Chapter 4
CHAPTER 4

SECURITY ANALYSIS IN BODY AREA NETWORKS USING ATTRIBUTE-BASED RING SIGNCRYPTION SCHEME

4.1. INTRODUCTION

Wireless Body Area Networks (WBANs) (Otto et al., 2006) are a type of wireless sensor networks, where a group of sensors placed on the human body measure specific physiological parameters of a person and relay it to the monitoring medical center or hospital. This relay happens via the Internet or a cellular network, using personal digital assistants (PDAs) or cellular phones as intermediary devices. Thus, WBANs seem to be a promising solution for the problem of continuous health monitoring. However, with a patient’s personal health data travelling in the open, typically in a wireless channel, to reach the intermediary device and then the monitoring station, securing this data becomes critical. This, coupled with the fact that medical decisions are made based on the data received, assumes significant focus in the research on WBANs.

Data 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 of a BAN in opposition to an outsider is majorly concentrated. In view of the fact that a BAN consists of all entities touching the body, the objective is to secure the communication of these devices against outsider devices that do not touch the body.

To achieve security in any network, the messages to be transmitted are encrypted using specialized encryption schemes and a special encryption key, and decrypted at the receiver end. Many advanced encryption algorithms, which are used for securing wireless networks, cannot be used in WBANs, given that they have severe power constraints and resource constraints since they are small sensor devices residing on a person (Otto et al., 2006). Thus, it becomes crucial to design algorithms that are simple in computation and resource utilization, yet achieve the desired security. At the heart of any encryption algorithm is the successful management of the special encryption key. The key generation scheme must also be computationally inexpensive yet secure.
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 (Tan, C.C., et al., 2008), (Morchon, O.G., et al., 2006) (Malasri, K., et al., 2007). BANs delivers the same bits of data independent of the application domain, but this data can have distinct purposes in different domains. For example, heartbeat can carry an indication of health in the care domain or an indication of performance potential in domains of sports or entertainment. This example shows that semantic interoperability requires not only sharing of data and concepts, but also positioning them in the specific purpose of the application for their appropriate use.

Ontologies have been acknowledged in the literature as a means to achieve interoperability between systems at semantic level (Ouksel, A., et al., 1999). Ontology is a conceptualization of real-world phenomena (Guizzardi, G., et al., 2005), so need to investigate which concepts should be included in ontology to achieve semantic interoperability between sensor networks and sensor applications, and what is required to direct their appropriate use.

4.1.1. SIGNCRYPTION

Signcryption can offer authentication and confidentiality simultaneously with better efficiency than traditional signature-then-encryption approach. Ring signature enables a user to conscribe arbitrarily a group of ring members and sign a message on behalf of the ring without revealing the real identity. By integrating the notion of signcryption and ring signature, ring signcryption has been initialized to leak secrets in an authenticated and confidential way anonymously.

In cryptography, signcryption is a public-key primitive that simultaneously performs the functions of both digital signature and encryption. Encryption and digital signature are two fundamental cryptographic tools that can guarantee the confidentiality, integrity, and non-repudiation. Until 1997, they were viewed as important but distinct building blocks of various cryptographic systems. In public key schemes, a traditional method is to digitally sign a message then followed by an encryption (signature-then-encryption) that can have two problems: Low efficiency and high cost of such summation, and the case that any arbitrary scheme cannot guarantee security.
Signcryption provides the properties of both digital signatures and encryption schemes in a way that is more efficient than signing and encrypting separately. This means that at least some aspect of its efficiency (for example the computation time) is better than any hybrid of digital signature and encryption schemes, under a particular model of security. Note that sometimes hybrid encryption can be employed instead of simple encryption, and a single session-key reused for several encryptions to achieve better overall efficiency across many signature-encryptions than a signcryption scheme but the session-key reuse causes the system to lose security under the relatively weak CPA model. This is the reason why a random session key is used for each message in a hybrid encryption scheme but for a given level of security (i.e., a given model, say CPA), a signcryption scheme should be more efficient than any simple signature-hybrid encryption combination.

As one of the extension of signcryption, ring signcryption was initially formalized and allowed a signer conscripts a group of ring members and signcrents one message on behalf of the ring without revealing his real identity. Furthermore, the procedure of signcryption does not need the cooperation of other ring members. Thus, ring signcryption can be applied in some concrete applications where authenticity, confidentiality and anonymity receive concern simultaneously.

