An Efficient Access Control Scheme Using Elliptic Curve Cryptography in Wireless Medical Sensor Data

Gayathri.S[1], Vanaja.B[2]

[1] *PG scholar,Department of computer science and engineering , Sri Vidya College Of Engineering & Technology, Tamilnadu, India*
[2] *Assistant professor, Department Of Information Technology, , Sri Vidya College Of Engineering & Technology , Tamilnadu, India*

ABSTRACT

Wireless sensor network is an important role in healthcare IT. It is used to reduce the healthcare cost and improve the quality of care. The critical requirements in healthcare is privacy of data confidentiality and Patient data privacy. This needs a secure and light weight user authentication and access control .Due to the dynamic network topology the symmetric key based access control is not suitable for WSNs. In this paper we propose a Mutual Authentication and Access control Scheme based on Elliptic Curve Cryptography. This is a secure light weight public key based security scheme. For using this technique the medical data is not exposed to an unauthorized person. The benefits of this techniques are requires lesser memory and more scalable. Additionally it is much more lightweight than other public key based schemes. Access Control is one of the technique of security that can be used to control who or what can view or use resources.

Keyword : - *Elliptic curve cryptography, User Authentication, Access control, Wireless Sensor Networks.*

1. INTRODUCTION

The Wireless sensor networks are combination of sensing, computation and communication into single small devices. This networks are deploying a large number of small nodes and configure themselves. This is used for real time tracking, to monitoring of environmental conditions, to ubiquitous computing environments, to monitoring the health of structures. The applications of wireless sensor networks are monitor remote environments for low frequency data trends. The large number of sensor node devices spread over a large field. It is a combination of Wireless sensing and Data networking. For Example, a Chemical plant could be easily monitored for cracks by hundreds of sensors that spontaneously form a wireless interconnection network and suddenly report the detection of any chemical cracks. Driven by technology improvement in medical sensors and low-power networked systems we have testified in fresh years the emergence of wireless sensor networks in healthcare.these wireless networks implementing the promise of strongly updating and expanding the quality of care throughout a wide variety of settings and for different sections of the population Wireless Sensor Network (WSN) is a self-build network of tiny sensor nodes, where the sensor nodes can interact among themselves using radio signals, and these sensor nodes can sense, monitor and understand the physical environment. That contains 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 up-to-date networks implement to restrain the proceeding of the sensors. The growth 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. The WSN is connection of "nodes", where more number of sensors are connected to each node. The challenges of sensor networks are (i) Low computational power (ii) Poor communication bandwidth (iii) Radio congestion and (iv) Limited energy budget[12].

The Mobile medical is one of the transcend of healthcare technology. A remote wireless patient monitoring system that exploits the modern technologies in clinical sensor and actuator systems and large-area wireless communication networks to donate best healthcare services in a large-range of displays. Mobi Care contains three prominent structuring modules: a body sensor network (BSN) containing the wearable sensors and sensors with wireless inter-connections. A BSN Manager that connects the BSN to an large-area transmission interface using large-area cellular wireless link and back-end infrastructure tolerate at healthcare providers to appliance needful healthcare events. MobiCare processes a large-range of programmable and redesigned services with capable remote monitoring for mobile patient care. This will help to develop acceptable systems that will meet the legislated needs of the organizations wishing to pursue the application of this technology with respect to medical care. Privacy of medical information is a very important requirement as the information has a large potential for abuse.

2. RELATED WORK

There is an early consumption stage between each medical sensor and each data server. For each medical sensor, three secret keys are pre-deployed and pre-shared with three data servers, respectively. Each secret key is used to create a secure channel between the sensor and one data server. In addition, one more secret key is pre-deployed in each sensor in order to generate random numbers. Note that different medical sensors are deployed with different secret keys. When a medical sensor sends a sensitive numerical patient data(e.g., temperature reading) to the distributed patient database, to prevent any data server from understanding the patient data and revealing the patient privacy the medical sensor splits the patient data into three integers .

$$\alpha+\beta+\gamma=\rho \quad (1)$$

2.1 Data collection protocol

The medical sensor sends a sequence of sensitive numerical patient data to the three data servers, it firstly generates a sequence of random numbers with SHA-3

$$\gamma_i = \rho_i - \alpha_i - \beta_i \quad (2)$$

2.2 Access control protocol

If any user can get access to the patient data then the user generates a public and private key. To get access to the patient data, the user sends a request including the patient's identity, the data attribute, the signature of the user on the query, and the certificate of the user to the three data servers through the three secure channels. We use the secure channels for the user to submit his queries because the patient's personal information in the queries needs to be protected against outside attackers.

$$\rho = \text{Decrypt}(C1C2C3,sk)=\alpha+\beta+\gamma \quad (3)$$

3. PROBLEM STATEMENT

The development of a wireless healthcare application offers many novel challenges such as consistent data broadcast, node mobility, support and fast event detection, timely liberation of data, power management, node computation and middleware. Further however, deploying new technologies in healthcare applications without considering security often makes patient privacy vulnerable. For instance, the patient's physiological vital signals are very responsive (i.e., if a patient has some awkward illness).So any outflow of individual illness data could makes him/her mortified. In fact sometimes illuminating disease information can result in a person trailing his make it unfeasible for him/her to attain insurance guard.

