate, electrocardiography etc. A (Sampangi *et al*., 2012) security suite has been introduced for BAN that uses IAM (Independent and Adaptive Key Management) and KEMESIS (Key Management Scheme for security in Inter Sensor communication), mechanisms for security. In these kind of schemes, the usage of keys that are randomly generated is applied for the purpose of encryption and decryption at the sender and receiver side in an independent manner and no key distribution or exchange of keys among sensors is required. There are multiple means for the distribution of the key. The keys distribution to the sensors could be prior to deployment. But this approach is not very flexible. The keys can also be distributed with the support of bio channels such as Inter Pulse Interval (IPI) etc. A security suite has been presented for BAN that employs a new key agreement scheme which permits the nodes in the neighborhood in BAN to be able to share a common key that is generated by ECG signal (Zhang *et al*., 2012). The IJS (Improved Jules Sudan) is introduced for the authentication of message. The ECG-IJS key agreement can perform the secure data communication over BAN in the absence of any kind of key distribution overhead. The newly introduced key generated form is actually a universally measurable physiological stimulus (ECG) which is unique and distinct for every person.

A secure and effective Ordered Physiological Feature based Key Agreement (OPFKA) for use in BAN is introduced in Hu *et al*. (2013a). Two sensors accept over a symmetric cryptographic key generated from the physiological signal characteristics that are overlapping. This approach requires no pre distribution of keys. The secret characteristics that are computed from the identical physiological signal observed at various parts of the body by means of sensors with some overlapping though not the same entirely. The OPFKA is evolved for transferring the secret features of one sensor to another so that two sensors can be able to recognize the ones that are overlapping. It is a secure, resourceful and practical protocol. The features by each sensor generated are ordered in order to create a feature vector. The sender transmits the secret features in addition with the data with noise to the receiver. The receiver then generates a key in accordance with the features that are common. The sender recognizes the common characteristics present in its own feature vector and accordingly does the key computation. The aim of OPFKA is enabling a secure inter-sensor communication within a BAN. A security system based on biometric (Ramli *et al*., 2013) is introduced for the purpose of data authentication in the BAN. The ECG feature of the sender is chosen as the biometric key for authentication of data in BAN. Hence there is no risk of one patient's record getting mixed up with another patient.

In Liu and Kwak (2010) a hybrid security protocol for BAN is presented for supporting to secure a communication wireless channel. This protocol has a better tradeoff among security and resource restraints. A hybrid kind of key management methodology (Alsadhan and Khan, 2013) is introduced which is actually a combination of the physiological values along with the preloaded keys. The Local Binary Pattern (LBP) is employed by ECG based agreement for generating common keys which are to be agreed upon for the purpose of encryption and decryption with the goal of making the inter sensor communication far more secure. The two important concepts of this approach constitute feature generation and key agreement. Master key is basically preloaded in the medical server of the BAN present remotely for authenticating personal server. In case, an adversary happens to compromise a personal server, medical server cancels the existing key belonging to the personal server. Then the recovery of the Personal server is performed by making use of the master secret key.

System model and preliminaries network model: A health-care system network model is considered. There are two most important present in this system: The BAN of a patient and also the external user(s). In specific, the BAN comprises one BAN controller with several (implantable or wearable) devices. The devices are typically sensors that observe critical body parameters or their movements and manage the human body by means of yielding life support, visual/audio feedback, etc. These BAN devices keep in touch with the BAN controller either directly or by means of multi-hop communications. The BAN controller not only communicates with the BAN devices however evens the Internet. Furthermore, BAN controllers in that are in the neighborhood possibly will generate an ad hoc network along with Wireless Personal Area Network (WPAN) techniques.

Here, the presence of a trusted third party KS -i.e., a key distribution server is presumed-which is capable of verifying the identity corresponding to a legal external user (e.g., a doctor) and distributes credentials for use to the external user. The identity pertaining to the external user is a collection of features that describe the essential user details. It must be noted that KS is hence not necessary to be connected online while an emergency-room doctor requires communicating with the BAN a patient is present in- i.e., it therefore cannot develop into the form of a single point-of-failure for the system.

Adversary model: Here, both categories of adversaries are taken into account:

- Adversaries that are passive and which do message eavesdropping sent (wirelessly) within the BAN or among the BAN and the external user.
- Active adversaries which control the sent messages. Moreover, the multiple adversary collusion case is also considered. It must be noted that an adversary might be either an external user having no authorized access permission to the BAN, or an "insider" which intends to manipulate/retrieve the medical information that it has no authorization to access.

