ISSN No. 0976-5697

Volume 7, No. 3, May-June 2016

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# A HYBRID CIPHERTEXT-POLICY WITH HIERARCHICAL ATTRIBUTE-BASED RING SIGNCRYPTION TO ENHANCE SECURITY AND PRIVACY IN BODY AREA NETWORKS

A. Arul Jothi
Assistant Professor, PG & Research Department of Computer Science,
Gobi Arts & Science College
Gobichettipalayam, Tamil Nadu-638453, India

Dr.B.Srinivasan
Associate Professor, PG & Research Department of Computer Science,
Gobi Arts & Science College
Gobichettipalayam, Tamil Nadu-638453, India

***Abstract:***A Body Area Network (BAN) is a wireless network of health monitoring sensors designed to deliver personalized healthcare. Securing inter sensor communications within BANs is essential for preserving not only the privacy of health data, but also for ensuring safety of healthcare delivery. This paper proposes a cryptosytem for BAN security known as Ciphertext-Policy Hierarchical Attribute-based Ring Signcryption (CP-HARS). Initially, patient's dataset has been pre-processed with the use of Enhanced Independent Component Analysis (EICA). By analysing the generalization, EICA achieves retrieval performance by operating in a reduced Principal Component Analysis (PCA) space.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. In a CP-HARS approach, the attributes are arranged in a matrix format, in which the higher level user attributes can be hand over to the users in lower level. An efficient data sharing can be enabled using the features in the larger BAN hierarchical groups, in which the keys are hand over to the number of users in the body area network organization. By non-interactive assumptions, the approach provides evidence to enhance security. The proposed CP-HARS is compared to existing Attribute-based Ring Signcryption Scheme (ARSS) and Elliptic Curve Cryptography with Fuzzy Ontology (ECC with FO) signcryption.

***Keywords:***Body Area Network (BAN); ciphertext-policy; hierarchical; Attribute-based Ring Signcryption; Enhanced Independent Component Analysis(EICA); Ant Colony Optimization (ACO); Fuzzy Ontology (FO).

## I. INTRODUCTION

Body Area Networks (BANs) [1] materialized to act as a solution to build personal health monitoring system. To sense, sample, process and to communicate with physiological signals such as blood pressure, blood glucose level, blood oxygen saturation, heart rate, body temperature, blood pressure and physical activity such as level of activity, type and body posture along with environmental parameters such as atmospheric pressure, light, temperature, location, humidity multiple miniaturized network nodes has been designed. These miniaturized nodes can be placed in human body or in the users' clothes as small patches. If wireless communication happens, then the system is known as WBAN or wireless area networks.

To monitor the daily activities BAN can be enabled to sense the physical activity, environmental conditions and health status. Data gathered based on the BAN nodes can be recorded, analyzed and merged in the personal server. The network coordinator of BAN plays the role of a personal server and can be executed either on smart phones or some dedicated devices. The data is given to the cloud, forwarded by the personal server hence it can be available for familiar caregivers, users' investigation and approved health care providers. The healthcare application monitoring system can be integrated to provide assistance for living, oversee ambulatory therapy and individual monitoring of health to fitness. For instance, if the BAN is enabled by integrating with the smart phone applications, the monitoring of the individual daily activities can be recorded and the feedbacks are forwarded to maintain optimal health. By the gathered information, the insufficient body mass index should be elevated based on the alert from the personal BAN server. Parameters such as height, age and gender values are recommended for monitoring.

The integration of personal server and BAN provides tele-medical system that comprises of medical personnel. The medical server collects all the data related with the users and can be extended over a period for long term and the markers available in the server indicates the significant changes occur in the human health status such as improving health status, deteriorating. The alert provided by the markers reminds the healthcare professionals to track the users. Added, the health status information provided by BAN used to monitor cardiac patients' progress while rehabilitation in ambulatory settings, patients' observance about treatment guidelines such as regular exercise, users effects on drug therapy and compliance.

In this paper, hybrid Ciphertext-Policy Hierarchical Attribute-based Ring Signcryption (CP-HARS) is proposed for body area network security. The initial process of proposed system is preprocessed the patient's dataset using Enhanced Independent Component Analysis (EICA). 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. The proposed CP-HARS provides authentication, public verifiability, forwarding secret message confidentiality, veracity, non-refutation and message confidentiality. CP-

HARS uses secure symmetric algorithm to encrypt messages quickly and provides security in establishing health monitoring and dealt with the resource constraint devices. The remaining part of the paper illustrated as follows: Section 2 discussed the related work of existing security schemes of BAN. Section 3 discussed the proposed CP-HARS for BAN. Section 4 discusses the experiments and results. Finally Section 5 concludes the paper.

## II. Related Work

In this division, the most significant existing research is summarized. In BANs, secure sensor association is a non-trivial issue, because a healthcare worker must check whether a group of sensors are correctly and securely associated with an intended patient before any data communication happens. Lots of previous works focus only on group key agreement in sensor nodes [2].