On the other hand, to use biometric-based identities in the Identity-based cryptosystem, attribute-based cryptography has been proposed in 2005 (Sahai, A, et al., 2005). (Guo, Z, et al., 2013) introduced ring signcryption in the attribute-based cryptography by integrating the notion of attribute-based ring signature (Li, J, et al., 2008) and attribute-based encryption. In an attribute-based signcryption, a signer can get its private key for attributes set from a trusted private key generator. Then, this signer can signcrypt message on behalf of a subset. Here, all users with this attributes subset can be considered as the ring. A concrete attribute-based ring signcryption based on bilinear pairings has also been suggested in this work. Any signcryption scheme should have the following properties:

**Correctness**

Any signcryption scheme should be verifiably correct.
**Efficiency**

The computational costs and communication overheads of a signcryption scheme should be smaller than those of the best known signature-then-encryption schemes with the same provided functionalities.

**Security**

A signcryption scheme should simultaneously fulfil the security attributes of an encryption scheme and those of a digital signature. Such additional properties mainly include: Confidentiality, Unforgeability, Integrity, and Non-repudiation. Some signcryption schemes provide further attributes such as Public verifiability and Forward secrecy of message confidentiality while the others do not provide them. Such properties are the attributes that are required in many applications while the others may not require them. Hereunder, the above-mentioned attributes are briefly described.

- **Confidentiality**: It should be computationally infeasible for an adaptive attacker to gain any partial information on the contents of a signcrypted text, without knowledge of the sender's or designated recipient's private key.

- **Unforgeability**: It should be computationally infeasible for an adaptive attacker to masquerade as an honest sender in creating an authentic signcrypted text that can be accepted by the unsigncryption algorithm.

- **Non-repudiation**: The recipient should have the ability to prove to a third party (e.g. a judge) that the sender has sent the signcrypted text. This ensures that the sender cannot deny his previously signcrypted texts.

- **Integrity**: The recipient should be able to verify that the received message is the original one that was sent by the sender.

- **Public verifiability**: Any third party without any need for the private key of sender or recipient can verify that the signcrypted text is the valid signcryption of its corresponding message.

- **Forward secrecy of message confidentiality**: If the long-term private key of the sender is compromised, no one should be able to extract the plaintext of previously signcrypted texts. In a regular signcryption scheme, when the long-term private key
is compromised, all the previously issued signatures will not be trustworthy any more. Since the threat of key exposure is becoming more acute as the cryptographic computations are performed more frequently on poorly protected devices such as mobile phones, forward secrecy seems an essential attribute in such systems.

4.1.2. ATTRIBUTE BASED ENCRYPTION

Attribute-Based Encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

The concept of attribute-based encryption was first proposed by Amit Sahai and Brent Waters and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters. Recently, several researchers have further proposed Attribute-based encryption with multiple authorities who jointly generate users' private keys.

Types of Attribute-Based Encryption schemes

Attribute-Based Encryption schemes can be typified under two broad categories: Key-Policy Attribute-Based Encryption (KP-ABE) and Cipher Text-Policy Attribute-Based Encryption (CP-ABE). In KP-ABE, users' secret keys are generated based on an access tree that defines the privileges and scope of the concerned user, and data are encrypted over a set of attribute. However, CP-ABE uses access trees to encrypt data and users' secret keys are generated over a set of attribute.

Usage

Attribute-based encryption (ABE) can be used for log encryption. Instead of encrypting each part of a log with the keys of all recipients, it is possible to encrypt the log only with attributes which match recipients' attributes. This primitive can also be used for broadcast encryption in order to decrease the number of keys used. Although the
concept of ABE is very powerful and promising, ABE systems suffer mainly from two drawbacks: non-efficiency and non-existence of attribute revocation mechanism. The other challenges include i) Key coordination, ii) Key escrow, and iii) Key revocation

4.1.3. KEY COORDINATION

A key management server in a Storage Area Network (SAN) provides encryption keys for source and destination storage objects and also associates destination storage objects with source storage objects. When a source object is to be replicated, a replication facility in a storage system of a new destination object requests the key management server to associate the destination object with the source object and assign the data encryption key of the source object or a new data encryption key to the destination object. For recovery of the source object, a replication facility in the storage system of the source object obtains information from the key management server about the replica associated with the source object for replicating data from the destination object back to the source object.

In view of the above, there has been a method and system for automation of coordination of encryption keys in a SAN based environment where an encryption engine, device management, and key management are not co-located. A key management server in a storage area network provides encryption keys for source and destination storage objects and also associates destination storage objects with encrypted source storage objects. When an encrypted source object is to be replicated, a replication facility in a storage system of a new destination object requests the key management server to associate the destination object with the source object and assign the data encryption key of the source object or a new data encryption key to the destination object.