PROPOSED METHODOLOGY

This section introduces the chief idea behind the proposed access control structure which imposes various access rights for various kinds of users. It improves the security of patient's information for health care in BAN. Subsequently, the four algorithms of ARSS are explained. And the overall performance of proposed system also explained.

System overview: System overview is illustrated in Fig. 1. It shows the overall architecture of proposed system. In this proposed system, Attribute-based Ring Signcryption Scheme is used for body area network security. The initial process of proposed system is

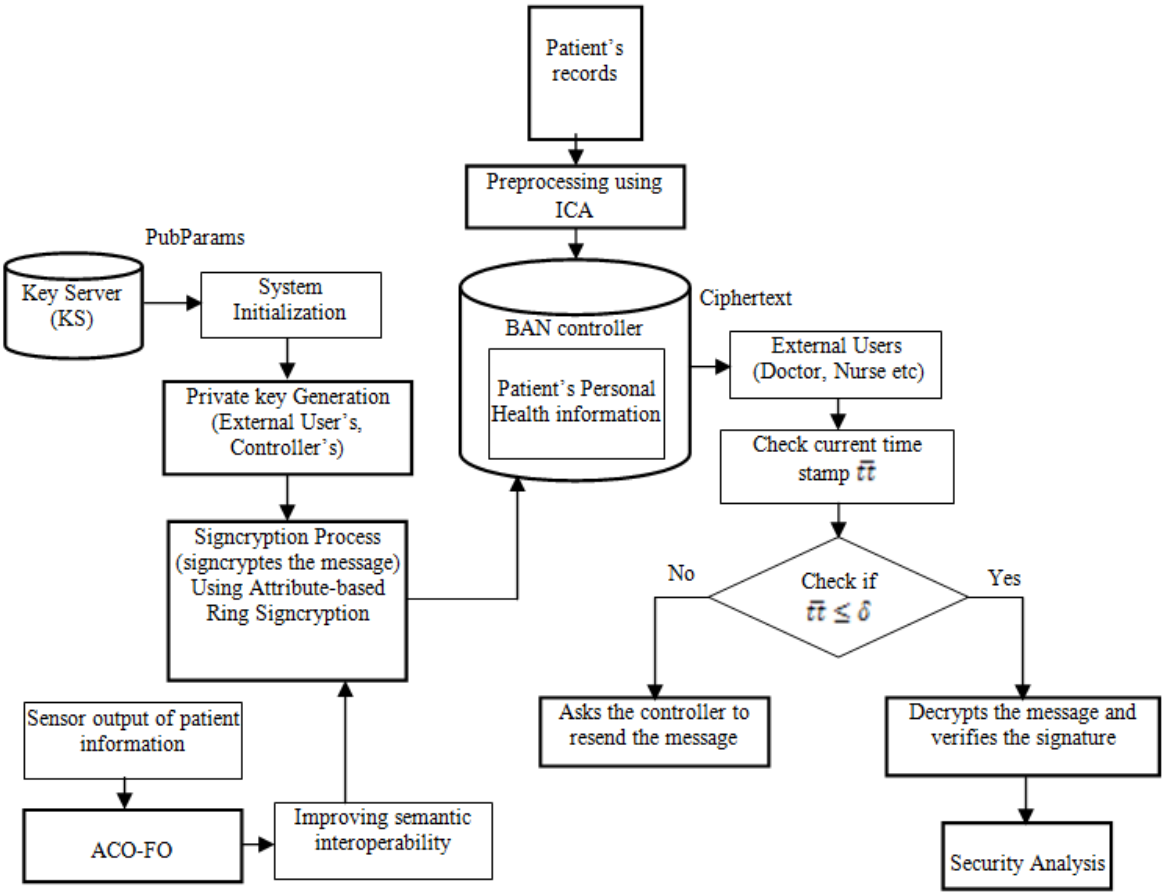

Fig. 1: Overall architecture diagram for proposed system

preprocessed the patient's dataset using Independent Component Analysis. Then interoperability is defined by semantics and the semantic interoperability among body area sensor networks is used Ant Colony Optimization based Fuzzy Ontology (ACO-FO). In order to safe-guard against the exposure of information because of theft or a loss of the BAN controller, the personnel identification must be authenticated when they get connected with the controller. In order to have access control to the controller, the attribute-based signencryption over ARSS will be examined. In case of attribute-based encryption, a ciphertext is tagged with a collection of attributes in addition to a private key is related to an access structure which has the control over the ciphertext that person is capable of decrypting in the same way, access structures are utilized for controlling the access rights of several users of the BAN controller.

