PRESERVATION OF PRIVACYAND SECURTITY FOR INFORMATION IN WIRELESS MEDICAL SENSOR NETWORKS

A.Shirisha[1], Sana Mateen[2]

ABSTRACT

Wireless Sensor Networks (WSN) is an emerging technology that has the potential to transform the way of human life. Healthcare applications are considered promising fields for Wireless Medical Sensor Network, where patient's health can be monitored using Medical Sensors. Wireless Medical Sensor Networks (WMSNs) are the key enabling technology in healthcare applications that allows the data of a patient's vital body parameters to be collected by wearable biosensors. Current WMSN healthcare research trends focus on patient reliable communication, patient mobility and energy-efficient routing. Security and Privacy protection of the collected data is a major unsolved issue. To overcome these issues, symmetric algorithms and attribute based encryptions techniques are adopted, which secures the data transmission and access control system for MSNs.

Keywords- Access Control, Data Transmission, Medical Sensor Networks, Privacy, Security.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a self-configure network of small sensor nodes, where the sensor nodes can communicate among themselves using radio signals, and these sensor nodes can sense, monitor and understand the physical environment. It consists of spatially distributed sensors to monitor physical or environmental conditions and to pass the data through the network to a destination location. The bi-directional modern networks enable to control the activity of the sensors. The development of the wireless sensor networks was motivated by military applications such as battlefield surveillance and is also used in many industrial and consumer applications like industrial process monitoring and control, machine health monitoring, etc [3]. The WSN is built of "nodes", where one or more sensor is connected to each node. Each sensor node consist of several parts, like radio transceiver with an internal antenna to an external antenna, microcontroller, electronic circuit for interfacing with the sensors and an energy source like a battery.

II. WIRELESS MEDICAL SENSOR NETWORKS

WSNs deployed at a large scale in a distributed manner, and their data rates differs based on their applications, where the Wireless Medical Sensor Networks have direct human involvement are deployed on a small scale must support mobility (a patient can carry the devices), and WMSNs requires high data rates with reliable communication. Physiological conditions of patients are closely monitored by deploying Wireless medical sensor motes.

These medical sensors are used to sense the patient's vital body parameters and transmit the sensed data in a timely fashion to some remote location without human involvement. Using these medical sensor readings the doctor can get the details of a patient's health status. The patient's vital body parameters include heart beats, body temperature, blood pressure, sugar level, pulse rate [3].

WMSNs carry the quality of care across wide variety of healthcare applications. In addition, other applications that also benefit from WMSNs include sports-person health status monitoring and patients self-care. Several research groups and projects have started to develop health monitoring using wireless sensor networks.

Wireless Medical healthcare application offers a number of challenges, like, reliable transmission of data, secured data transmission, nodes mobility, detection of event delivery of data in time, power management, etc. Deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable. For instance, the patient's physiological vital signals are very sensitive so the leakage of the patient's diseased data could makes the patient embarrassed. Sometimes revealing disease information can make it impossible for them to obtain insurance protection and also result in a person losing their job [6].

Further, wireless medical sensor networks cover a broad range of healthcare applications, such as physiological data monitoring, activity monitoring in health-clubs, location tracking for athlete are the broad range of healthcare applications. WMSNs share individual data with physicians and insurance companies. Thus unauthorized collection and use of patient data by adversaries can cause life-threatening risks to the patient and make the patient's private matters publically available. For example, In[16] a simple scenario, a patient's body sensors transmit the body data to a nurse, the patient's privacy is breached when some attacker is eaves dropping. Later that attacker can post the patient data on social site and pose risks to the patient's privacy.

Indeed wireless healthcare can offer many advantages to patient monitoring, but the medical health data of an individual are highly vulnerable to various threats, so security and privacy become some of the big concerns for healthcare applications, when it comes to adopting wireless technology. A healthcare provider is subjected to strict civil and criminal penalties if Health Insurance Portability and Accountability Act (HIPAA) rules are not followed properly [4]. Thus the security and privacy of the sensed data is the major concern in healthcare applications**.**

III. LITERATURE SURVEY

Cryptographic algorithms are either symmetric algorithms which uses symmetric keys (secret keys), or asymmetric algorithms which uses asymmetric keys (public and private keys). In [12], both the algorithms have the following advantages and disadvantages.

