A Novel Secure System for Wireless Medical Sensor Networks using HASBE

Roopashree G.
Dept. of Information Science of Engineering
Sai Vidya Institute of Technology
Bangalore. India

Navya K.
Dept. of Information Science of Engineering
Sai Vidya Institute of Technology
Bangalore. India

Jamuna M.
Dept. of Information Science of Engineering
Sai Vidya Institute of Technology
Bangalore. India

Ranjitha K. V.
Dept. of Information Science of Engineering
Sai Vidya Institute of Technology
Bangalore. India

***Abstract*—Wireless medical sensor networks is an emerging technology in which health related data are collected by biosensors are stored in server. Privacy preserving and security of data plays an important role. This paper focuses on providing efficient flexibility, fine grained access control over health related data and fairly retrieving data from the server in case of medical disputes . We achieve the same by using Hierarchical Attribute Set Based Encryption (HASBE) which is an extension of Cipher text Policy - Attribute Set Based Encryption (CP-ASBE) with user hierarchical structure in the system.**

I. INTRODUCTION

Currently there is rapid development of biosensors and wireless medical sensor networks because of its efficiency of usage in fields like medical field, research field etc. Frequently used for monitoring health at health centres, hospitals, home etc. Health related information are continuously monitored in real time and then updated. These updates are processed and transferred to servers which are maintained centrally specifically storing health related data. These data are used and modified by various users like doctors, authorised person, health committee, patients and their family members. So it can be inferred that this is an efficient way of maintaining health care related data. This helps in emergency treatments and diagnosis of the patients efficiently [1].

In Fig 1. we show the architecture of a wireless medical sensor. Wireless medical sensor consists of patient area network in this network various biosensors like ECG, tilt, motion, Sp02 sensors are deployed and also consists of a controller, this controller can be smartphone, laptop, notebook etc. Biosensors are of two types of wearable biosensors and implantable biosensors. Wearable biosensors are the one which can be attached on to the body surface and implantable biosensors are the one which are implanted inside the body. Wireless medical sensor networks topology can be simple star topology or enhanced multi hop wireless mesh network. Here the biosensors collect the patient health related data and forward these data to controller and the data from controller is forwarded to the medical database or server. The patient related data stored is private information and should be secured, any modification done to this data can put a patient's life at risk. Users who access this data should be authenticated. Since the biosensors are resource limited it is difficult for biosensors to authenticate users. Hence the user authentication