Data preprocessing using ICA: Data preprocessing is frequently advantageous for reducing the data dimensionality using ICA. It is a technique to present the patient's data in a more detailed manner by exposing the structure that is hidden in the data and often reduces the dimensionality pertaining to the representation. It can also be considered as a technique of reducing the dimensionality as a highly minimized representation of the data is found.

Dimensionality reduction is not the first and foremost goal of ICA and factually, many of the ICA algorithms are in favor of reasonable dimensionalities of data. The major concept with respect to the ICA presumes that the data are linearly combined through a collection of separate autonomous sources and thereafter demix those signal sources according to their statistical independency measure obtained through mutual information. For the purpose of validating its approach, basically it is assumed that at the most only one source in the mixture model can be permitted to be as a Gaussian source. This is because of the fact that a linearly mixing Gaussian sources is yet a Gaussian source. The main aim of ICA is to reduce the dimensionality of data. In ICA, the high dimensionality data are considered as irrelevant data and it all removed from data set. Provided a collection of n-dimensional data vectors $[x^{(1)}, x^{(2)}, .., x^{(N)}]$, the directions (vectors) in the direction of where the projections statistics of the data vectors are independent of one another comprise the independent elements. It means, when A represents a change from the reference frame given to the independent component reference frame, at that moment:

$$x = Ae \quad (1)$$

In order that $p(e) = \pi_{pa}(et)$. Where $pa(.)$ represents the marginal distribution and $p(e)$ stands for the joint distribution on the n-dimensional vector e. Generally, the scheme for carrying out Independent Component Analysis (ICA) is observed as the scheme for the purpose of deriving one particular W:

$$y = Wx \quad (2)$$

In order that every component of y (i.e., each yi) goes on to become independent of one another. When the individual marginal distributions are seen to be non-Gaussian, subsequently the marginal densities that are derived result in a scaled permutation of the actual density functions when one W such as this can be got. One general learning scheme (Ouksel and Sheth, 1999) for finding one W (as derived from the normal gradient descent of Kullback-Leibler divergence among joint density and the product of marginal densities) is:

$$\Delta W = \eta(I - \phi(y)y^T)W \quad (3)$$

Where $f(y)$ represents a nonlinear function with respect to the output vector y (like a cubic polynomial or a polynomial having odd degree, or a summation of polynomials with odd degrees, or a sigmoidal function). The preprocessed data is stored and maintained in BAN controller database. Based on this data information, the encryption and signcryption methods key information is discussed.

Access control structure: The proposed system's main concept is about designing a security scheme based on attribute that sees the identities (of external users) in the form of groups of attributes and imposes a lower limit on the amount of attributes common among a user's distinctiveness and the access rights specifications of the sensitive data. Consider an identity includes n attributes and every attribute could be regarded as a string having length that can be arbitrary. Instances of identities of patients include Ipd_1 = {doctor, Identity, department, title}, Ipd_2 = {Name, title, Dept.}, etc. This further allows to indicate access privileges of users in accordance with attributes. The access structure of a user in the form:' d out of n attributes', that permits the user to get hold of the information from the BAN controller. Especially, a collection of attributes for every user from the access control structure is defined since a BAN that is personal generally does not possess a large number of users.

ACO-FO based approach for improving semantic interoperability: The proposed system adopted the ACO based fuzzy rule ontology- approach to support the semantic interoperability of the platform. The Fuzzy Rule Learning (FRL) is big problem in Fuzzy ontology. To solve this problem using ACO and it's improved the fuzzy rules.