3.1 Symmetric Algorithm

Advantage

- More secured
- Requires less space
- Same key for both encryption and decryption

Disadvantage

- Key distribution problem

3.2 Asymmetric Algorithm

Advantage

- Solves key distribution problem
- Securely exchange message

Disadvantage

- High computation time is required
- Requires more space

In [2], a lightweight and secure system for MSNs is proposed to provide a safe transmission of sensed data, the system employs hash-chain based mechanism and proxy-protected signature technique to achieve secure transmission of the sensed data and access control. The basic idea is as follows, the user registers to the network server, and the registered user is allowed to issue commands to access the collected PHI or control the biosensors according to their access privilege. To achieve this proxy-protected signature by warrant (PSW) is introduced into the system. An original signer and proxy signer are the two important participants. The original signer gives the proxy signer a warrant, and the proxy signer generates a proxy signature using the proxy key given by the original signer. The verifier validate proxy signatures with the public key of the original signer and also verifies the proxy key of the original signer. This prevents the unauthorized access and limits power consumption of sensor nodes.

In [1], in order to evaluate the behaviour of each node a secured multicast strategy is proposed; in this only trustworthy nodes are allowed to participate in communications so that the misbehaviour of malicious nodes is prevented. Trust is defined as “during the interaction with other node, how a node is trustworthy, secure, or reliable”. The criterion for choosing nodes for multicast technique is based on the trust value. By evaluating the node’s trust enables the trust system to track the behaviour of all the nodes, security evaluations feedback of other nodes are recorded, and corresponding reactions are made to the tracked behaviour. By this correct nodes can be chosen to participate in the communication and malicious nodes can be avoided.

In [9], the focus is on three secure sharing use cases; proof of ownership, where the data owner must prove the ownership of the data tracking, where the data owner must trace unauthorized sharing of the bio signal data and content authentication, and the data owner must prove whether the bio-signal data has been maliciously altered. To address these use cases, a robust watermarking technique is developed to embed security information into bio-signal data in order to protect the semantic fidelity of the data, the bio-signal waveforms are imperceptibly altered, and the watermark is not easily recovered, corrupted or spoofed by malicious attackers. Thus the integrity of the bio-signal is preserved by Water Marking and the data owners can easily track the usage of their data.

In [6], a secure and privacy-preserving opportunistic computing framework, called SPOC, is proposed for medical Healthcare emergency. Using SPOC smart phone resources including computing power and energy can be opportunistically gathered to process the computing-intensive personal health information (PHI) during m-Healthcare emergency with minimal privacy disclosure. To leverage the PHI privacy disclosure and the high reliability of PHI process and transmission in m-Healthcare emergency, an efficient user-centric privacy access control in SPOC, which is based on an attribute-based access control and privacy-preserving scalar product computation (PPSPC) technique, allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data.

In [10], a novel key agreement scheme that allows neighbouring nodes in BANs to share a common key generated by electrocardiogram (ECG) signals. The improved Jules Sudan (IJS) algorithm is proposed to set up the key agreement for the message authentication. The ECG-IJS key agreement secures data communications over BANs without any key distribution overheads. In this the simulation and experimental results are presented, which demonstrate that the ECG-IJS scheme can achieve better security performance in terms of performance metrics such as false acceptance rate (FAR) and false rejection rate (FRR) than other existing approaches. Based on the IJS algorithm described earlier, propose an ECG-IJS key agreement to secure data communication in BANs. Thus privacy and authentication are preserved in energy efficient way.

In [4], stochastic data traffic models for medical wireless sensor networks (WSN's) are presented that represent the traffic generated by a single WSN node monitoring body temperature and electrocardiogram (ECG) data. The models are based on public domain medical signal databases. For energy conservation, it is likely that some medical WSN nodes will employ source coding to reduce the amount of data that must be transmitted. The first scenario to consider is the straightforward case where the node simply transmits the raw 11 bit ECG data at the 360 Hz sampling rate. The second scenario is the more complex case where the node employs source coding. The work considers lossy compression due to the very high compression ratios possible with lossy techniques.