For recovery of the source object, a replication facility in the storage system of the source object obtains information from the key management server about the replica associated with the source object for replicating data from the destination object back to the source object. The replication can occur locally for the case where the source object and the destination object are in storage of the same storage system, or the replication can occur remotely for the case where the source object and the destination object are in different storage systems.
In a preferred implementation, the key management server also keeps track of replication status of the associated source and destination storage objects. A replication facility can ask the key management server whether replication for a destination object is ongoing or has been completed, or whether restoration of a source object is ongoing or has been completed. Thus, a replication facility can recover from a failure to access an encrypted storage object having at least one replica by requesting the key management server to identify and provide the key information and replication status of any suitable replicas that may provide data for restoration of the failed storage object.

If a replica is found that is a complete copy of the failed storage object, then the identity and the key information of that replica can be used for fully restoring the failed storage object. The key information can be inspected to determine whether or not that replica and the failed storage object use the same data encryption key or whether they use different data encryption keys, in order to coordinate the decryption and encryption of the data copied from the replica to the failed storage object for the case where that replica and the failed storage object use different data encryption keys.

4.1.4. KEY ESCROW

Key escrow (also known as a “fair” cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees’ private communications, or governments, who may wish to be able to view the contents of encrypted communications.

The technical problem is a largely structural one since access to protected information must be provided only to the intended recipient and at least one third parties. The third party should be permitted access only under carefully controlled conditions, as for instance, a court order. Thus far, no system design has been shown to meet this requirement fully on a technical basis alone. All proposed systems also require correct functioning of some social linkage, as for instance the process of request for access, examination of request for 'legitimacy' (as by a court), and granting of access by technical personnel charged with access control. All such linkages / controls have serious problems from a system design security perspective. Systems in which the key may not be changed
easily are rendered especially vulnerable as the accidental release of the key will result in many devices becoming totally compromised, necessitating an immediate key change or replacement of the system.

On a national level, this is controversial in many countries due to technical mistrust of the security of the escrow arrangement (due to a long history of less than adequate protection of others’ information by assorted organizations, public and private, even when the information is held only under an affirmative legal obligation to protect it from unauthorized access), and to a mistrust of the entire system even if it functions as designed. Thus far, no key escrow system has been designed which meets both objections and nearly all have failed to meet even one.

Key escrow is proactive, anticipating the need for access to keys; a retroactive alternative is key disclosure law, where users are required to surrender keys upon demand by law enforcement, or else face legal penalties. Key disclosure law avoids some of the technical issues and risks of key escrow systems, but also introduces new risks like loss of keys and legal issues such as involuntary self-incrimination. The ambiguous term key recovery is applied to both types of systems.

4.1.5. KEY REVOCATION

In the operation of some cryptosystems, usually Public Key Infrastructures (PKIs), a Certificate Revocation List (CRL) is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted. There are two different states of revocation defined in Internet Engineering Task Force’s RFC 5280:

- Revoked: A certificate is irreversibly revoked if, for example, it is discovered that the certificate authority (CA) had improperly issued a certificate, or if a private-key is thought to have been compromised. Certificates may also be revoked for failure of the identified entity to adhere to policy requirements, such as publication of false documents, mis-representation of software behaviour, or violation of any other policy specified by the CA operator or its customer. The most common reason for revocation is the user no longer being in sole possession of the private key (e.g., the token containing the private key has been lost or stolen).
Hold: This reversible status can be used to note the temporary invalidity of the certificate (e.g., if the user is unsure if the private key has been lost). If, in this example, the private key was found and nobody had access to it, the status could be reinstated, and the certificate is valid again, thus removing the certificate from future CRLs.

Expiration dates are not a substitute for a CRL. While all expired certificates are considered invalid, not all unexpired certificates should be valid. CRLs or other certificate validation techniques are a necessary part of any properly operated PKI, as mistakes in certificate vetting and key management are expected to occur in real world operations.

In a noteworthy example, a certificate for Microsoft was mistakenly issued to an unknown individual, who had successfully posed as Microsoft to the CA contracted to maintain the ActiveX 'publisher certificate' system (VeriSign). Microsoft saw the need to patch their cryptography subsystem so it would check the status of certificates before trusting them. As a short-term fix, a patch was issued for the relevant Microsoft software (most importantly Windows) specifically listing the two certificates in question as "revoked".

Eventually, a public key will need to be removed from service. This may be because that the corresponding private key has been compromised or irretrievably lost. "Role" keys, such as those for Postmaster, provide good examples of innocently compromised keys. When a member of staff leaves an institution, it is undesirable that they should still be able to read mail addressed to Postmaster, or to be able to sign documents as if they still had that role. Key revocation is the manner in which PGP public keys are permanently retired.