Ant colony optimization algorithms for learning fuzzy rules: To apply ACO algorithms to a FRL problem, the following steps have to be carried out:

Step 1: A FRL problem is Obtained ant it is represented as a graph or a comparable structure simply covered by ants. In order to build the graph, the following steps are taken:

- Conclude the rules: A rule $R_i - i = 1, \ldots N_r$ −defined by means of an antecedent combination, $R_i = IF\ X_1$ is A_{i1} and X_n is A_{in} will be included in the graph if and only if: $\exists e_l = (x_1^l, \ldots, x_n^l, y^l) \in E$ in order that $\mu A_{il}(x_1^l) \ldots \mu A_{in}(x_n^l) \neq 0$. Specifically, there is at the least one example positioned in the fuzzy input subspace characterized by the antecedents considered in the rule.
- Link the rules to consequents: The rule R_i will be connected to the consequent B_j —$j = 1.., N_c$— (taken from the collection of labels of the output fuzzy partition) if and only if it satisfies the following condition: $e_l = (x_1^l, \ldots, x_n^l, y^l) \in E$ in order that $\mu A_{il}(x_1^l) \ldots \mu A_{in}(x_n^l).\mu B_j(y^l) \neq 0$. Specifically, there is not less than one example placed in the fuzzy input subspace which gets covered by such a result.

Step 2: Determine the way of allocating a heuristic preference to every choice that the ant has to take in each step to produce the solution. Construct the set $E_i^{'}$ composed of the input-output data pairs that are placed in the input subspace defined by $E_i^{'} = \{e_l = (x_1^l, \ldots, x_n^l, y^l) \in E$ such that $\mu A_{il}(x_1^l) \ldots \mu A_{in}(x_n^l).\mu B_j(y^l) \neq 0\}$.

Step 3: Set up a suitable way of initializing the pheromone. Pheromone value of every assignment is obtained as given below:

$$T_0 = \frac{\sum_{i=1}^{N_r} max_{j=1}^{N_c} \eta_{ij}}{N_r} \quad (4)$$

Step 4: Determine a fitness function which has to be optimized. The fitness function sets up the quality of a solution. The measure taken will be the function called Mean Square Error (MSE), which defined as:

$$MSE(RB_k) = \frac{1}{2.|E|} \sum_{e_l \in E} \left(y^l - F_k(X_0^l)\right)^2 \quad (5)$$

Step 5: Choose an ACO algorithm and execute it to the FRL problem.

The collection of nodes attainable from Ri (set of possible neighborhood of node Ri) will be $J_k(i) = \{j \text{ such that } \eta_{ij} \neq 0\}$ in the transition rules taken by both ACO schemes when constructing the solution.

The amount of pheromone that the ant k applies on the couplings which belongs to the solution created by it will equate to $1/\text{MSE}(RB_k)$, with RB_k being the RB produced by ant k.

In case of the local pheromone trail update rule of the ACO scheme, the most common manner of computing$\Delta T_{ij}, \Delta T_{ij} = T_0$, will be used, as a result considering the simple-ACO scheme.

Subsequently, from knowledge base, the system will retry all the ACO based fuzzy rules defined in the context. Fuzzy ontology calculates membership degree (ranging from 0 to 1) for each ontology class and applies a label with its degree. At this step, fuzzy ontology used for matching semantic words from search patients details to fuzzy linguistic variables and terms. Finally, the system is ready to generate OWL descriptors and make them machine-readable data and improving the semantic interoperability.

Attribute-based ring signcryption scheme: In this scheme proposed, the external user's controller is able to perform a message signcrypting on the part of d attributes, where d will get defined in the Setup algorithm. Then the Lagrange interpolation is reviewed as follows. Given d points $q(1), .., q(d)$ on a $d-1$ degree polynomial, q(i) for any $i \in Zp$ can be calculated by means of following the Lagrange interpolation technique. Consider S to be a set in Z_p with d-elements and the Lagrange coefficient $\Delta_{i,S}$ be defined for $i \in Zp$ as below:

$$\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-i}{i-j} \quad (6)$$

Setup (k): Assume a security parameter k, the trusted private key generator (PKG) primarily defines the group of universal attributes U in Z_p, where $|U| = l$. Further after, a $d-1$ default attributes set from Z_p can be expressed as $\Omega = \{\Omega_1, \dots, \Omega_{d-1}\}$. Moreover, PKG chooses a pairing $e: G1 \times G1 \rightarrow G2$ in which the order of G_1 and G_2 is prime $p > 2^k$ and also a generator g of G_1. PKG then chooses $t_1, .., t_l, t_{l+1}, \dots, t_{l+d-1} \in z_p$ at random and calculates $T_i = g^{t_i}$ where $1 \leq i \leq l + d - 1$. PKG also selects $\alpha \in Z_p$ randomly and computes $Y = e(g,g)^{\alpha}$. Finally, PKG selects three cryptographic hash functions: $H_1: G_2 \rightarrow \{0,1\}^{|M|} \times Z_p^* \times G_1, H_2: \{0,1\}^* \rightarrow Z_p^*$ and $H_3: \{0,1\}^{|M|} \times Z_p^* \rightarrow Z_p^*$, where $|M|$ represents the length of the ciphertexst. The public parameters PK are expressed as follows:

$$PK = (G_1, G_2, e, g, \{T_i\}_{i=1}^{l+d-1}, Y, H_1, H_2, H_3) \quad (7)$$

The master secret key MK is represented as $MK = (\alpha, \{t_i\}_{i=1}^{l+d-1})$.