IV. EXISTING SYSTEM

A lightweight and secure system, for MSNs employs hash-chain based key updating mechanism and proxy-protected signature technique to achieve efficient secure transmission and access control. The basic idea of the existing system is given as follows. After a user registers to the network server, the user is allowed to issue commands to access the collected PHI or control the biosensors according to their privilege. To achieve this proxy-protected signature by warrant (PSW) is introduced into the system.

There are two kinds of participants, i.e., an original signer and proxy signers. The proxy signer registers in the network server, which is the original signer generates the proxy keys before the proxy server enters the MSN. Now after obtaining the keys the proxy user becomes the authorized user and can generate commands using those keys to get access to the data [2]. The validity of the key is verified by the network server so that it can prevent unauthorized users.

The system involves four phases. The system initialization phase is performed by the network server to set up an MSN. User joining phase is involved before a user can issue commands to the MSN. During the regular use phase, the data from each biosensor node are securely transmitted to the network server via the controller.

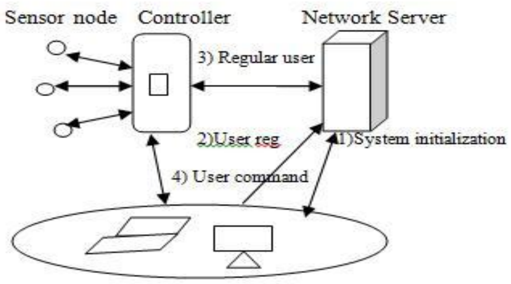


Figure 4.1 Flow of Security Information

In the user command phase, if a network user has a new command, he/she will need to construct the command and the proxy signature and then send them to the network server (or the controller of a target PAN). If the command verification passes, the network server (or the controller of a target PAN) responds to the user's command. The controller and node side programs are executed on the resource limited sensor nodes, and the network server programs are executed on the PC. Here AES encryption algorithm is used to encrypt the sensed data before transmission. Usually data block of 128 bits is encrypted using three different keys such as 128-bits, 192-bits and 256-bits of key length. MD5 is a one way hash function, where the hash value should match the received data correctly and is used to compress the data size in order to minimize the energy consumption.

V. PROPOSED SYSTEM

Even though AES is used for encrypting the data is less secured and requires more computation time.

In [2], the sensed data is transmitted individually and it requires more energy and data fusion is not done.

The enhancement of security and privacy of the sensed data can be achieved in the proposed system by implementing various symmetric encryption algorithms which are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms.

In Fig. 5.1, consist of various symmetric key algorithms such as mentioned in the below.

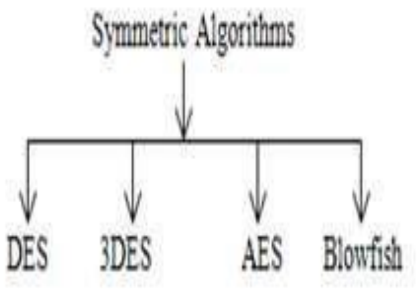


Fig 5.1:Symmetric Key Encryption

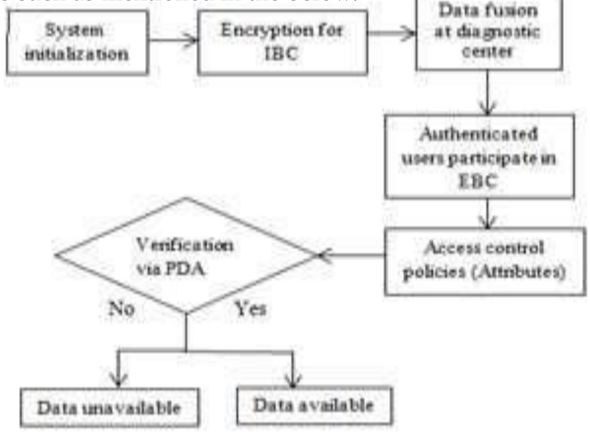

System initialization
Encryption for IBC
Data fusion at diagnostic center
Authenticated users participate in EBC
Access control policies (Attributes)
Verification via PDA
No
Yes
Data unavailable
Data available

