AUTHENTICATION AND OPTIMIZATION PROCESS THROUGH IMAGE KEY MANAGEMENT USING GENETIC ALGORITHM IN BODY AREA NETWORK FOR INTERNET OF THINGS (IoT)

Pradeep Kumar[1], Anand Sharma[2]
[1,2]Mody University of Science and Technology, Lakshmangarh, Sikar-332311, Rajasthan, India

I. INTRODUCTION

Internet of Things (IoT), helping interconnected sensors (i.e., wireless body area network (WBAN), can treat in real time monitoring of patient health status and manage patients and treatment. Likewise IoT will play a helping role in the next-generation healthcare establishment. Although IoT-based patient health status monitoring has become very popular, monitoring patients remotely outside of hospital settings requires augmenting the capabilities of IoT with other resources for health data storage and processing. In this paper, we propose an IoT-based authentication and optimization process through image key management using genetic algorithm in body area network. Recent advances in wireless communications technologies for medical/fitness applications. Particular, it analyzes the following related developments may cover the following topics:

- Status of M2M standardization, market and development in general and specifically for medical/wellness applications
- Development and standardization of the Wireless Body Area Network (WBAN) and Medical Body Area Network (WMBAN), including their markets specifics
- Underlying technologies:
  - Bluetooth and its Medical Profile
  - ZigBee and its Medical Profile
  - Wi-Fi low-power consumption technology
  - Z-Wave, Ant and other technologies
  - Self-powered wireless sensors

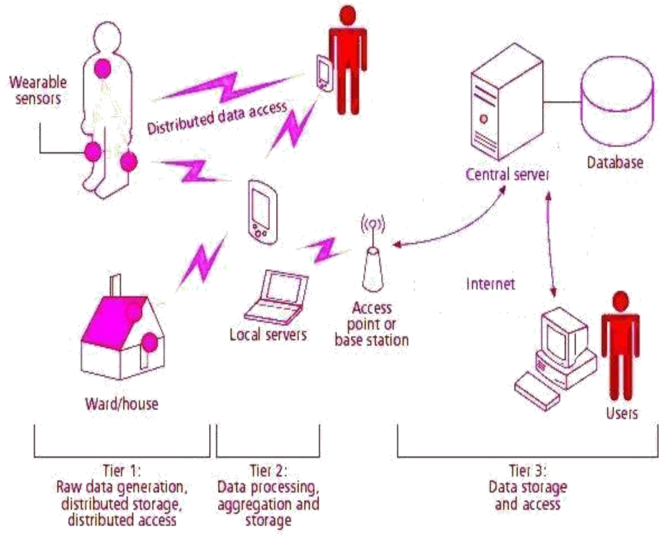
Wearable sensors
Distributed data access
Central server
Database
Internet
Access point or base station
Local servers
Ward/house
Users
Tier 1: Raw data generation, distributed storage, distributed access
Tier 2: Data processing, aggregation and storage
Tier 3: Data storage and access

Figure 1. Basic 3 -Tier structure of BANs

II. RELATED WORKS

This section briefly compare through a table formed chart, the existing related user access control schemes that are currently proposed in resource-constrained wireless sensor networks[3].

We use elliptic curve cryptography (ECC) for our proposed user access control scheme for a wireless body area network. RSA (Rivest et al., 1978) may also be used to authenticate external users and Diffie and Hellman (1976) over DLP (discrete logarithm problem) used to establish shared keys between external users and sensor nodes in the network. However, the evaluation of a 1024-bit modular exponentiation for the DLP of the form 2x (where x is at least 160 bits) requires more than 50 s (Malan et al., 2004; Watro et al., 2004) on both MICA1 and MICA2 motes (Atmel Corporation, 2010).

In Gura et al. (2004), Gura et al. implemented the assembly language for ECC and RSA on the Atmel ATmega 128 processor (Atmel Corporation, 2010), and they showed in their implementation that a 160 bit-point multiplication of ECC required 0.81 s, whereas 1024-bit RSA public and private key operations required 0.43 s and 10.99 s, respectively.

Compared with RSA, ECC can achieve the same level of security with a smaller size key. For example, a 160-bit ECC provides comparable security to a 1024-bit RSA and a 224-bit ECC provides the comparable security of a 2048-bit RSA (Rivest et al., 1992).