Recently, Keoh et al. [3] and Li et al. [4] propose some protocols considering both sensor association and key agreement. In [3], each sensor node can be securely associated with the controller using public key based authentication. However, it does not take sensor-to-patient authentication into account. It is easily for malicious nodes to join the BAN to achieve the important medical data.

In [4], Group Device Pairing (GDP) is implemented to perform authentication and establish group keys. However, the computation and communication cost of GDP is very high. In particular, in order to achieve the group key, each sensor node needs n + 3 times modular exponentiation operations, where n is the total number of sensor nodes in the BAN. It is a large burden for the power and resource constrained medical sensor nodes.

JianShen et al., [5] proposed ECC and hash chains for perform authentication and key generation. First, a patient and a healthcare worker authenticate each other. Secondly, the authenticated healthcare worker associates the medical sensor nodes with the intended patient. Each node can establish a shared secret key with the Patient Controller (PC), and then the Light Strip Expansion (LED) blinking pattern can be transmitted using the shared secret key. The healthcare worker can confirm the secure sensor association when all the sensor nodes have the synchronized LED blinking pattern. Thirdly, a group key is computed by the PC, which then distributes the group key to all the sensor nodes by utilizing the shared secret keys. Note here that key distribution based on symmetric key cryptography is fast and efficient. We'd like to emphasize that ECC and hash chains are very efficient methods in cryptography. In particular, a point multiplication in ECC is more proficient compared to the modular exponentiation in RSA [6] [7]. In addition, hash operation is a kind of lightweight cryptographic primitive. The use of ECC and hash chains can satisfy the requirement of the resource limited medical sensors in BANs.

Lin Yao et al., [8] proposed A Biometric Key Establishment Protocol for Body Area Networks to provide security, integrity and confidentiality regarding the sensitive health care information. This approach steps forward to solve the issues integrated with privacy and security of the BANs. It also attempts to gather and distribute the session key secretly and efficiently to the biosensor and CU. This method mainly concerns with the biometric encryption. Here, the dynamic biometrics (electrocardiogram (ECG)) used to provide authenticity between CU and biosensor. The idea behind to use ECG, move towards from observing the dynamic and complex human body and subjecting the time variance and randomness of the subjects physiological state. In accordance with data minimization, the ECG data is collected and utilized in many applications.

Eschenauer and Gligor [9] demonstrates a Key-Management Scheme for Distributed Sensor Networks to assure both security requirement and operational functionality of DSNs. Selective distribution and revocation of keys are included in this scheme, to provide re-keying without considerable communication capabilities and computation. The approach uses simple set of rules for shared key discovery, re-keying, addition of incremental nodes, key revocation and path key establishment by relying on probabilistic key sharing amongst the random nodes of the graph. To determine the network connectivity and security, key management schemes are simulated and discussed in detail.

Poon et al., [10] proposed a Novel Biometrics Method to Secure Wireless Body Area Sensor Networks to provide security to the M-Health and Telemedicine for a wireless BAN, and demonstrate the concept by using IPI as example. By collecting 838 datasets from around 99 subjects, the method is evaluated and initiated that the minimum HTER is about is 2.58 percent i.e. FRR =3.99 percent and FAR = 1.18 percent. By sampling the signals at 1000 Hz and coded trait is about 128-bit binary sequence. There are few issues opened up for further investigations including coding schemes, compensation scheme of different channels for asynchrony and some other biometric traits. The parameter includes physiological phenomena, diction errors, motion artifacts and diseases.

## III. Proposed Methodology Of Cp-Hars For Ban

### *System overview*

System overview is illustrated in Fig 1. It demonstrates 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 preprocessed the patient's dataset using Enhanced Independent Component Analysis (EICA). 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). To protect information when the BAN controller lost or theft, the personal identification should be confirmed when attached with the controller. Investigation of CP-HARS is performed when to direct the access over the controller. A set of attributes and a private key label is provided to the ciphertext, in an attribute-based encryption which is organized with the access control, hence decryption can be performed similarly. To control the access rights, access structures are given to different users belonging to BAN controller.

### *A. Data preprocessing using ICA*

The dimensionality of the Data is reduced using preprocessing in EICA. It is a method of presenting the patient's data in a more comprehensible way by revealing the hidden structure in the data and often reducing the dimensionality of the representation. The BAN patient information contains more number of attributes. So EICA is used to reduce the attributes. A proper space has to be chosen, excluding the trailed eigen values to improvise the generalization performance of ICA, in EICA. To get rid of the trailed eigen value, ICA should precede space dimensionality reduction procedure before performing ICA whitening step. The generalization procedure of ICA can be enhanced and produce reduced computational complexity using the Principal Component Analysis (PCA) which belongs to a proper dimensionality reduction procedure.