It is suggested that a key revocation certificate should be generated as soon as the key pair is created. This certificate should be held by a trusted third party, exactly as the key-escrow facility described above. Once more, adequate proof of identity will be required before the certificate is released and issued, to guard against malicious denial of service attacks. If the keys are generated by the institution, there will be no difficulty in also generating the revocation certificate and storing it securely. If the user generates the key pair, they must be able to obtain advice on how safely to create, store, recover and use a revocation certificate. The present PGP documentation is rather lacking in this respect.
4.2. METHODOLOGY

In this research work, Attribute-based Ring Signature Scheme (ARSS) is proposed for Body Area Network security. The initial process of proposed system is pre-processed 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 using 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, unforgeability, non-repudiation, public verifiability, and forward secrecy of message confidentiality. Since it is based on ARSS can use any fast and secure symmetric algorithm for encrypting messages, it has great advantages to be used for security establishments in health monitoring and when dealing with resource constrained devices.

4.2.1. DATA PREPROCESSING USING INDEPENDENT COMPONENT ANALYSIS (ICA)

Data pre-processing is often beneficial to reduce the dimensionality of the data using ICA. 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. It can also be seen as a method of dimensionality reduction as finding a parsimonious representation of the data. Dimensionality reduction is not the primary aim of ICA and in fact most ICA algorithms favour moderate dimensionalities of data.

In signal processing, independent component analysis (ICA) is a computational method for separating a multivariate signal into additive subcomponents. This is done by assuming that the subcomponents are non-Gaussian signals and that they are statistically independent from each other. ICA is a special case of blind source separation. A common example application is the "cocktail party problem" of listening in on one person's speech in a noisy room. Independent component analysis attempts to decompose a multivariate signal into independent non-Gaussian signals. As an example, sound is usually a signal
that is composed of the numerical addition, at each time t, of signals from several sources. The question then is whether it is possible to separate these contributing sources from the observed total signal. When the statistical independence assumption is correct, blind ICA separation of a mixed signal gives very good results. It is also used for signals that are not supposed to be generated by a mixing for analysis purposes.

A simple application of ICA is the "cocktail party problem", where the underlying speech signals are separated from a sample data consisting of people talking simultaneously in a room. Usually the problem is simplified by assuming no time delays or echoes.

An important note to consider is that if N sources are present, at least N observations (e.g. microphones) are needed to recover the original signals. This constitutes the square case (J = D, where D is the input dimension of the data and J is the dimension of the model). Other cases of underdetermined (J > D) and over determined (J < D) have been investigated. That the ICA separation of mixed signals gives very good results is based on two assumptions and three effects of mixing source signals. Two assumptions:

1. The source signals are independent of each other.
2. The values in each source signal have non-Gaussian distributions.

Three effects of mixing source signals:

1. Independence: As per assumption 1, the source signals are independent; however, their signal mixtures are not. This is because the signal mixtures share the same source signals.

2. Normality: According to the Central Limit Theorem, the distribution of a sum of independent random variables with finite variance tends towards a Gaussian distribution. Loosely speaking, a sum of two independent random variables usually has a distribution that is closer to Gaussian than any of the two original variables. Here we consider the value of each signal as the random variable.

3. Complexity: The temporal complexity of any signal mixture is greater than that of its simplest constituent source signal.

Those principles contribute to the basic establishment of ICA. If the signals we happen to extract from a set of mixtures are independent like sources signals, or have
non-Gaussian histograms like source signals, or have low complexity like source signals, then they must be source signals.

The major concept of the ICA presumes that data are linearly combined through a collection of separate independent sources and demix these signal sources in accordance with their statistical independency measured through mutual information. In order to validate its approach, an underlying assumption is that at most one source in the mixture model can be allowed to be a Gaussian source. This is due to the fact that a linear mixture of Gaussian sources is still 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 \([x^{(1)}, x^{(2)}, \ldots, x^{(N)}]\), the independent elements are the directions (vectors) along which the statistics of projections of the data vectors are independent of each other. It means, when \(A\) represents a transformation from the given reference frame to the independent component reference frame, at that moment

\[x = Ae\]

In order that \(p(e) = \pi_{pa}(et)\).

Where \(pa(.)\) represents the marginal distribution and \(p(e)\) stands for the joint distribution over the n-dimensional vector \(e\). Generally, the scheme for carrying out Independent Component Analysis (ICA) is expressed as the scheme for the purpose of deriving one particular \(W\),

\[y = Wx\]

In order that each component of \(y\) (i.e., each \(y_i\)) becomes independent of each other. When the individual marginal distributions are non-Gaussian, subsequently the derived marginal densities turn out to be a scaled permutation of the original density functions when one such \(W\) can be obtained. One general learning scheme (Zhang et al., 2012) for the purpose of finding one \(W\) (as derived from the normal gradient descent of Kullback-Leibler divergence among joint density and the product of marginal densities) is

\[\Delta W = \eta(I - f(y)y^T)W\]
Where \( f(y) \) is a nonlinear function of the output vector \( y \) (such as a cubic polynomial or a polynomial of odd degree, or a sum of polynomials of 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.