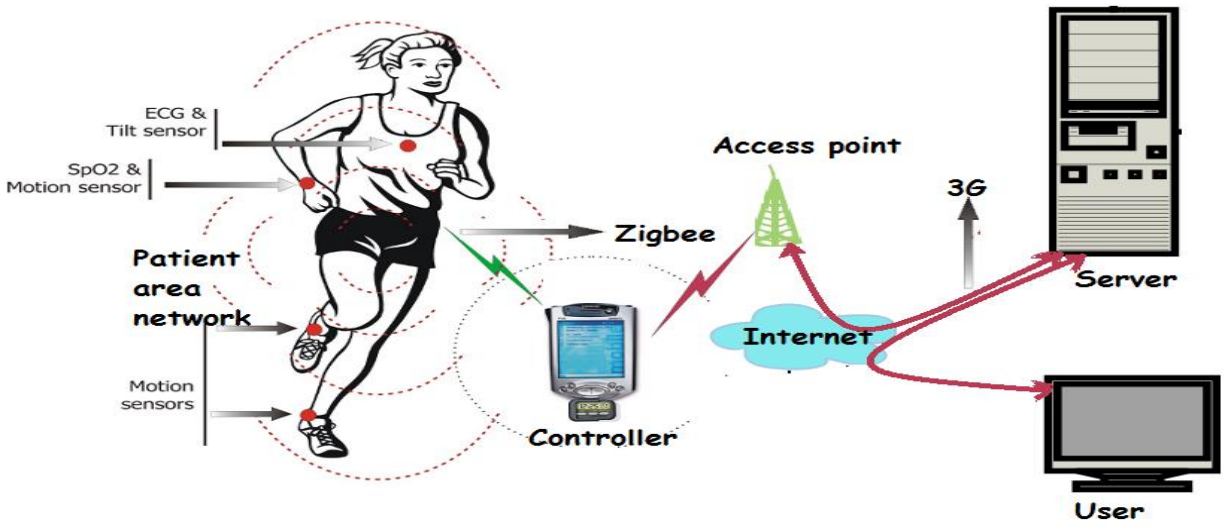

Fig 1. *Architecture of wireless medical sensor network*

should be provided by controller or the medical server. The authentication provided should be in such a way that the data should be protected from adversary and various attacks like Denial-of-Service (DoS) attack.[2].

II. REQUIREMENTS FOR SECURE SYSTEM

In this part of the paper we list many features, characteristics, requirements for an efficient and secure medical sensor networks [1].

A. Fine Grained Access control

Patient related data should be authorized appropriately according to the situation with respect to the system. Since patient data is private and should be secured so that data is not misused by any unauthorized people and access must be denied for such people.

B. Flexibility

According to the requirements of the patient and according to time, location, and other situations of the patient, the access policy should be changed with respect to the patient's data. This is defined by authorized users, patients, healthcare committees. For instance, when necessary another doctor who is not authenticated should be allowed to access the patient's data. If not in critical situations if treatment is delayed patient's health is at risk which can lead to death of the patient.

C. Confidentiality

Disclosure of patient's related information like blood pressure, blood glucose level, heartrate, can be mishandled which in turn puts patient's life at risk. Information stored should not be affected and must be hidden from various attacks and no data should be disclosed due to attack.

D. Scalability

The system proposed should work efficiently even for large number of users, large data, networks of large range. Thus system should be strongly built and should not crash in any situation.

E. Data Integrity

As there is lot of transferring of data in health care network, a patient information is invigorating in health care network if the patient information is modified at any time it would lead to bad situation in patient's life. Therefore data integrity should be maintained.

III. EXISTING SYSTEM

In the existing system various cryptographic methods and attribute based encryption methods are used. Some of these methods result in heavy computational overhead due to key distribution and inefficient data management which results in inefficient system [3].

A. Identitiy based encryption

In this method arbitrary key is used for data encryption and decryption, for authorization purpose key is mapped by a key.

B. Hierarchial identity based encryption

It is a form of single Identity based encryption. This method explains the concept of security. In this method only one private key is generator which in distributes private keys to every other user. [3]There exists a 2 level HIBE scheme which has root private key generator, domain private key generator and users and each of which is associated with Primitive ID. Hence this encryption method allows hierarchy of certificate authorities and users in their respective domains.

C. Key policy attribute based encryption

1) The Initial stage:

In this method [3] algorithm takes inputs like security parameters k which returns a key called public key and master secret key and for encryption purpose the senders use public key. Secret keys for users are generated using master key which is known only to the authorized people.

2) Encryption stage:

In this stage encryption takes input as message M the public key PK and set of attributes and produces output which is cipher text [4].

3) Key generation stage:

For generating the key, master key and access structure is the input, and for the user to decrypt a message it should match with the set of attributes and the output is SK secret key T[5].

4) Decryption stage:

The input for this stage is Secret key SK of user for access structure T and cipher text T which is then encrypted under attribute set. If and only if attribute set meets the conditions of users access structure T and produces output message M.

D. Cipher Text Policy Attribute based encryption

This type of encryption is used to encrypt the data which is to be kept confidential even if it's stored in an untrusted storage server.[3] A primary key is associated with various attributes. In another scenario if a person encrypts a message of this system they would be asked to specify the access structure associated with attributes. If attributes of the user passes through access structure of cipher text then only cipher text can be decrypted. Access trees describe the access structure of the system at mathematical level. Every user of the system should have proper authentication and authorization to access the data.