### *1) Generalization analysis of ICA*

ICA should precede space dimensionality reduction procedure before performing ICA whitening step, to get rid of trailed eigen value. Excluding the trailed eigen values to improvise the generalization performance of ICA, in EICA. To minimize the mutual information of the random vector, the independent component has three major steps: normalization, rotations and whitening. Initially, the random vector is transformed into unit covariance matrix in the whitening process. By higher order cumulants, the mutual information is minimized by separating the source from independent components in the rotation operation. Lastly, in terms of phase (sign), norm and order a unique ICA representation is derived from the normalization procedure.

Specifically, let $x \in R^N$be a random vector representing a patient attributes, where, $N$ is the dimensionality of the data space. The data present in the rows and columns, is concatenated to form a vector when the unit variables are not proportionate. The standard variable provides unit norms are so desirable. Standardization avoids using variable with large variance which dominates the other variables unduly.

Let $\sum_x \in R^{N\times N}$ be the covariance matrix of $x$. The PCA of $x$ defines an orthogonal eigenvector matrix $\psi \in R^{N\times N}$ and a diagonal eigenvalue matrix $\Delta\in R^{N\times N}$ with diagonal elements in decreasing order: $\psi = [\psi_1, \dots, \psi_N], \Delta= diag\{\delta_1, \dots, \delta_N\}, \delta_1 \geq \delta_2 \geq \cdots \geq \delta_N$be a projection matrix whose column vectors are the first $n(n < N)$ leading eigenvectors of$\sum_x$ :

$$P = [\psi_1, \psi_2, \dots, \psi_N]$$

The new random vector $y \in R^n$ in this reduced ($n$-dimensional) PCA space is defined as follows

$$y = P^t x$$

The ICA method implemented in this appropriately reduced ($n$ -dimensional) PCA space is called as an Enhanced ICA method.

### *2) Criteria for deriving EICA method*

The enhanced generalization performance of the EICA method depends on the appropriate PCA space where the EICA method is implemented. The two roles of the PCA procedure: for patient data attribute representation and for ICA generalization. From the representation point of view, to choose a PCA space that keeps as much information as possible in order to faithfully represent the original data. For example, the proposed methods consider attribute name of Blood Pressure (BP) means it represent the high BP and Low BP. The PCA space is used to separate this kind of information based data processing. Then the same space eigen values are grouped under one clustering and other eigen values are formed another cluster. The PCA space chooses by based on two criterions such as energy and magnitude criterion.

Energy Criterion: The transformation from the high dimensional space to a low dimensional one should be constrained in such a way that as much representative information of the original data is reserved as possible.

Magnitude Criterion: The reduced PCA space doesn't includes small-value trailed eigen values, when implementing the EICA method.

### *3) Dimensionality of the reduced PCA space*

Based on both the representation and magnitude criterion, ICA computation is resolute for reducing the dimensionality of the PCA. Representation criteria shows high dimensionality and magnitude criteria shows low dimensionality, the main goal is to attain the balance between the two roles of PCA procedure. Specifically, for enhanced generalization performance, EICA's dimensionality reduction procedure should preserve a proper balance between the energy criterion- the need that the selected eigenvalues account for most of the spectral energy of the original data, for representational adequacy, and the magnitude criterion —the requirement that the eigenvalues of the covariance matrix in the reduced PCA space are not too small, for better generalization.

## *B. 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 ACO used to improve the fuzzy rules.

### *1) Ant Colony Optimization Algorithms for Learning Fuzzy Rule*

To apply ACO algorithms to a FRL problem, the following steps have to be performed:

Step 1: A FRL problem is Obtained ant it is represented as a graph or a similar structure easily covered by ants.

Step 2: Define the way of assigning a heuristic preference to each choice that the ant has to take in each step to generate the solution. Build the set of the input-output data pairs composed of $E_i'$that are situated in the input subspace defined by $E_i' = \{e_l = \left(x_1^l, \dots, x_n^l, y^l\right) \in E$ such that $\mu A_{il}\left(x_1^l\right) \dots \mu A_{in}\left(x_n^l\right). \mu B_j(y^l) \neq 0\}$.

Step 3: Establish an appropriate way of initializing the pheromone. Pheromone value of each assignment is obtained as follows $T_0 = \frac{\sum_{i=1}^{N_r} \max_{j=1}^{N_c} \eta_{ij}}{N_r}$

Step 4: Define a fitness function to be optimized. The fitness function establishes the quality of a solution. The measure considered will be the function called mean square error (MSE), which defined as $\mathrm{MSE}(\mathrm{RB}_k) = \frac{1}{2.|E|} \sum_{e_l \in E} \left(y^l - \right.$ FkX0l2.

Step 5: Select an ACO algorithm and apply it to the FRL problem.