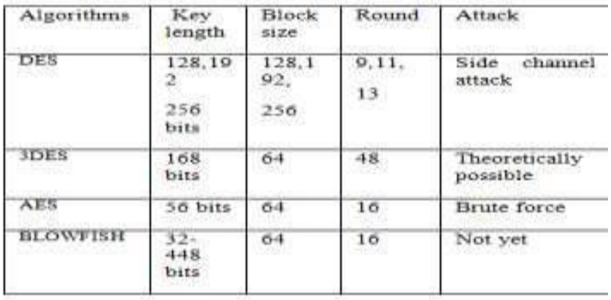
Fig 5.2: Architecture of Proposed System Algorithm

Symmetric algorithms like DES, 3DES, AES, Blowfish can be implemented to compare the different computation time take by various algorithms.

The above Figure 5.2 is the architecture of the proposed system. Since medical data is of a great privacy concern proper security mechanisms should be adopted while transmitting the data.

In the proposed work, the system is initialized by deploying the bio-sensors, and these sensors collect the vital body parameters like heartbeat, sugar level, blood pressure, etc. Various algorithms like DES, 3DES and Blowfish can be implemented and the best is chosen based upon their computation time. The collected data is encrypted using the best symmetric key encryption algorithm, In [11] blowfish algorithm which uses variable number of bits ranging from 32 to 448 bits encrypts the data 16 times than the other encryption algorithms and is said to be the fastest encryption algorithm, and is transmitted to the diagnostic center through controller via internet. Table a, provides the comparative study of different symmetric algorithms used for encryption.

Table a: Comparison of Symmetric Key Algorithms



Algorithms	Key length	Block size	Round	Attack
DES	128,192 256 bits	128,192, 256	9,11, 13	Side channel attack
3DES	168 bits	64	48	Theoretically possible
AES	56 bits	64	16	Brute force
BLOWFISH	32-448 bits	64	16	Not yet

The comparitive study shows that blowfish is the best among the implemeted algorithms as it is not exposed to any attack.

The type of communication between the sensor node and the controller is called as Intra Body Communication (IBC). Then data fusion will be done in the diagnostic center where several data is fused into one single packet in order to reduce the network traffic and transmission time. Omnibus data fusion model can be adopted where the sensed data is fused using either soft or hard data fusion and the sensor manager is used to manage the fusion. The fused data sent from controller to the diagnostic center and access control policies are adopted with the use of Attribute-based Encryption Signature. The Attribute-based Encryption algorithm consist of four steps:

1. Setup (λ, U) → (PK, MK)

The setup algorithm takes as input a security parameter λ and a universe description U. PK which is the public parameters and the master secret key MK is the output.

2. Encrypt (PK, M, S) → CT

The public parameters PK is given as input to the encryption algorithm, a message M and a set of attributes S and outputs a ciphertext CT associated with the attribute set.

3. KeyGen (MK, A) → SK

The key generation algorithm takes as input the master secret key MK and an access structure A and outputs a private key SK associated with the attributes.

4. Decrypt (SK, CT) → M

A private key SK associated with access structure A is given as input to the decryption algorithm and a cipher text CT associated with attribute set S and outputs a message M.

The communication between the controller and diagnostic center is called Extra Body Communication (EBC). The authenticated users can participate in EBC. The authentication is achieved through the email id, which is the Secret Key(SK) generated by the key generation algorithm. Strict access control policies can be adopted at the diagnostic center based on the user's attributes, i.e. doctors can gain access to the entire medical data, the technicians can access only few data of the patients, and the patients have very limited access to others data. The verification can be done via PDA at the center and the data is available only to the authorized user and unauthorized users cannot access the data.

