CREATING USER SECURITY GUARANTEES FOR HEALTHCARE APPLICATIONS USING
IOT WEARABLE MEDICAL SENSOR DEVICES

T. MANORANJANI  B. VIJAYA NIRMALA,
PG Scholar, Department of computer science and engineering, R.V.S Educational
Trust's Group of Institutions, Dindigul - 624 005
mailmanoranjani@gmail.com

B. VIJAYA NIRMALA,
Assistant Professor, Department of computer science and engineering, R.V.S Educational
Trust's Group of Institutions, Dindigul - 624 005
bvijayanirmalace@gmail.com

Received 21 Apr 2017; Accepted 03 May 2017

1. ABSTRACT:
Internet of things- IoT came into existence in the year 1999. It is the concept of connecting
objects to the internet using radio frequency identification and other sensor equipment for
a better management and identification of objects. Internet of things is a new technology of
connecting several types of sensor devices to the internet. The sensor devices range from
microphone, camera, speaker, keyboard, displays, Bluetooth, near field communications
(NFC), etc. In this paper we study about Internet of Things in terms of medical field. Body
sensor system and its application in medical field is discussed in this proposed paper. The
main concept is that a patient is monitored thoroughly by using heartbeat sensors,
temperature sensors, ECG, pressure sensors, MEMS (micro electromechanical system) and
oxygen sensors. We have proposed a novel patient-centric framework along with data
access technology to control PHRs that are stored in a semi trusted server. To have a
secured, fine-grained and scalable access to PHR records we use Elliptic curve
cryptographic (ECC) techniques. This helps in encrypting patient’s PHR files. The novel
method is proved to be efficient under standard assumption. The simulation results show
that the proposed technique is efficient in encryption and decryption.

2. INTRODUCTION:
BSN- Body Sensor Network is the most commonly used IoT technique in
healthcare systems. It consists of lightweight and low power wireless
sensor nodes to monitor human functions and the surrounding environment. As we
are aware that BSN nodes are used in hostile situations to collect crucial
information it is most to have strict security gate mechanisms. There are
several wearable devices available in the market for personal fitness, healthcare
and activity awareness. With the advancement in such devices, there are
several applications developed to monitor health remotely when it comes to
recording the information in clinical applications. It is predicted that with such
advancement in wearable devices it is possible for one to have the complete
physical examination done by just
monitoring these inexpensive wearable sensor devices. The sensor will collect the records of your physiological parameters and the data in turn will be stored in the linked health records. So the doctor will not only have the lab/clinical results but also the complete reading of the various physiological recording of the patient. Using the available data and the decision support systems the doctor is capable of making more precise diagnosis and recommend treatment and suggest change in lifestyle, early intervention, etc that could enhance the quality of the patients living style and health.

Security is the major concern when it comes to these systems. Security can be defined in several aspects based on the person notion towards the term. However, we have a general definition for security which states security is similar to safety of a person or a system. Communication in sensor networks like BSN generally work in wireless and hence there is several security threats attached to these systems.

3. Related work

Prosanta Gope et al proposed that the existing hash-based lightweight solutions for RFID system are not applicable. Hence the author proposed an anonymous authentication protocol for RFID system. The comparison study made with the existing methods proved that the proposed method provides a stronger security features but with a higher computational process and large storage requirement. The proposed method can be applied to active and semi-passive tags based RFID system.

A. Wood et al invented a wireless sensor network called the ALARM-NET that is used for monitoring health parameters in residential environments and in assisted living. This system is designed to adapt to the privacy policy enforcement, power management and the individual life patterns of the residents and the collected information is fed into the system. This is achievable using sensor devices to gather the data of the individual along with Dempster-Shafer evidential theory. In order to secure these confidential information the author uses IP and WSN communication along with SRP and SecureComm, a hardware accelerated security suite for Chipcon CC2420-based devices.


The device is designed using a thermoelectric generator in form of a watch. The watch monitors body heat and attains full energy autonomy. Hence the requirement of a battery is eliminated and only a small (super) capacitor is used for energy buffering. With 22 degree Celcius of temperature it can provide more than 100 IW of electrical power. The signal processing happens in the sensor.

Marco Bazzani et al proposed a study on building a solution based on VIRTUS IoT middleware that is different from the current IoT solutions. VIRTUS implements an Instant Messaging protocol (XMPP) that provides real-time authentication and a reliable communication channel for heterogeneous devices. This approach was implemented on a healthcare case study. A cost-savvy remote body movement
monitoring system was developed to capture patient's daily activities. The paper discusses in detail about the features in VIRTUS solution and also gives a comparison with other popular systems.