Key Extract (MK, ω): With the user provided with a set of attributes, $\omega \subseteq u$, the PKG does the private key generation for ω in the following manner:

- A $d-1$ degree polynomial q(x) is selected randomly so that $q(0) = \alpha$.
- a new attribute set $\hat{\omega} = \omega \cup \Omega$ is generated and $D_i = g^{\frac{q(i)}{t_i}}$ is computed for every $i \in \hat{\omega}$.
- Consequent is the private key D_i for each $i \in \hat{\omega}$.

Signcryption (m, ω_S, ω_R): In order to signcrypt a message m to a receiver R, the sender S performs the steps that follow:

- Selects a subset ω'_Shaving d elements from $\hat{\omega}_s$ (in which f attributes $\{i_1, \dots, i_f\}$ are selected from ω_S for message signcryption and $d-f$ attributes are selected from default attributes set Ω).
- The sender S then picks up $r \in Z_p^*$ randomly and set $s = H_3(m,r)$, $U = g^s$ and $X = Y^s = e(g,g)\alpha.s$. S then calculates $E_i = T_i^s$ for every $i \in \omega's$ and for each $j \in \omega_R$.
- Let $\omega_S' = \{1, \dots, d\}$ and selects $k \in \omega'_S$ randomly. Define the elements present in set $\omega_S' \cup \omega_R$ to form the ring. For $l \in \omega'_S \cup \omega_R \; and \; l \neq k$, selects $U_l \in Z_p^*$ randomly and $h_l = H_2(m, U_l, X, \omega_S' \cup \omega_R, l)$ is computed, where $|\omega_S' \cup \omega_R| = n_R + d$. For l = k, selects r_k from Z_p^* at random and then computes:

$$U_k = E_k^{r_k} \Big/ \prod_{l \in \omega_S' \cup \omega_R, l \neq k} U_l . E_l \quad (8)$$

$$= g^{t_k . r_k . s} \Big/ \prod_{l \in \omega_S' \cup \omega_R, l \neq k} U_l . g^{t_1 . h_l . s} \quad (9)$$

$$h_k = H_2(m, U_k, X, \omega_S' \cup \omega_R, k) \quad (10)$$

$$V = E_k^{r_k + h_k} \quad (11)$$

- Compute $y = (m \| r \| V \oplus H_1(X))$
- At last, the ciphertext CT is represented as:
- $CT = \left(y, \omega_S', \omega_R, U, \{U_l\}_{l=1}^{n_R+d}\right), \{E_i\}_{i=1}^{d}, \{E_i\}_{i=1}^{n_R}$

For,

$$CT = \left(y, \omega_S', \omega_R, U, \{U_l\}_{l=1}^{n_R+d}\right), \{E_i\}_{i=1}^{d}, \{E_i\}_{i=1}^{n_R} \quad (12)$$

Choose a subset ω'_R with subset having d-elements from attribute set ω_R.

- Computes:

$$X' = \prod_{j\in\omega_R'} e\left(D_j, E_j\right)^{\Delta_{j,S}(0)} \quad (13)$$

$$\prod_{j\in\omega_R'} e\left(g^{\frac{q(j)}{t_j}}, g^{t_j \cdot s}\right)^{\Delta_{j,S}(0)} \quad (14)$$

And retrieves m', r', V' as $\left(m'\|r'\|V'\right) = y \oplus H_1(X')$:

- Computes $s' = H_3(m', r')$ and verifies if $U = g^{s'}$ is satisfied or not.
- For $l \in \{1, \ldots, n_R + d\}$, $h_l' = H_2(m, U_l, X, \omega_S' \cup \omega_R, l)$ is computed and hence verified if $e(g, \prod_{l=1}^{n_R+d} U_l . g^{t_l . h_l' . s'}) = e(g, V')$ satisfies or not. If yes, then R acknowledges CT in the form of the valid ring signcryption on the message m'; R rejects otherwise.