4.2.2. ANT COLONY OPTIMIZATION BASED FUZZY ONTOLOGY (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, this research adopted ACO and its improved the fuzzy rules.

Ant Colony Optimization Algorithm

In computer science and operations research, the ant colony optimization algorithm (ACO) is a probabilistic technique for solving computational problems which can be reduced to finding good paths through graphs. This algorithm is a member of the ant colony algorithms family, in swarm intelligence methods, and it constitutes some meta-heuristic optimizations. Initially proposed by Marco Dorigo in 1992 in his PhD thesis, the first algorithm was aimed to search for an optimal path in a graph, based on the behaviour of ants seeking a path between their colony and a source of food. The original idea has since diversified to solve a wider class of numerical problems, and as a result, several problems have emerged, drawing on various aspects of the behaviour of ants. From a broader perspective, ACO performs a model-based search and share some similarities with Estimation of Distribution Algorithms. In the natural world, ants of some species (initially) wander randomly, and upon finding food return to their colony while laying down pheromone trails. If other ants find such a path, they are likely not to keep travelling at random, but instead to follow the trail; returning and reinforcing it if they eventually find food (see Ant communication).

Over time, however, the pheromone trail starts to evaporate, thus reducing its attractive strength. The more time it takes for an ant to travel down the path and back again, the more time the pheromones have to evaporate. A short path, by comparison,
gets marched over more frequently, and thus the pheromone density becomes higher on shorter paths than longer ones. Pheromone evaporation also has the advantage of avoiding the convergence to a locally optimal solution. If there were no evaporation at all, the paths chosen by the first ants would tend to be excessively attractive to the following ones. In that case, the exploration of the solution space would be constrained. The influence of pheromone evaporation in real ant systems is unclear, but it is very important in artificial systems.

The overall result is that when one ant finds a good (i.e., short) path from the colony to a food source, other ants are more likely to follow that path, and positive feedback eventually leads to all the ants following a single path. The idea of the ant colony algorithm is to mimic this behaviour with "simulated ants" walking around the graph representing the problem to solve.