Chun Tung Chou et al builds a method based on adaptive algorithm. The author developed the theory of adaptive compressive sensing to collect information from WSNs. The purpose of this algorithm is to have projections in iteration to maximize the weightage of information gain per energy expenditure. Since this approach high computation process, a number of heuristic steps are introduced to make it easy. Evaluation of the method is done on both simulation and an outdoor WSN test bed. The results give more accurate solution for a given energy expenditure.

Prosanta Gope et al introduced a secure and a lightweight authentication method that helps in maintaining the user anonymity for roaming services in GLOMONET. One-way hash function and EXCLUSIVE-OR function is implemented in this approach. Though there are previous works for authentication protocols in GLOMONET security, those methods are not to the standard to achieve the desired results against eavesdroppers, communication security, etc. Hence they are open to various attacks and security issues. The proposed method can withstand these attacks and prove to be secure and efficient when compared to other existing authentication schemes available in GLOMONET.

Prosanta Gope et al also proposes another method based on IoT system architecture. It’s an anonymous authentication scheme that has some unique properties like sensor un-traceability, cloning attacks, etc. It is observed that this method based on IoT can be used in several applications based on IoT like Bio-sensor based IoT healthcare system, RFID based IoT system, etc where privacy is of utmost priority.

Tzonelih Hwang et al introduce a real time based Authentication Encryption (AE) environment. In this method the real-time key stream is generated using any of the secure block algorithms like AES hence contributing to a real-time based AE environment. We have two modes of operation involved in the process called cipher feedback (IAR-CFB) and integrity aware real-time based counter (IAR-CTR).

These modes offer confidentiality and integrity of data/information without using any Message Authentication Code (MAC) and non-crypto checksum Cyclic Redundancy Check (CRC). The proposed method is real-time robust and can withstand modification attacks and chosen plain-text attack at the same time. It can also deal with "limited error propagation" that exists in CFB, CTR and OFB, etc

4. The Medical Internet of Things

Electronic medical is developing with the advancement in information technology. Internet of Things has also been a part for this improvement in medical technology. With this emerging new field it gradually turned to be named as medical Internet-of-Things, a technology in which wireless sensors are used in medical equipments and to promote modern medical model.

5. Security and Privacy

IoT helps in capturing living style, well-being, and activity and so on using
wearable devices. Though it seems that these information are not confidential it is highly important to protect and secure these information from third party users. These lifestyle information could reveal various personal information like routine, personal preferences, lifestyle, etc that can be used by vendors to market their products and also worsen the situation with malicious intentions. Data corruption can badly hamper the device and can cause harm to the user.

6. Methodology

Information Sharing

With the huge number of information transaction happening in medical information can form a medical network in which authorized users can access the medical records. It not only contains medical records but other related information like insurance coverage of a patient, medical treatment, prescriptions, etc.

This network can share its network to community hospitals and central hospitals as well to help patients receive regular treatments and medical training.

Patient's condition can be thoroughly monitored using MEMS (micro electromechanical system, heartbeat, temperature sensor, etc using wireless communication. The readings are then transferred from the hardware to the system present in the hospital for the doctors to access the records and suggest the patients accordingly.

7. Body Medical Sensor

Body medical sensors are of two kinds namely: implant sensors and wearable sensors. They consume less power and easy to carry, lightweight, reliable and it has minimal invasive to human body. It is convenient to be worn and easy to be handled. However it is bound to certain limitations where it can serve only on the human body or surface. Its advancement at times makes it complicated where the wireless sensor needs to implanted inside human body and this makes it difficult to be manipulated and used. Wireless capsules like endoscopy helps in transmitting images to outside systems using wireless communication.

Due to the MBAN sensors in RMMP-HI is to focus on human, it is important to consider the mobility of the sensor. It also considers automatic character, portability and integrity for measuring and adaptability.

The existing methods do not serve all the above features and hence a new and novel technique is required. The sensors used in MBAN are EEG/ECG, body temperature, breathing CO, position body local angle, alcohol, weight and some momentum sensors on exercise.

8. Elliptic Curve: Some Definitions

Elliptic curve cryptography (ECC) is the most efficient cryptography method in use. We can discuss about the two important eras in the history of cryptography: classical era and the modern era. In 1977, during the introduction of Diffie-Hellman key and the RSA algorithm, modern cryptography
came into picture. The concept of declaring the key that is used for encryption as public key and the key used for decryption as private key. In 1985, cryptographic algorithm was formed on the basis of esoteric branch of mathematics called elliptic curves. In this proposed paper we use elliptic curve algorithm for encryption and decryption of data received from sensor nodes.