EXPERIMENTAL RESULT AND DISCUSSION

The experimental simulations are carried out in MATLAB 2012. In this section, the performance of proposed Ring Signcryption Scheme (ARSS) is evaluated and the results are compares with the existing Attribute-based Eliptic Curve Cryptography Signcryption (ECCS) and Fuzzy Attribute-Based Signcryption (FABS) (Sahai and Waters, 2005) Attribute-Based Encryption (ABE) (Hu *et al*., 2013b).

Performance analysis: In this subsection, a quantitative performance study is presented.

Message size: In the scheme proposed, the computation of the total message size corresponding to a ciphertext can be done as below. The ciphertext is the joining of attributes, message and time.

Figure 2 illustrates the relationship that exists between the total message size and the number of users at various security levels. It specifies that the message size is not dependent on the number of users.

Figure 3 demonstrates the functional relationship present between the message size and the security level. From Fig. 3, it can be observed that there is a linear relationship of the message size with the security level.

Communication overhead: Figure 4 exhibits the relationship observed between the communication overhead and the security level. The communication

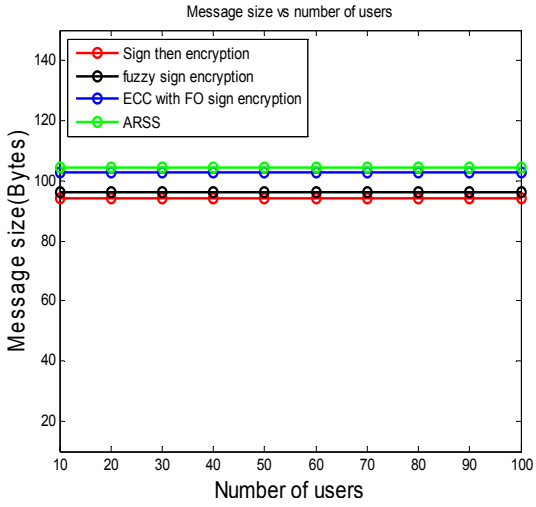

Fig. 2: Message size vs. number of users

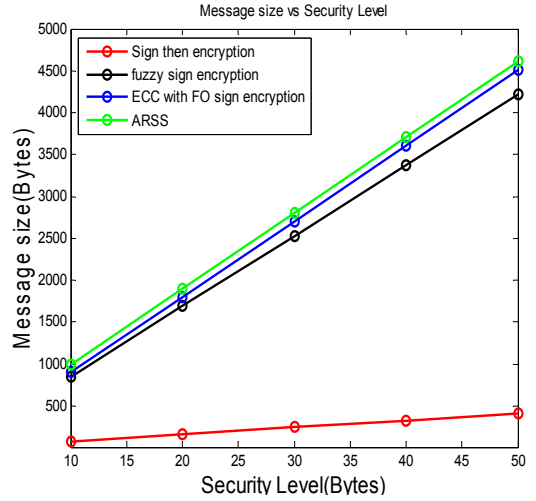

Fig. 3: Message size vs. security level

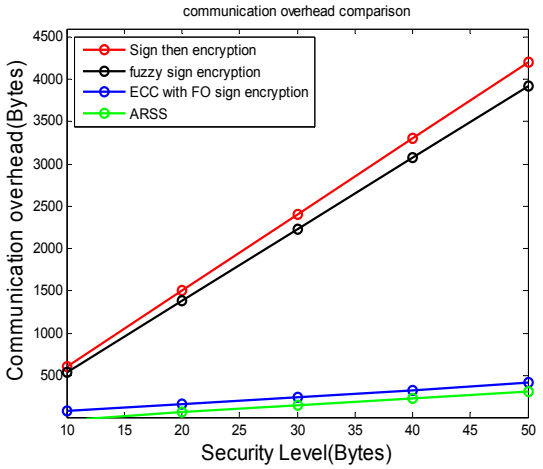

Fig. 4: The communication overhead vs. security level

Unsigncryption CT: Once the ciphertext CT is received, R does the ciphertext decryption as below:

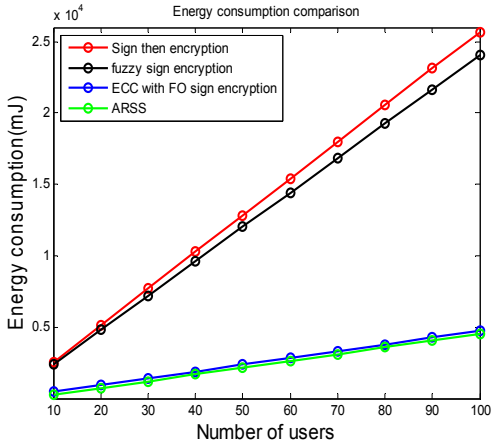

Fig. 5: Energy consumption on communications with respect to the number of users

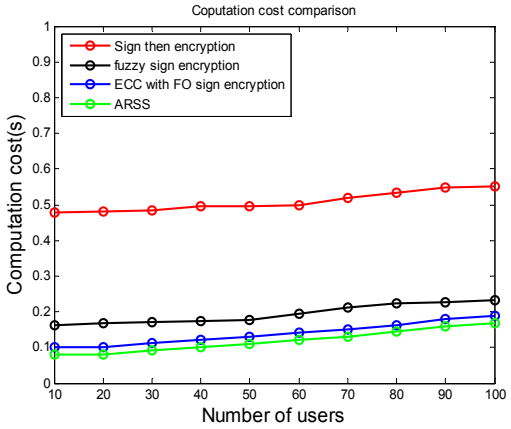

Fig. 6: Computation cost vs. number of zusers

overhead is proportional to security level. ARSS is less communication overhead and it improves the security when compare to existing ECCS, FABS and ABE schemes. The communication overhead has a significant association with the message size of signcryption. The overhead given in terms of q is $5|q|+4$ for the case of signcryption and 1 for designcryption.

Impact of energy consumption on communications: Figure 5 exhibits the relationship existing between the Energy consumption over the communication and the number of users. ARSS has a less power computation than ECCS, FABS and ABE schemes. The reduction technique reduced the energy consumption in ARSS.

Computational cost: Figure 6 illustrates the computation cost of ARSS and also the other schemes. ARSS is achieved less computation cost compare than existing ECCS, FABS and ABE schemes. The energy consumption of ARSS is less and it reduces the communication cost.

Security analysis: The security analysis is studied with regard to the security features which the protocol proposed has to satisfy. If sender sends similar messages exceptionally with the random number r that are same to multiple receivers, the Signcrypted message will be different for each Signcryption, since for each message the identifiers value will be different. The main advantage of ARSS over ECC with FO and Fuzzy signcryption is that the best algorithm known for solving the fundamental hard mathematical problem s.

This proves that considerably smaller parameters can be used in ARSS than in other systems such as ECC with FO and Fuzzy signcryption, but with comparable levels of security.

Efficiency: The computational costs and also the communication overheads of this signcryption approach is extremely smaller in comparison to those of the well-known signature-then-encryption approaches with the same kind of functionalities provided.

Security: Proposed signcryption approach concurrently fulfills the security attributes contained in an encryption scheme and digital signature. And many additional properties: Confidentiality, Unforgeability, Integrity and Non-repudiation, Public verifiability and Forward secrecy of message confidentiality

Confidentiality: The proposed algorithm is based on ARSS which most difficult to crack in the presently available techniques. Confidentiality is provided using receivers public key so without the receivers private key, message can't be disclosed to anyone.

Unforgeability: This is not possible for an attacker who is adaptive for masquerading a truthful sender in generating an authenticated signcrypted text which can be recognized by means of the unsigncryption scheme. Because of the reason that any attacker doesn't know what all parameters are involved in signcrypting a text.

Public verifiability: Any kind of third party or judge can do the verification that the text which is signcrypted is valid or not, without any requirement for the sender's private key or recipient because signature is calculated over encrypted message, so no need of decrypting the actual message for verification.

CONCLUSION

The secure communication within the BAN is required to keep the patient's privacy and security. In this study, Attribute-based Ring Signcryption Scheme (ARSS) is presented. The patient's dataset is preprocessed using Independent Component Analysis (ICA). Then interoperability is defined by semantics and the semantic interoperability among body area sensor networks is used Ant Colony Optimization based Fuzzy Ontology (ACO-FO). Then the proposed ARSS is simultaneously provides the attributes of message confidentiality, authentication, integrity, unforgeability,

non-repudiation, public verifiability and forward secrecy of message confidentiality. Proposed studies show that the ARSS scheme is a light weight and energy efficient scheme compare than existing ECCS, FABS and ABE schemes. And the detailed discussion on privacy and security in health care applications also provided. On a futuristic perspective, there is a necessity of a signcryption scheme that is more effective and much more secure compared to the already available signcryption schemes for Body Area Network.