It was noted in Carman et al. (2000) that the transmission energy consumption rates in wireless sensor networks are over three orders of magnitude greater than the energy consumption rates for computing. Therefore, the packet size and the number of packets in the transmission play a crucial performance role in designing an access control protocol in sensor networks. If a node is preloaded with the certificate by the base station, then the verifying RSA signature in the certificate takes less time than the ECC signature verification in the certificate because the signature will be generated offline by the base station prior to the deployment of sensor nodes in the target field.

However, compared with a 1024-bit RSA signature (Rivest et al., 1978), an ECC-based signature (Johnson and Menezes, 1999; Liao and Shen, 2006) in the certificate, will only require a 320-bit signature when a 160-bit ECC is used in the proposed scheme. This motivates us to use ECC instead of RSA in our proposed access control scheme so that we can achieve greater energy and bandwidth savings.

Use of symmetric key cryptographic techniques along with ECC to achieve communication and computational efficiency. Wireless body area networks (WBANs) are envisioned to provide health care and patient monitoring applications in the near future. This paper addresses the importance of secure patient data acquisition for different types of users. The proposed authentication scheme consists of multiple phases that involve the users, the medical server (base station) and the sensors.

The users' access is controlled through the use of binary mask value assigned to each user during the registration phase. Exchanged messages among parties are encrypted and signed using elliptic curve cryptography (ECC). The simulation of the proposed solution has been conducted through the use of the widely accepted AVISPA tool to evaluate the method against various known attack scenarios.

The formal and informal security analyses show the protocol's resilience to known security attacks. Wang et al. (2008) split the access control process into a local authentication conducted by a group of sensors physically close to a user and a remote authentication based on the endorsement of the local sensors. They implemented the access control protocol on a test bed of TelosB motes (Atmel Corporation, 2010). Based on ECC, they provided the local authentication. By using certificate-based authentication, the user access was verified by the sensor nodes. He et al. (2011) proposed a distributed privacy preserving access control scheme for WSNs. They identified the characteristics of a single-owner multi-user sensor network and the requirements of a distributed privacy preserving access control. Their scheme was based on a ring signature technique. The user initially registers with a network owner. The network owner then divides all users into groups. The same group has the same access privilege. The network owner maintains a group access list pool that contains the identity and other information of each group, and access control is provided based on the group.

Wen et al. (2011) proposed a user access control scheme for a wireless multimedia sensor network. In this scheme, an authorized user can access the real time multimedia data. Their proposed scheme used Chinese Remainder Theorem-based group rekeying.

s Li et al. (2010) discussed various practical issues required to fulfill the security and privacy requirements in WBANs. They explored the relevant security solutions in sensor networks and

WBANs while analyzing various applications. They proposed an attribute-based encryption for achieving fine-grained access control. This is a one-to-many encryption method where the cipher text is only readable by a group of users that satisfy a certain access policy.

Mahmud and Morogan (2012) proposed an identity-based user authentication and access control protocol based on an identity-based signature (IBS) scheme. They used an ECC based digital signature algorithm (DSA) for signing and verifying a message. At initialization, sensor nodes and users were registered to a base station and group identity and user access rights were also provided by the base station. User revocation was implemented through the expiration of user access time as assigned by the base station at the time of registration. The authenticated user was not allowed to gain access without the proper access rights. Though their scheme was secure against node capture and denial-of-service (DoS) attacks, the password change process was not supported. For new user additions, the base station needed to rebroadcast user parameters such as user ID, group ID and system timestamp, thus incurring more communication overhead in the network.

Wang et al. (2006) proposed an ECC-based user access control scheme. In this scheme, the user must register with the key distribution center (KDC) for access permission prior to authentication. The KDC maintains a user access list pool with the respective user's access privilege. This access privilege consists of user ID, group ID and a user access privilege mask; multiple users within the same group should have the same access privilege. Based on elliptic curve cryptography, the KDC generates the public key, the private key of the user and the access list certificate, based on the user's request. The user requests the sensor node by sending the certificate; the sensor node then selects one random number as a session key. In this scheme, the user authenticates a sensor node and a sensor node also authenticates the user; mutual authentication is thus provided between the user and the sensor node.