**PSEUDO CODE**

```pseudo
class ACO_MetaHeuristic

    procedure ACO_MetaHeuristic
        while(not_termination)
            generateSolutions()
            daemonActions()
            pheromoneUpdate()
        end while
    end procedure

definition Fuzzy Ontology

    Ontology can be defined as a systematic description of part-of relationships and entity dependencies [appropriate references are shown in the corresponding state-of-the-art document]. In other words, ontology consists of a hierarchical description of important classes (or concepts) in a particular domain, along with the description of the properties (of the instances) of each concept. The Web Ontology Language (OWL) is a family of knowledge representation languages for authoring ontologies and Description Logics (DL) are a family of knowledge representation languages which can be used to
represent the terminological knowledge of an application domain in a structured and formally well-understood way. Today description logic has become a cornerstone of the Semantic Web for its use in the design of ontologies.

**Table 4.1. ASPECT COMPARISON BETWEEN FUZZY AND CRISP ONTOLOGY**

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Fuzzy Ontology</th>
<th>Crisp Ontology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiply-located terms</td>
<td>Does not occur</td>
<td>Issue for disambiguation</td>
</tr>
<tr>
<td>Query expansion</td>
<td>Depends on membership value</td>
<td>Depends on location only</td>
</tr>
<tr>
<td>Customization</td>
<td>Simple, based on modification of membership values</td>
<td>Requires new ontology and/or ontology sharing</td>
</tr>
<tr>
<td>Intermediate locations for grouping</td>
<td>Unnecessary</td>
<td>Needed for construction may be useful</td>
</tr>
<tr>
<td>Storage required</td>
<td>Depends on the number of terms in the ontology and the membership values of the relations, can be smaller or larger than crisp</td>
<td>Depends on number of terms in the ontology</td>
</tr>
<tr>
<td>Knowledge representation</td>
<td>Related to use</td>
<td>Related to structure</td>
</tr>
</tbody>
</table>

The Web Ontology Language Description Logics (OWL DL) become less suitable in domains in which the concepts to be represented do not have precise definitions. In our case, this scenario is, unfortunately, likely the rule rather than an exception. To handle this problem, the use of fuzzy ontology offers a solution. Classical ontology languages are not appropriate to deal with imprecision or vagueness in knowledge. Therefore, DL for the semantic web can be enhanced by various approaches to handle probabilistic or possibilistic uncertainty and vagueness. Although fuzzy logic was introduced already in the 1960’s, the research on fuzzy ontologies was almost non-existent before 2000, so we can claim that this is a fairly new research field with a great potential.
This is even more surprising considering that Pena reasoned already in the 1980’s why the use of fuzzy logic as the basis for ontology building would be beneficial and solve many problems pertaining to classical ontologies. He proposed “to reject the maximality rule, according to which only altogether true sentences are true, and embracing instead the rule of endorsement, which means that whatever is more or less true is true”. The advantages of fuzzy ontology are:

- positing fuzzy predicates usually simplifies our theories in most scientific fields
- fuzzy predicates are much more plausible, and give us a much more attractive and cohesive worldview, than their crisp counterpart
- degree-talk and comparative constructions

In recent years, it has been pointed out that classical ontologies are not appropriate to deal with imprecise and vague knowledge, which is inherent to several real world domains (Sanchez, 2006).

Surveying the literature, we can find that there is no unique definition of fuzzy ontology. In the simplest case, a fuzzy ontology is a pair (C, R), where C is a set of (fuzzy) concepts and R is a set of (fuzzy) binary (n-ary) relations. In different approaches, this pair can be extended in numerous ways:

- individuals (I), fuzzy axioms (A), (Calegari, et al., 2007)
- concept hierarchy (H) and axioms
- attributes of a concept, concept hierarchy, fuzzy events of a concept (Zhou, G, et al., 2008)
Fuzzy ontology can be seen as an extended domain ontology which makes use of the specific domain and fuzzy information processing as follows: (i) the input is unstructured data; (ii) the definition of related concepts in the domain, e.g. instances, objects, and their relationships; (iii) the generation of domain ontology; (iv) the domain ontology extended as fuzzy ontology; and (v) applying the fuzzy ontology to the specific domain.

It is important to note, that most of the definitions in the literature are quite restrictive and are mostly anchored to a specific application area as “a fuzzy ontology is simply an ontology which uses fuzzy logic to provide a natural representation of imprecise and vague knowledge and eases reasoning over it.”

The description logic behind the reasoning, the most popular is fuzzy SHOIN(D), a fuzzy generalization of SHOIN(D) which is one of the classical logic schemes used in the Semantic Web. This approach allows concrete domains (data types) to be represented.

**Figure 4.1 THE PROCESS OF CONSTRUCTING A FUZZY ONTOLOGY AS EXTENDED DOMAIN ONTOLOGY**

- Unstructured data
- News article → Instances, Objects, Relations → Domain ontology → Apply ontology into domains → Fuzzy ontology
by fuzzy sets. Moreover, it introduces fuzzy modifiers, fuzzy axioms, fuzzy RBoxes, fuzzy TBoxes, and fuzzy ABoxes. The fuzzy SHOIN(D) was originally proposed for logic-based information retrieval in a document management system.