- The set of nodes attainable from $R_i$(set of feasible neighborhood of node $R_i$) will be $J_k(i) = \{j \text{ such that } \eta_{ij} \neq 0\}$ while constructing the solution for ACO algorithm with the transition rules.
- The solution constructed based on the amount of pheromone ant k it will be $1/\mathrm{MSE}(\mathrm{RB}_k)$, with $\mathrm{RB}_k$being the RB generated by ant k.
- In the local pheromone trail update rule of the ACO algorithm, the most usual way of calculating $\Delta T_{ij}$ , $\Delta T_{ij} = T_0$ , will be used, thus considering the simple-ACO algorithm.

Then, 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 strings from search patients details to fuzzy linguistic variables and terms.

### *C. Hybrid ciphertext-policy hierarchical attribute-based ring signcryption*

In this subsection, the hierarchical attribute-based ring signcryption with cipher-policy is explained.

The hierarchy of the attribute is higher it is placed in upper level i.e. primary doctor and the attribute with lower hierarchy is placed in the lower level i.e. nurse is arranged in the matrix of HARS. This arrangement leads to hierarchical vectors or attributes, by sampling the attributes from the upper level to lower level. Using delegation mechanism, new attributes can be added with the original attributes without the need of delegator, thus helps in knowing the secret key from the key generator.

The proposed ciphertext-policy HARS (CP-HARS), has been applied to the security information of BAN. In CP-HARS, the potential decryptors should consists of attribute vectors the generates an access policies in the cipher texts. Without considering attribute set and the subset, the higher level user can share the secret key with the user at the lower level. Later, the CP-HARS security can be defined. The public parameters, access policies, query of key with respect to set of attribute vectors and the created attribute vectors can be attained by the attackers in full security. The attackers project the challenge with the set of attributes and messages. In accordance with the challenge policies, two different messages are chosen for the generation of ciphertext. To satisfy the access policy of challenge message, it cannot be distinguished which message has to generate ciphertext and the attackers doesn't provide query key associated with attribute vectors of set.

By employing Linear Secret Sharing Scheme (LSSS), a CP-HARS scheme has been constructed to attain access structure of suitable expressiveness. An attempt has been made to construct CP-HARS from Hierarchical Identity-based Encryption (HIBE) by considering the attribute vector as an identity vector in the HIBE.The union of attribute vectors has to meet the access policy to meet the colluding users, when the straightforward construction is susceptible to collusion attacks, in which the coalition of users administers to decrypt ciphertexts. Such attacks can be prevented in the future practice. By addressing the problem associated with randomization of secret keys to the users, with the help of well-determined dual encryption techniques, proves that the -HARS scheme is secure in the standardized model (i.e., without using random oracles) under the assumption of several non-instructiveness. The unimportant construction causes growth of public key size exponentially with the increased hierarchy size. While constructing, the public key is provided with maximum hierarchy size and it is linear and the ciphertext size is sovereign of the user hierarchy or the number of users.

#### *1) Linear Secret Sharing Schemes*

A set of parties P with the secret sharing scheme over $Z_p$ is called linear if,

1. A vector is formed when share of party over $Z_p$

2. A share generating matrix A for $\pi$, when A has n columns and $l$ rows exists. For $i = 1, .., l$the i-$^{th}$ row of A is marked by a party$\rho_i$, where $\rho$→function from $1, \dots, l$ to P. While considering column vector $\vec{s} = (s, s_2, \dots, s_n)$, where $s \in Z_p$ is the shared secret and $s_2, \dots, s_n \in Z_p$ are chosen randomly. Then $A\vec{s}$→vector of $l$ shares of the secret s with respect to $\pi$. $A_i$→ the i-th row of A, when $\lambda_i = A_i\vec{s}$ is the share belong to $\rho_i$.

#### *2) Notations and basic ideas*

In a CP-HARS system, the attribute matrix is organized in a matrix, which consists of L rows and D columns and given by,

$$U = (U_1, .., U_i, \dots, U_L)^T$$

Where $U_i$→ i-$^{th}$ row of U and enclosed with D attributes and $M^T$→ transposition of a matrix M. In each $U_i$ there may be some empty attributes which can be organized by a special symbol "ϕ".

The attribute vector of depth k (or hierarchical attribute at level k) defined as

The hierarchical attribute at level k or the attribute vector of depth k is defined as

$$\vec{u} = (u_1, u_2, \dots, u_k)$$

Where for each i from 1 to k, $u_i \in U_i$. This means that an attribute vector of depth k is collection of k attributes and the i-$^{th}$ attribute is chosen from the i-th row of the attribute matrix.

The$\vec{u}$ is a prefix of $\vec{u}$ if $\vec{u}$= $(\vec{u}, u'_{k+1}, u'_{k+2}, \dots, u_k)$, where k represents the depth of $\vec{u}$.

Let S = $\{\vec{u}\}$ → set of attribute vectors cardinality → |s|. As stated in Definition 1.

The collection of non-empty subsets of a set of parties is known as access structure. A is a group of non-empty subsets with depth of the vector is given by K, access structure is A. If a set S ∈ A, the set S is given as authorized set and satisfies A.