Le et al. (2009) proposed an energy-efficient access control scheme based on ECC that improved on Wang et al. (2006). Their scheme was a public key cryptography based access control scheme where the user must accept access permissions from a key distribution center (KDC). The KDC maintains an access control list (ACL) pool and associated user identifications. The user's access privileges are defined in the ACL based on the user's access privilege mask. The public keys between the KDC and the sensor nodes are mutually exchanged during the pre-deployment phase. After registration, the user gains a public and private key. One signed certificate of the access control list is also issued by the KDC and sent to the user. The ssuser must then be authenticated by the sensor node for future communications.

Table: Impact of cryptography in security of WBAN

Security optimization through key management using genetic algorithm in body area network:

Genetic algorithm is a randomized search and optimization technique guided by the principle of natural selection systems. Three basic operators used in Genetic [2] algorithms contain: selection, crossover and mutation. The GA goes through the following cycle: Evaluate, select, mate, and mutate until some stopping criteria are reached. Reproduction and crossover together give genetic algorithms most of their searching power.

A. Selection It is quantitative criterion based on fitness value to choose the chromosomes from population which are going to reproduce.

B. Crossover
In crossover operation two chromosomes are taken and a new is generated by taking some attributes of first chromosome and the rest from second chromosome.[2]

For example, the strings 11001111 to 01101110 could be crossed over after the third locus in each to produce the two offspring 11001110 to 01101111.

Mutation
Mutation is used to maintain genetic diversity from one generation of population to the next. It is similar to biological mutation. GAs involves string-based modifications to the elements of a candidate solution. These include bit-reversal in bit-string GAs. This operator randomly flips some of the bits in a chromosome. For example, the string 01000100 might be mutated in its second position to yield 00000100.

III. PROPOSED METHODOLOGY

In the proposed method GA will be used in key generation process. The crossover and mutation operation is used along with Pseudo random number generators to make the key very complex. For encryption we have proposed AES. Symmetric key algorithm is proposed due to its computation speed and less overhead in key management. The process of generating the key from the Genetic Population has the following steps:
STEP 1: A pseudo random binary sequence is generated with the help of a small image like part of image of ECG sensor image. Means any image can be used as a cryptographic security key. Other key like sound frequency of patient can be used for cryptographic key for algorithm or material of mixture of various metal touches to sensor can be used for cryptographic security key just like biometric way.
STEP 2: The generated string or population is divided in to two halves.
STEP 3: On the selected string crossover operation is performed to achieve good randomness among the key.
STEP 4: After crossover operation the bits of the string are swapped again to permute the bit values.
STEP 5: The same process is iterated two times.
Here the crossover and mutation is done two times to create more complexity and randomness in the key. This key will be then used for encryption process. Here AES will be used for encryption as it is one of the most efficient symmetric key algorithms and its whole security lies in the key used.

IV. CONCLUSION

The BAN is an emerging technology that will alter people’s every day experiences revolutionarily. Privacy and data security in BANs is a significant area, and still there are number of challenges which need to be overcome. In this paper we have surveyed the papers of various authors with respects to authentication in BANs. Through authentication we can ensure that the wireless sensors in a BAN are transmitting data from and to an authenticated user. The research in this field is still in its beginning as of now, but it will draw interest of researches in upcoming years. Hopefully this paper will motivate researchers to do research in this domain and develop novel and practical designs of authenticated BANs and Security optimization through key management using genetic algorithm in body area network.

V. REFERENCE

[1] Pradeep Kumar, Anand Sharma,” AUTHENTICATION PROCESS IN BODY AREA NETWORK AND SECURITY OPTIMIZATION THROUGH KEY MANAGEMENT USING GENETIC ALGORITHM IN BODY AREA NETWORK”, ISSN (Online): 2347 – 4718, International Journal For Technological Research In Engineering Volume 4, Issue 9, May-2017,

[2] Aarti Soni, Suyash Agrawal,” Using Genetic Algorithm for Symmetric key Generation in Image Encryption”, ISSN: 2278 – 1323, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 1, Issue 10, December 2012

[3] Santanu Chatterjee , Ashok Kumar Das *, Jamuna Kanta Sing,” A novel and efficient user access control scheme for wireless body area sensor networks”, Journal of King Saud University Computer and Information Sciences (2014) 26, 181–201