In fact, SHOIN(D) is an equivalent of OWL DL, and from this follows that fuzzy SHOIN(D) is convenient as a formal basis for bringing vagueness into OWL. There are numerous proposals to encode vague information into OWL, such as using OWL extension, transforming fuzzy DL into classical DL, and last but not least using OWL2 annotations.

A recent development in the field is the appearance of type-2 fuzzy ontologies (T2FO). Lee et al., (2010) introduced a T2FO, which is composed of (i) a type-2 fuzzy personal profile ontology; (ii) a type-2 fuzzy food ontology; and (iii) a type-2 fuzzy-personal food ontology.

**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 and 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:

1. Conclude the rules: A rule $R_i - i = 1, ..., N_r$—defined by means of an antecedent combination, $R_i = \text{IF } X_1 \text{ is } A_{i1} \text{ and } X_n \text{ is } A_{in} \text{ will be included in the graph if and only if: } \exists e_1 = (x_1^l, ..., x_n^l, y^l) \in E \text{ in order that } \mu A_{i1}(x_1^l) ... \mu A_{in}(x_n^l) \neq 0$. Specifically, there is at least one example located in the fuzzy input subspace characterized by the antecedents considered in the rule.

2. 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: $e_1 = (x_1^l, ..., x_n^l, y^l) \in E \text{ in order that } \mu A_{i1}(x_1^l) ... \mu A_{in}(x_n^l). \mu B_j(y^l) \neq 0$. Specifically, there is at least one example placed in the fuzzy input subspace that is covered by such a consequent.
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 $E'_i = \{ e_i = (x_1^i, ..., x_n^i, y^i) \in E \text{ such that } \mu_{A_{il}}(x_1^i) ... \mu_{A_{ln}}(x_n^i), \mu_{B_j}(y^i) \neq 0 \}$. 

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

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

Step 4: Determine a fitness function 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 $\text{MSE}(RB_k) = \frac{1}{2 \cdot |E|} \sum_{e_i \in E} (y^i - F_k(X_0^i))^2$.

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

- The collection of nodes attainable from $R_i$ (set of possible neighbourhood of node $R_i$) 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 ant $k$ puts on the couplings belonging to the solution created by it will be $1/\text{MSE}(RB_k)$, 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.
4.2.3. ATTRIBUTE-BASED RING SIGNCRYPTION SCHEME (ARSS) FOR SECURITY

In this proposed scheme, the external user’s controller can signcrypt a message on behalf of \( d \) attributes, where \( d \) will be defined in the Setup algorithm. Then review Lagrange interpolation as follows. Given \( d \) points \( q(1), \ldots, q(d) \) on a \( d-1 \) degree polynomial, \( q(i) \) for any \( i \in \mathbb{Z}_p \) can be computed by adopting Lagrange interpolation technique. Assume \( S \) be a set in \( \mathbb{Z}_p \) with \( d \)-elements and the Lagrange coefficient \( \Delta_{i,S} \) for \( i \in \mathbb{Z}_p \) as follows.

\[
\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x - i}{i - j}
\]

**Setup (k)**

Given a security parameter \( k \), the trusted private key generator (PKG) first defines the set of universal attributes \( U \) in \( \mathbb{Z}_p \), where \( |U| = 1 \). After that, a \( d-1 \) default attributes set from \( \mathbb{Z}_p \) is given as \( \Omega = \{\Omega_1, \ldots, \Omega_{d-1}\} \). Furthermore, PKG selects a pairing \( e : G_1 \times G_1 \rightarrow G_2 \) where the order of \( G_1 \) and \( G_2 \) is prime \( p > 2^k \), and a generator \( g \) of \( G_1 \). PKG then chooses \( t_1, \ldots, t_l, t_{l+1}, \ldots, t_{l+d-1} \in \mathbb{Z}_p \) randomly and computes \( T_i = g^{t_i} \) where \( 1 \leq i \leq l + d - 1 \). PKG also picks \( \alpha \in \mathbb{Z}_p \) at random and computes \( Y = e(g, g)^{\alpha} \). Finally, PKG selects three cryptographic hash functions: \( H_1 : G_2 \rightarrow \{0,1\}^{|M|} \times \mathbb{Z}_p^* \times G_1, H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_p^* \) and \( H_3 : \{0,1\}^{|M|} \times \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^* \), where \( |M| \) denotes the length of the cipher text. The public parameters PK are published as follows:

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

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

**Key Extract (MK, \( \omega \))**

Given the user with attribute set \( \omega \subseteq u \), the PKG generates the private key for \( \omega \) as follows:

- A \( d - 1 \) degree polynomial \( q(x) \) is picked at random such that \( q(0) = \alpha \).
- Generates a new attribute set \( \hat{\omega} = \omega \cup \Omega \) and computes \( D_i = g^{q(i)} \) for each \( i \in \hat{\omega} \).
- Outputs the private key \( D_i \) for each \( i \in \hat{\omega} \).
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 \(\hat{\omega}_S\) (where \(f\) attributes \(\{i_1, \ldots, i_f\}\) 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 \(X = Y^s = e(g, g)a.s.\) Then computes \(E_i = T_i^s\) for each \(i \in \omega'_S\) and each \(j \in \omega_R\).

- Let \(\omega'_S = \{1, \ldots, d\}\), 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

\[
U_k = \frac{E_k^{r_k}}{\prod_{l \in \omega'_S \cup \omega_R, l \neq k} U_l \cdot E_l} = g^{t_k r_k s} \prod_{l \in \omega'_S \cup \omega_R, l \neq k} U_l \cdot g^{t_1 h_l s} \]

\[h_k = H_2(m, U_k, X, \omega'_S \cup \omega_R, k)\]

\[V = E_k^{r_k + h_k}\]

- Compute \(y = (m||r||V \oplus H_1(X))\)

- Finally, the ciphertext \(CT\) is denoted as \(CT = (y, \omega'_S, \omega_R, U, \{U_l\}_{l=1}^{n_R+d}, \{E_i\}_{i=1}^{d}, \{E_i\}_{i=1}^{n_R})\)

Unsigncryption CT

After receiving the ciphertext \(CT\), \(R\) decrypts the ciphertext as follows.