The access structure of the multi-level LSSS is given in definition 2: depth of the attribute vector k, access structure A, with the product of i-throw the sharing matrix is generated. The i$^{th}$ matrix of the A in the injection function ρ maps with the depth of attribute vector K. the hierarchical attribute is mapped with the row A in the injection function. The vector of the first coordinate is mapped with the depth of vector K.

In a CP-HABE system, a ciphertext generated with an access structure A is decryptable by a key associated with set S under the condition that $S \in A$. If a key for set $S'$ is able to delegate a key for a set S, it is required that each attribute vector of S have a prefix in $S'$. This yields the concept of Set Derivation of two sets.

For a set $S'$ of attribute vectors of depth k and a set S of attribute vectors of depth k + 1, we say that S is derived from $S'$, denoted by $S <= S'$, if $\forall\vec{u} \in S, \exists\vec{u} \in S'$, such that $\vec{u} = (\vec{u}, u_{k+1})$where $u_{k+1} \in U_{k+1}$.

#### *3) Modeling CP-HARS*

The description of CP-HABE and its protection model is given. A CP-HABE system for message space M and access structure space AS consists of the following four (probabilistic) algorithms.

*a)Setup (k):*The algorithm Setup takes no input other than the security parameter k and outputs the public key PK and a master secret key MSK. Given a security parameter k, the trusted Private Key Generator (PKG) first defines the set of universal attributes U in $Z_p$, where $|U| = l$. After that, a $d - 1$ default attributes set from $Z_p$is given as $\Omega = \{\Omega_1, \dots, \Omega_{d-1}\}$. Furthermore, PKG selects a pairing $e : G_1 \times G_1 \to G_2$ where the order of $G_1$ and $G_2$ is prime $p > 2^k$, and a generator g of $G_1$. PKG then chooses $t_1, .., t_l, t_{l+1}, \dots, t_{l+d-1} \in z_p$randomly and computes $T_i = g^{t_i}$where $1 \le i \le l + d - 1$. PKG also picks $\alpha \in Z_p$at random and computes $Y = e(g, g)^\alpha$. Finally, PKG selects three cryptographic hash functions: $H_1 : G_2 \to \{0,1\}^{|M|} \times Z_p^* \times G_1, H_2 : \{0,1\}^* \to Z_p^*$ and $H_3 : \{0,1\}^{|M|} \times Z_p^* \to Z_p^*$, where $|M|$denotes the length of the ciphertext. The public parameters PK are published as follows:

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

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

*b) Key Extract (MSK, ω):*To generate a secret key for the attribute set ω of attribute vectors of depth $\omega \subseteq u$, first choose random elements $r \in Z_p, R_0, R_1 \in G_3$ and compute

$$K_0 = g^{\alpha} g^{aw} R_0, K_1 = g^{w} R_1$$

Next, for each j from 1 to|S|, pick random elements

$$t_j \in Z_p, R_{(j,0)}, R_{(j,1)}, R_{(j,k+1)}, \dots., R_{(j,L)} \in G_3$$

For each attribute vector $\vec{u} = (u_1, u_2, \dots, u_k)$ of S, choose $v_x$ by finding $u_1$ as the x-th attribute of $U_1$ and compute its key component

$$K_{(j,0)} = V_x^{\omega} \left(H_1^{u_1} \dots H_k^{u_k}\right)^{t_j} R_{(j,0)}, K_{(j,1)} = g^{t_j} R_{(j,1)}, K_{(j,k+1)} = h_{k+1}^{t_j} R_{(j,k+1)}, \dots, K_{(j,L)} = h_L^{t_j} R_{(j,L)}$$

Outputs the private key $D_s = (K_0, K_1, \{K_{(j,0)}, \dots, K_{(j,L)}\}_{j=1}^{|S|})$

*c)Signcryption $(m, \omega_S, \omega_R)$:* To signcrypt a message m to a receiver R, the sender S follows the steps below:

- Chooses a subset $\omega'_S$with d elements from $\widehat{\omega}_s$(where f attributes $\{i_1, \dots, i_f\}$are chosen from $\omega_S$to signcrypt the message, and $d - f$attributes are chosen from default attributes set $\Omega$).
- The sender S randomly chooses $r \in Z_p^*$, and set $s = H_3(m, r)$, $U = g^s$, and $X = Y^s = e(g, g)\alpha. s$. S then computes $E_i = T_i^s$for each $i \in \omega' s$and for each $j \in \omega_R$.
- Let $\omega'_s = \{1, \dots, d\}$, and chooses $k \in \omega'_s$ randomly. Defines the elements in set $\omega'_S \cup \omega_R$to be the ring. For $l \in \omega'_s \cup \omega_R$ and $l \neq k$, chooses $U_l \in Z_p^*$at random and computes $h_l = H_2(m, U_l, X, \omega'_S \cup \omega_R, l)$, where $|\omega'_S \cup \omega_R| = n_R + d$. For $l = k$, chooses $r_k$ from $Z_p^*$randomly and computes
- $U_k = {E_k^{r_k}} \Big/ {\prod_{l \in \omega'_S \cup \omega_R, l \neq k} U_l . E_l}$
- $= {g^{t_k . r_k . s}} \Big/ {\prod_{l \in \omega'_S \cup \omega_R, l \neq k} U_l . g^{t_1 . h_l . s}}$
- $h_k = H_2(m, U_k, X, \omega'_S \cup \omega_R, k)$
- $V = E_k^{r_k + h_k}$
- Compute $y = (m \| r \| V \oplus H_1(X))$
- Finally, the ciphertext CT is denoted as $CT = \left(y, \omega'_S, \omega_R, U, \{U_l\}_{l=1}^{n_R+d}\right), \{E_i\}_{i=1}^{d}, \{E_i\}_{i=1}^{n_R}$

*d)Unsigncryption CT:* After receiving the ciphertext CT, R decrypts the ciphertext as follows.

- For $CT = (y, \left(y, \omega'_S, \omega_R, U, \{U_l\}_{l=1}^{n_R+d}\right), \{E_i\}_{i=1}^{d}, \{E_i\}_{i=1}^{n_R})$, select a subset $\omega'_R$ with d-elements subset from attribute set $\omega_R$.
- Computes
- $X' = \prod_{j \in \omega_{R'}} e\left(D_j, E_j\right)^{\Delta_{j,s}(0)}$
- $\prod_{j \in \omega_{R'}} e\left(g^{\frac{q(j)}{t_j}}, g^{t_j . s}\right)^{\Delta_{j,s}(0)}$
- And retrieves $m', r', V'$ as $\left(m' \| r' \| V'\right) = y \oplus H_1(X')$
- Computes $s' = H_3(m', r')$ and verifies whether $U = g^{s'}$ holds or not.
- For $l \in \{1, \dots, n_R + d\}$, computes $h'_l = H_2(m, U_l, X, \omega'_S \cup \omega_R, l)$ and verifies $e(g, \prod_{l=1}^{n_R+d} U_l . g^{t_l . h'_l . s'}) = e(g, V')$ holds or not. If so, R accepts CT as the valid ring signcryption on the message $m'$; R rejects otherwise.

The depth of the system is small in its maximum practice. The system public key is linear, when the no. of attributes in the matrix is linear with the no. of total attributes in the system. With the deepest level, the attribute vector is linear with the size of the secret key along with the linear depth of the number of available attribute vectors. At the setup phase, the pair is pre-computed hence no signcryption algorithm is needed in pairing operation. The ciphertext are independent at the receiver side, in the receiver hierarchy and access structure with the number of attribute vectors are also linear. When the access structure of the attribute vector is linear, the pairing operation also satisfies the decryption algorithm.

## IV. PERFORMANCE EVALUATION AND SECURITY ANALYSIS

In this section, the performance of proposed system is evaluated and the results are compares with the existing methods of ARSS and ECC with FO signcryption.

### A. *Performance Analysis*

A quantitative performance analysis is presented in this section. The energy consumption while message transmission and computation is the principle concern of this section. The size of the message being transmitted is analyzed, in which the energy consumption related directly with the message size.

#### 1) *Message Size*

The size of the complete cipher text is computed in this scheme. The cipher text is the concatenation of time, message and attributes.

Figure 3 illustrates the affiliation between the no. of users and the total message size at various levels of security. The message size with respect to the number of users is indicated by curves in Figure 3.

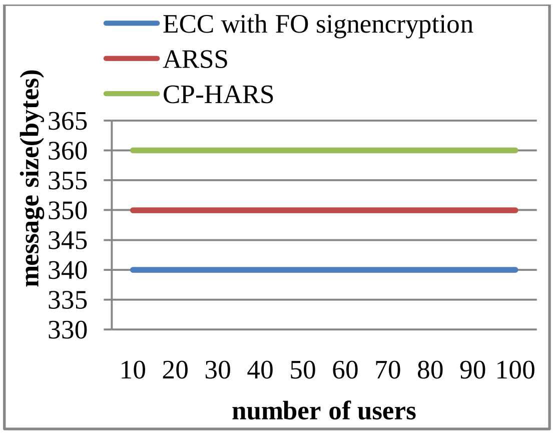

Figure 3: message size vs. number of users

Figure 4 shows the functional relationship between the message size and the security level. From Fig. 4, the message size has a linear relationship with the security level is observed. From Figure 4 the proposed CP-HARS achieved high security compare than existing ARSS and ECC with FO signcryption schemes.