REFERENCES

Alsadhan, A. and N. Khan, 2013. An LBP based key management for secure Wireless Body Area Network (WBAN). Proceeding of the 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing. Honolulu, HI, pp: 85-88.

Guizzardi, G., 2005. Ontological foundations for structural conceptual models. Ph.D. Thesis, University of Twente.

Hanson, M.A., H.C. Powell Jr., A.T. Barth, K. Ringgenberg, B.H. Calhoun, J.H. Aylor and J. Lach, 2009. Body area sensor networks: Challenges and opportunities. Computer, 42(1): 58-65.

Hu, C., X. Cheng, F. Zhang, D. Wu, X. Liao and D. Chen, 2013a. OPFKA: Secure and efficient ordered-physiological-feature-based key agreement for wireless body area networks. Proceeding of the IEEE INFOCOM. Turin, pp: 2274-2282.

Hu, C., N. Zhang, H. Li, X. Cheng and X. Liao, 2013b. Body area network security: A fuzzy attribute-based signcryption scheme. IEEE J. Sel. Area. Comm., 31(9): 37-46.

Jovanov, E., A. Milenkovic, C. Otto and P.C. de Groen, 2005. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. J. NeuroEng. Rehabil., 2(1): 6.

Li, M., W. Lou and K. Ren, 2010. Data security and privacy in wireless body area networks. IEEE Wirel. Commun., 17(1): 51-58.

Liu, J. and K.S. Kwak, 2010. Hybrid security mechanisms for wireless body area networks. Proceeding of the 2nd International Conference on Ubiquitous and Future Networks (ICUFN, 2010). Jeju Island, Korea (South), pp: 98-103.

Liu, J., Z. Zhang, R. Sun and K.S. Kwak, 2012. An efficient certificateless remote anonymous authentication scheme for wireless body area networks. Proceeding of the IEEE International Conference on Communications (ICC, 2012). Ottawa, ON, pp: 3404-3408.

Lorincz, K., D.J. Malan, T.R.F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh and S. Moulton, 2004. Sensor networks for emergency response: Challenges and opportunities. IEEE Pervas. Comput., 3(4):16-23.

Malasri, K. and L. Wang, 2007. Addressing security in medical sensor networks. Proceeding of the 1st ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments (HealthNet'07), pp: 7-12.

Morchon, O.G., H. Baldus and D.S. Sanchez, 2006. Resource-efficient security for medical body sensor networks. Proceeding of the International Workshop on Wearable and Implantable Body Sensor Networks (BSN'06). Cambridge, MA, pp: 80-83.

O'Donovan, T., J. O'Donoghue, C. Sreenan, D. Sammon, P. O'Reilly and K.A. O'Connor, 2009. A context aware wireless Body Area Network (BAN). Proceeding of the 3rd International Conference on Pervasive Computing Technologies for Healthcare. London, pp: 1-8.

Ouksel, A.M. and A. Sheth, 1999. Semantic interoperability in global information systems. ACM SIGMOD Rec., 28(1): 5-12.

Patel, M. and J. Wang, 2010. Applications, challenges and prospective in emerging body area networking technologies. IEEE Wirel. Commun., 17(1): 80-88.

Ramli, S.N., R. Ahmad, M.F. Abdollah and E. Dutkiewicz, 2013. A biometric-based security for data authentication in Wireless Body Area Network (WBAN). Proceeding of the 15th International Conference on Advanced Communication Technology (ICACT, 2013), PyeongChang, pp: 998-1001.

Sahai, A. and B. Waters, 2005. Fuzzy Identity-Based Encryption. In: Cramer, R. (Ed.), Advances in Cryptology – EUROCRYPT 2005. Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, 3494: 457-473.

Sampangi, R.V., S. Dey, S.R. Urs and S. Sampalli, 2012. A security suite for wireless body area networks. Int. J. Netw. Secur. Appl., 4(1): 97-116.

Tan, C.C., H. Wang, S. Zhong and Q. Li, 2009. IBE-Lite: A lightweight identity-based cryptography for body sensor networks. IEEE T. Inf. Technol. B., 13(6): 926-932.

Zhang, Z., H. Wang, A.V. Vasilakos and H. Fang, 2012. ECG-cryptography and authentication in body area networks. IEEE T. Inf. Technol. B., 16(6): 1070-1078.