- For \(CT = (y, \omega'_S, \omega_R, U, \{U_l\}_{l=1}^{n_R+d}, \{E_i\}_{i=1}^{d}, \{E_i\}_{i=1}^{n_R})\), select a subset \(\omega'_R\) with \(d\)-elements subset from attribute set \(\omega_R\).
• Computes

\[ X' = \prod_{j \in \omega_R} e(D_j, E_j)^{\Delta_{j5}(0)} \]

\[ \prod_{j \in \omega_R} e \left( \frac{q(j)}{g^{q(j)j}, g^{q(j)s}} \right)^{\Delta_{j5}(0)} \]

And retrieves \( m', r', V' \) as \( (m \parallel || V') = y \oplus H_1(X') \)

• Computes \( s' = H_3(m', r') \) and verifies whether \( U = g^{s'} \) holds or not.

• For \( l \in \{1, \ldots, n_R + d\} \), computes \( h'_l = H_2(m, U_l, X, \omega'_S \cup \omega_R, l) \) and verifies \( e(g, \prod_{l=1}^{n_R+d} U_l, g^{t:h'_l:s'}) = e(g, V') \) holds or not. If so, \( R \) accepts \( CT \) as the valid ring signcryption on the message \( m' \); \( R \) rejects otherwise.

### 4.3. EXPERIMENTAL RESULTS

This ARSS-Advanced key management scheme provides better performance by reducing storage space requirement and energy consumption. It also reduces Communication overhead by establishing communication with only C-neighbours (Communication-neighbours). As it uses ARSS, the computations are less compare to other public key algorithm like ECC with FO and fuzzy signcryption. Thus ARSS is more suitable to small sensor nodes. In this scheme, if one node is compromised then the probability of compromising other node is zero since each node has its own private key and public key only (Arul Jothi, A, et al., 2016).

In this subsection, a quantitative performance study is presented. Proposed main concern is the energy consumption spent on message computation and transmission. Since the message size is directly related to the energy consumption on message transmissions, and the message size is analyzed.

**Message Size**

In the proposed scheme, the total message size of a cipher text can be computed as follows. The cipher text is the concatenation of attributes, message and time.
Figure 4.2 depicts the relationship between the total message size and the number of users at different security levels. Figure 4.3 shows the functional relationship between the message size and the security level. The curves in Figure 4.2 indicate that the message size is independent of the number of users. From Figure 4.3, it is observed that the message size has a linear relationship with the security level.

![Figure 4.2 MESSAGE SIZE VS. NUMBER OF USERS](image)

**Figure 4.2 MESSAGE SIZE VS. NUMBER OF USERS**
Communication Overhead

From communication aspect, signcryption is the main contributor to the communication overhead, i.e., the communication overhead is mainly associated with the message size of signcryption. The overhead in terms of $q$ is $5|q| + 4$ for signcryption and 1 for designcryption. Figure 4.4 demonstrates the association between the communication overhead and the security level. The communication overhead is increasing along with the security level is noticed.
Figure 4.4 THE COMMUNICATION OVERHEAD VS. SECURITY LEVEL

Energy Consumption on Communications

The energy consumption of Signcryption in ARSS is calculated from the formula $E = U \times I \times T$, where $I$ is set of individual objects, $T$ is code running time. On the other hand, while the public and private key generation speeds have been raised, encrypting and decrypting large volume of data is extremely slow in existing system. The energy cost of fuzzy, sign-then-encryption and ECC with FO are compared to ARSS signencryption energy consumption to demonstrate that ARSS considerably lessens energy consumption.

The results give an extremely compelling argument for ARSS, showing that, in accordance with the assumed battery life, the device using ARSS could execute the number of key exchange operations. Figure 4.5 illustrates the relationship between the Energy consumption on communications and the number of users. ARSS has a less
power computation than other schemes. Nonetheless, when consider the (energy) consumption incurred by both computation and communication; ARSS is still relatively efficient when number of users is large.

![Figure 4.5 ENERGY CONSUMPTION ON COMMUNICATIONS REGARD TO THE NUMBER OF USERS](image)

**Computational Cost**

The cost of a computation is calculated based on the time taken by the message and the cost of the hardware used for the computation. Figure 4.6 depicts the computation cost of ARSS signencryption and the other schemes. One can make the following observations from the figure: First, ARSS signencryption has a less computation cost than other schemes. Nonetheless, when consider the (energy) consumption incurred by both computation and communication; ARSS is still relatively efficient when number of users is large. Moreover, signcryption is an emerging technique, which is under rapid development. Finally, since the BAN controller is supposed to have a less computation capacity, ARSS can be best used to secure communications between the controller and external devices.
4.4. SUMMARY

In this chapter, the proposed Attribute-based Ring Signcryption Scheme (ARSS) is presented in its details. The patient’s dataset is pre-processed using Independent Component Analysis (ICA). Then interoperability is defined by semantics and the semantic interoperability among body area sensor networks is assumed to follow Ant Colony Optimization based Fuzzy Ontology (ACO-FO) technique. The various tests conducted on the proposed ARSS provide the attributes of message confidentiality, authentication, integrity, unforgeability, non-repudiation, public verifiability, and forward secrecy of message confidentiality. Proposed study shows that the ARSS scheme is a light weight and an energy-efficient scheme. And the detailed discussion on privacy and security in health care applications also provided in the forthcoming chapters.