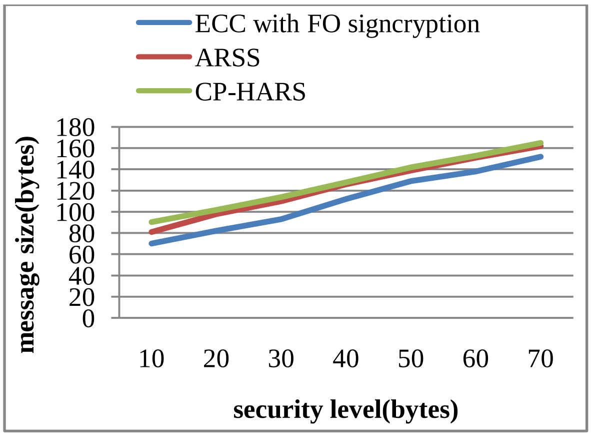

Figure 4: message size vs. security level

*2) Communication Overhead*

From the point concerns with communication, signcryption plays a vital role in contributing communication overhead. The overhead associated with the signcryption is the size of the message. The overhead for signcryption and designcryption are 5|q| + 4 and 1 respectively.The relationship between the security level and communication overhead is represented in Figure 5. The communication overhead for the proposed CP-HARS increases along with the security level. The communication overhead of the proposed CP-HARS is lesser compared to ECC with FO signcryption and ARSS scheme.

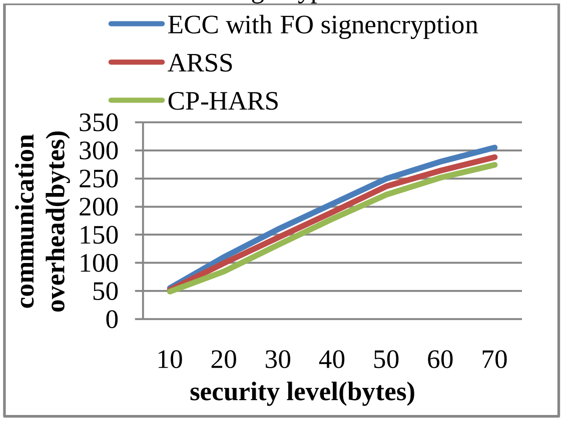

Figure 5: the communication overhead vs. security level

*3) Energy Consumption on Communication:*

The energy consumption of Signcryption in ARSS is calculated from the formula $E = U * I * T$, where I-is set of individual objects, T is code running time. However, while the public and private key generation speeds have been increased, encrypting and decrypting large volume of data is slow in existing system. The energy cost of fuzzy and sign then encryption and ECC with FO are compared to ARSS signcryption energy consumption to show that ARSS significantly reduces energy consumption. The results provide a very compelling argument for ARSS, showing that, based on an assumed battery life, the device using ARSS could execute the number of key exchange operations. Figure6 illustrates the relationship between the Energy consumption on communications and the number of users. ARSS has a less power computation than other schemes. Energy consumption while performing communication and computation is considered inclusively. When the number of users is higher, ARSS performs efficient communication. The energy consumption of CP-HARS is lesser when compared to the ECC with FO signcryption and ARSS scheme.

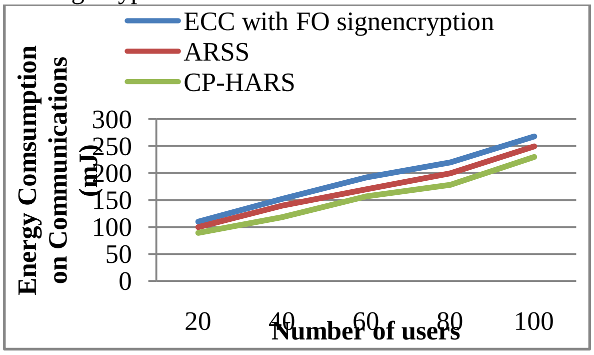

Figure 6: Energy consumption on communications with respect to the number of users

*4) Computational Cost:*

The cost of a computation as the message of the time taken by the computation and the cost of the hardware used for the computation.

Figure 7 demonstrates the computational cost of ARSS signencryption with other schemes. The observation can be figure out as follows: initially, the computational cost of signencryption is lesser compared to the other schemes. Energy consumption while performing communication and computation is considered incursively. When the number of users is higher, ARSS performs efficient communication. Signcryption shows rapid development since it is an emerging technique. ARSS provides better secured communication, since BAN controller provides less computation capacity between the external devices and controller. CP-HARS is achieved less computation cost compare than existing ARSS and ECC with FO signcryption schemes.