IV. PROPOSED SYSTEM

We propose a hierarchical attribute set based encryption scheme here for data access.

A. Modules involved in this system are

1) Data owner module: In this system data owner is patient where data is generated by sensors attached in PAN (Patient Area Network). The controller encrypts the data using the public key generated during system set up, based on depth of the key structure in the architecture. Data owner has the access privilege to the encrypted data. Here the depth involves 3 levels: Hospital admin, Doctor, Patient.

*2) Data access Module:*Here the doctor must be registered before he can login to see the user's data. Server generates private key by using master key. It also generates public key for the doctor. Hospital management gives authority to access patient record for a particular doctor.

When a doctor is from other hospital then authority is given to access patient record for a particular session, at first he has to request permission from hospital management to get access for the patient's record and then doctor is provided with a key which expires after a session time-out.

3) Server module: Hospital authority is associated with an unique ID and attributes. They select a bi-linear group of random numbers with depth of key structure. Public key and master key is generated. Patient data is generated at PAN and sent to controller. The controller encrypts the data by public key and Master key and a cipher text is generated. When doctor has to access patient record from server, he has to register to server and it provides private key by using public key and master key. Then the doctor requests for a patient record with provided Patient ID, then the server sends encrypted data. The doctor by using private key decrypts the data.

B. System operations involvoed in this scheme are

1) System Setup : During the system set up, the hospital authority selects a bilinear group, depth of the key structure and some random numbers. Here Public Key (PK) and Master Secret Key (MK) is generated with several exponentiation operations.

2) Top level Hospital authority/ User Grant : A hospital authority is associated with an unique ID and a recursive attribute set. A doctor is linked with certain attributes, which is the set of higher level domain authority here recreation of the key (PK) is done.

3) New File Creation : In this operation, the patient record data file is encrypted using the public key (PK) and master key (MK) ,a cipher text (C) is generated.

4) Private Key(P) : Private key (P) is generated by using master key. Public key (PK) is generated for the doctor.

5) User Revocation : Hospital authority maintains some information of doctor's keys and assigns new value for expiration time to a doctor's key. When re-encrypting files, the patient just needs two exponentiations for cipher text components associated with Expiration-time as the attribute.

6) File Access : In this method, the decryption of encrypted data files is done. Using (C) and (P) as input we generate message (M).

7) File Deletion : This operation is done at top level hospital management when files are to be deleted or stored at backend of the server.

Fair record retrieval is achieved in situation like medical disputes and accidents using HASBE. In such situation Top level Hospital authority takes all the decisions to solve the problem.

V. CONCLUSION

In the paper we have proposed a secure scheme in medical sensor networks to achieve efficient flexibility, fine grained access control by employing Hierarchical attribute set based encryption which is more efficient and advantageous over existing schemes.

VI. REFERENCES

[1] Daojing He, Sammy Chan, Shaohua Tang, Chun Chen, Jiajun Bu and Pingxin Zhang,"A Novel and Lightweight System to Secure Wireless Medical Sensor Networks" Biomedical and Health Informatics, IEEE Journal of (Volume:18 , Issue: 1)pp 316-326,January 2014

[2] D. He, C. Chen, S. Chan, and J. Bu, "DiCode: DoS-resistant and distributed code dissemination in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946-1956, May 2012.

[3] Poonam Joshi, Yash Shah, Harsh Sanghani, Sharvari Vartak "File Sharing Application Using HASBE Scheme", International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869, Volume-3, Issue-1, January 2015.

[4] S. Gokuldev, S.Leelavathi," HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013.

[5] Sanchal Ramteke, Purva modi, Apurva Raghojiwar, Vijaya Karad, Prof.P.D. Kale," A Hierarchical Attribute-Based Encryption in Cloud Computing "May 2014.