VI. CONCLUSION

Healthcare applications are considered promising fields for WMSNs, where patients can be monitored. Transmission in wireless environment needs safety and privacy of medical data. The disadvantage of public-key algorithm is that they are more computationally intensive than symmetric algorithms, this is not significant for a short text message , hence Symmetric cryptographic algorithms can be used to provide security while transmitting the sensed data and access control policies are adopted by attribute based signature technique. Hence the privacy and integrity of data can be perceived during the transmission in wireless environment.

REFERENCES

[1] AzzedineBoukerche, and YonglinRen," A Secure Mobile Healthcare System using Trust-Based Multicast Scheme",IEEE Journal On Selected Areas In Communications, Vol. 27, No. 4, May 2009,316-325.

[2] Daojing He, Sammy Chan, Member, IEEE, and Shaohua Tang, Member, IEEE," A Novel and Lightweight System to Secure Wireless Medical Sensor Networks", IEEE Journal Of Biomedical And Health Informatics, Vol. 18, No. 1, January 2014,23-32.

[3] Denis Trcek And Andrej Brodnik, University Of Ljubljana," Hard And Soft Security Provisioning for Computationally Weak Pervasive Computing Systems In E-Health", IEEE Wireless Communications August 2013,45-53.

[4] Geoffrey G. Messier and Ivars G. Finvers," Traffic Models for Medical Wireless Sensor Networks", IEEE Communications Letters, Vol. 11, No. 1, January 2007,21-30.

[5] Oscar Garcia-Morchon, Thomas Falck, Tobias Heer, Klaus Wehrle,"Security for Pervasive Medical Sensor Networks", Vol.12, No.2, June 5th 2009,126-134.

[6] Rongxing Lu, Member, IEEE, Xiaodong Lin, Member, IEEE, and Xuemin (Sherman) Shen, Fellow, IEEE," SPOC: A Secure and Privacy-preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency", IEEE Transactions On Parallel And Distributed Systems, Vol. 12, No. 2, May 2012,452-461.

[7] Shu-Di Bao, Student Member, IEEE, Carmen C. Y. Poon, Student Member, IEEE, Yuan-Ting Zhang, Fellow, IEEE, and Lian-FengShen," Using the Timing Information of Heartbeats as an Entity Identifier to Secure Body Sensor Network", IEEE Transactions On Information Technology In Biomedicine, Vol. 12, No. 6, November 2008,155-162.

[8] S. Moller, T. Newea, S. Lochmannb," Prototype of a secure wireless patient monitoring system for the medical Community", 2011 Elsevier B.V. All rights reserved.

[9] VishwaGoudar and MiodragPotkonjak," A Robust Watermarking Technique for Secure Sharing of BASN Generated Medical Data", 2014 IEEE International Conference on Distributed Computing in Sensor Systems.

[10] Zhaoyang Zhang, Honggang Wang, Athanasios V. Vasilakos, and Hua Fang," ECG- Cryptography and Authentication in Body Area Networks", IEEE Transactions On Information Technology In Biomedicine, Vol. 16, No. 6, November 2012,321-332.

[11] E.surya,C.Divya, " A Survey on Symmetri Key Encryption Algorithms", International Journal of Computer Science & Communication Networks,Vol 2(4), 475-477.

[12] Tingyuan Nie, and Teng Zhang ,"A Study of DES and Blowfish Encryption Algorithm", IEEE, 2009.

[13] Singh, S preet, and Maini, Raman "Comparison of Data Encryption Algorithms", International Journal of Computer science and Communication,vol.2,No.1,January-June 2011,pp.125-127.A.

14] Behrouz A.Forouzan", Cryptography and Network Security", 2nd Ed, Tata Mcgraw hill.

[15] Himani Agrawal and Monisha Sharma,"Implementation and analysis of various Symmetric Cryptosystems", Indian Journal of science and Technology vol.3,No.12,December 2012.

[16] Pardeep Kumar and Hoon-Jae Lee," Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey", Published: 22 December 2011, Sensors 2012, 12, 55-91.