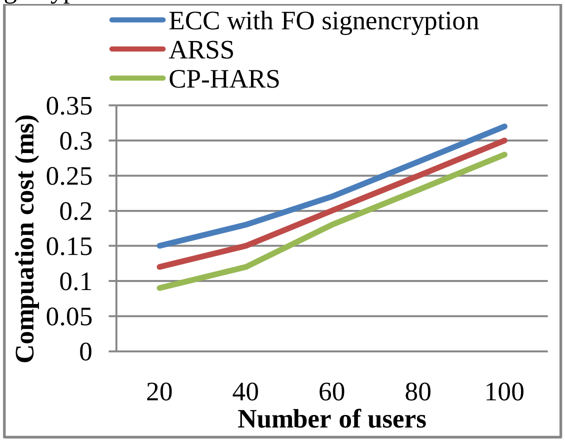

Figure 7: Computation cost vs. the number of users

Security analysis

The proposed method should satisfy the security analysis with respect to the features of security. The identifiers message value is different, even when the sender transmits the same message to different receivers with the random number r. Since, the message will be different for the individual Signcryption. The proposed CP-HARS compare to RSA and DSA. This proves that considerably smaller parameters can be used in CP-HARS than in other systems such as RSA and DSA, but with comparable levels of security.

*1)Correctness:*The algorithm is well verifiable as shown above. Unique unsigncryptability- The arbitrary length of the given message is m, the signcrypt message m and the output text is c. when the inputs is c, the algorithm unsigncrypts c and recuperate the original message.

*2) Security:*Proposed signcryption scheme simultaneously fulfill the security attributes of an encryption scheme and digital signature. And many additional properties: Confidentiality, Unforgeability, Integrity, and Non-repudiation, Public verifiability and Forward secrecy of message confidentiality

*3) Confidentiality:*The proposed algorithm is based on CP-HARS 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.

*4)Unforgeability:* This is not possible for an adaptive attacker to pretense the sender by creating a genuine signcrypted text that can be established by the unsigncryption algorithm. Because of the reason that any attacker doesn't know what all parameters are involved in signcrypting a text.

*5)Non-repudiation:*Since the points presents in the cipher message are selected form the sequence of points generated by selected private key using shared CP-HARS. Hence the user cannot deny because it's unique for every key.

## V. Conclusion

In this research, the proposed versatile cryptosystem submitted to as Ciphertext-Policy Hierarchical Attribute-based Ring Signcryption (CP-HARS) proposed for BAN security. The initial process of proposed system is preprocessed the patient's dataset using Enhanced Independent Component Analysis (EICA). Then ACO-FO is used to improve the interoperability of BAN system. A CP-HARS scheme is constructed with short ciphertexts. The scheme is proven secure in the standard model under non-interactive assumptions. The proposed CP-HARS is compared to existing Attribute-based Ring Signcryption Scheme (ARSS) and Elliptic Curve Cryptography with Fuzzy Ontology (ECC with FO) signcryption. The experimental output provides unforgeability, authenticity, non-repudiation and confidentiality to achieve higher security, lower energy consumption, lesser computational cost and communication overhead. The future work contributes, designing of efficient signcryption schemes to achieve reduced storage costs, meet the design necessities of the BANs and computational cost. Based on attribute encryption, and a lightweight signcryption scheme, designing of efficient signcryption approach to meet the security concern of the controller and to improve the inter-sensor communications amongst BANs.

## VI. References

[1] E.Jovanov, and A. Milenkovic, "Body Area Networks for Ubiquitous Healthcare Applications: Opportunities and Challenges", Journal of Medical Systems, vol. 35, no.5, pp.1245-1254, 2011.

[2] T. Donovan, J. Donoghue, C. Sreenan, D. Sammon, P. Reilly, and K. A. Connor, "A Context Aware Wireless Body Area Network (BAN)," in proc. of the Pervasive Health Conference, pp. 1-8, April 2009.

[3] S. L. Keoh, E. Lupu, and M. Sloman, "Securing Body Sensor Networks: Sensor Association and Key Management," proc. of the 7th Annual IEEE Int. Conference on Pervasive Computing and Communications (PerCom), Galveston, Texas, pp. 1-6, March 2009.

[4] M. Li, S. Yu, W. Lou, and K. Ren, "Group Device Pairing based Secure Sensor Association and Key Management for Body Area Networks," proc. of IEEE INFOCOM, San Diego, CA, pp. 1-9, March 2010.

[5] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: Securing Sensor Networks with Public Key Technology," in Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04), Washington, DC, USA, pp. 59-64, October 2004.

[6] D. J. Malan, M. Welsh, and M. D. Smith, "A Public- Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography," in 1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON'04), Santa Clara, California, pp. 71-80, October 2004.

[7] J.Shen, S.Moh, and I. Chung, "A Novel Key Management Protocol in Body Area Networks" , ICNS: The Seventh International Conference on Networking and Services, 2011.

[8] L.Yao, B.Liu, G.Wu, Kai Yao, and JiaWang, "A Biometric Key Establishment Protocol for Body Area Networks", IJDSN, vol.2011.

[9] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks", Version, pp. 41–47, November 2002.

[10] C. Poon, Y.-T. Zhang and S.-D. Bao, "A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health" ,vol. 44, no. 4, pp. 73–81, April 2006.