- **Scalar Multiplication**: Let, \( k \) and \( P \) be the given integer that lies on the elliptic curve. Then the elliptic scalar multiplication \( kP \) is the result of adding Point \( P \) to itself \( k \) times.

- **Order**: The order of a point \( P \) is defined as the smallest integer \( r \) where \( rP = 0 \). With \( c \) and \( d \) as integers then \( cP = dP \) iff \( c \equiv d \pmod{r} \).

- **Curve Order**: Curve order is the number of points that lies on the elliptic curve and is denoted as \( \#E \).

**9. Elliptic Curve Equation**

Let's consider an elliptic curve \( F_p \), then the points that satisfy the "curve equation" is:

Here, \( a, b, x \) and \( y \) are within the curve \( F_p \) in other words they are the integers modulo \( p \).

The coefficients \( a \) and \( b \) are called as the characteristic coefficients of the curve and they determine the points that will fall on the curve. The curve coefficients should satisfy the below condition:

**10. Curve cryptosystem parameters**

Now, all the discussed mathematical concepts are to be converted into a cryptosystem and for which there must be sufficient parameters to perform the operation. There are 6 distinct values of \( F_p \) to determine the domain parameters.

1. \( p \): is a prime number that defines the field where the curve operates, \( F_p \). All the points taken into account will have modulo \( p \).

2. \( G \): is called the generator or base point. It is that distinct point on the curve that defines the start of the curve. This is provided as \( G \) or as two points called \( g_x \) and \( g_y \).

3. \( n \): it is order of the curve generator point \( G \). It is the number of different points on the curve that can be manipulated by multiplying a scalar with \( G \). This value is required only for digital signing using ECDSA the operations are congruent modulo \( n \), not \( p \).

4. \( h \): is the cofactor of the curve and is the quotient of the number of curve-points or \( \#E(F_p) \), divided by \( n \).

**11. Elliptic Curve Cryptography**

- ECC is based on the hardness of discrete logarithm problem.

- Consider \( P \) and \( Q \) as any two points on the elliptic curve satisfying the condition, \( kP = Q \).

- Here \( k \) is a scalar and it is complex to find \( k \) when \( P \) and \( Q \) are provided.

- \( k \) is the discrete logarithm of \( Q \) to the base \( P \).

- Point operation is the main operation to be performed.
The scalar k is multiplied with p, k*p in order to achieve another point Q.

12. Elliptic Curve Digital Signature Algorithm Signing

The below algorithm is to perform the signing a message m sent by A using A’s private key d.

1. Compute e=HASH (m), here HASH is a cryptographic hash function where SHA-1
2. Take a random integer k from [1, n-1]
3. Calculate \( r = x_1 \mod n \), where \( (x_1, y_1) = k * G \). If \( r = 0 \), go to step 2
4. Calculate \( s = k - 1(e + dr)(mod \ n) \). If \( s = 0 \), go to step 2
5. The signature is the pair \( (r, s) \)

13. Elliptic Curve Digital Signature Algorithm Verification

In order to authenticate A’s signature from B, B must contain A’s public key Q.

1. \( r \) and \( s \) must be integers in \([1,n-1]\). If this does not satisfy then the signature is invalid.
2. Calculate \( e = \text{HASH} (m) \)
3. Calculate \( w = s - 1 (mod \ n) \)
4. Calculate \( u_1 = ew \ (mod \ n) \) & \( u_2 = rw \ (mod \ n) \)
5. Calculate \( (x_1, y_1) = u_1*G + u_2*Q \) 6. The signature is valid if \( x_1 = r\ (mod \ n) \) than 1. All of these experimental results are in good agreement with the previous analytical and simulation results, and therefore, validate the strong boost ability of the proposed inverter. In this experiment non-optimized input inductor with high winding resistance is used, and IGBT is used even for switch voltage stress of high volts. Use of optimized inductor with less winding resistance and high current rated IGBT will decrease the overall losses and improve the voltage gain of the proposed inverter.

CONCLUSIONS:

Security is being implemented in the four layers of IoT enabled healthcare tools and applications. In this paper, we discuss on the current scenario of IoT in medical field and also about the future health monitoring technologies to immerse in near future. Wearable devices with IoT are the talk of the town and it offers various attractive features for healthcare sector. Security is implemented in IoT using ECC algorithm which is fast and powerful method used for encryption and decryption of data.

REFERENCES:

[7] Prosanta Gope, Tzonelih Hwang, “Untraceable Sensor Movement in Distributed IoT Infrastructure”, 1530-437X (c) 2015 IEEE.