3.1 Security and Privacy Issues

The security issues in wireless healthcare applications, it is worthwhile to assume the scale of deployment of healthcare applications using WMSNs. In this regards, we have considered three wireless healthcare scenarios, namely, a nursing home, in-home monitoring, and in-hospital monitoring. WMSNs certainly improve patient's quality-of-care without disturbing their comfort. The medical sensor senses patient sensitive body data and transmits it over the wireless channels which are more susceptible than wired networks. Thus, patient sensitive physiological variables must remain secure and private from security threats, so this sub-section discusses the possible security

threats that would be harmful for the wireless healthcare. The medical sensor senses patient sensitive body data and transmits it over the wireless channels which are more susceptible than wired networks. Thus, patient sensitive physiological variables must remain secure and private from security threats, so the possible security threats that would be harmful for the wireless healthcare success.

As wireless healthcare applications are not limited to monitoring the patient's physiological data, but they also include emergency management, healthcare data access, electronic health records, Further, individuals share their data with physicians insurance companies and health-coaches or with family So there is value in addressing the privacy issues that are ethical from a social point of view. We adopt the privacy definition from National Committee for Vital and Health Statistics, which is consultative board of the United States Department of Health and Human Services. "Health information privacy is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. To maintain privacy, patients should have the rights to determine which data should be collected, used or disclosed. Any unauthorized collection or leakage of patient data could harm the patient. For example, an unauthorized person may use the patient data for their personal benefit, such as for medical fraud, fraudulent insurance claims, and sometimes this may even pose life-threatening risks. As the medical data is very sensitive by the European Union Data Protection Directive. In wireless healthcare applications, huge amount of health and life-style data are gathered that need close attention to who controls it, what is gathered, who has rights to access it and where/how/whether that data is stored or not .

In a patient medical record system, insiders may modify the medical records intentionally. For example, suppose an insider wrongly alters the patient's medical data, such as, illness conditions, severe allergies, and specifically blood type, all of which pose life-threatening risks.The privacy issues in a pervasive healthcare monitoring. The authors identified a few privacy issues in pervasive healthcare, such as, misuse of medical information, leakage of prescriptions, eavesdropping on medical data, and social implications for the patient**.**

4. PROPOSED METHOD

The first step is to establish key between two nodes. To meet scalability requirements for a large number of sensor nodes, we propose a public key management scheme based on Elliptic Curve Cryptography (ECC). Compared to symmetric key cryptography, ECC is more scalable, requires lesser memory for storing keys, introduces low communication overhead, and is easy to deploy. The main contribution of this paper is securely distributing the patient data in multiple data servers and employing the Paillier and ElGamal cryptosystems to perform statistic analysis on the patient data without compromising the patients' privacy. The primary purpose of encryption is to protect the confidentiality of digital data stored.

4.1 Elliptic curve cryptography

ECC was introduced by Victor Miller and Neal Koblitz in 1985.For DSA, RSA we need larger key length.ECC requires significantly smaller key size with same level of security. Benefits of having smaller key sizes : faster computations, need less storage space. ECC ideal for constrained environments: Pagers , PDAs, Cellular Phones , Smart Cards. ECC is an asymmetric cryptosystem based on the elliptic curve discrete log problem.

4.1.1 ECC Key Generation

A public key $Q = (x_Q, y_Q)$ associated with a domain parameter (q, a, b, G, n, h) is generated for an entity A using the following procedure :

(i)Select a random or pseudo-random integer d in the interval [1,n-1].

(ii)Compute Q = dG.

(iii)A's public key is Q; A's private key is d.

Public key cryptographic algorithms (asymmetric key algorithms) play an important role in providing security services:

- Key management
- ser authentication
- Signature
- Certificate

1.Source Initialization λS_{ix}

2.Rout Discovery β_{sx}

3.Packets and ID's P_{id}

4.Set the threshold value (T_H =45)

5.To Generate Secrete Key (Encode, Decode) Process

6.For Normal transmission

$\beta_{sx} \leftarrow T_H(x) + P_{id}$

7.For(T_H =0; $T_H \leq N$; T_H ++)

8.If

$T_H \leftarrow A$ // Satisfied the Threshold Value

9.Else

$T_H \leftarrow B$ // Not satisfied the Threshold the value some threads injected

10.For Secure Transmission Process

Step:1 Secrete key generated

11.Encode key generated

$E_{id} \leftarrow \beta_{sx} + 1(x)$

$D_{id} \leftarrow \beta_{sx} + 1(y)$

12.Encode Security Key -1 $E_{id} \leftarrow 0x1hj@$ //Packet key injected Source Side

13. Decode Security Key -2 $D_{id} \leftarrow 0x1hj@$ //Packet key injected Destination Side

14. // Same Process Following by coming Packet

Step: 2 Route Discovery

$\beta_{sx} \leftarrow E_{id}(x) + D_{id}(y)$

$\lambda S_{ix} \leftarrow \beta_{sx} + 1$ // Retransmission process

Step 3: Identify the Duplicate packet

$\beta_{sx} \leftarrow P_{id}(x)$

$\lambda S_{ix} \leftarrow \beta_{sx} + 1$ // Retransmission process the same

Step 4: Destination Side

$R_{ax} \leftarrow \beta_{sx} + \lambda S_{ix} + 1$ //Receive the Correct Packets reply the Ack.

5.CONCLUSION AND FUTURE WORK

The security and privacy issues in the medical sensor data collection, storage and queries have been investigated and presented a complete solution for privacy-preserving medical sensor network. To secure the communication between medical sensors and data servers, the lightweight encryption scheme and MAC generation scheme based on SHA-3 proposed are used. To keep the privacy of the patient data, a new data collection protocol which splits the patient data into three numbers and stores them in three data servers, respectively is proposed. One of the most critical security concerns before deploying a WSN in healthcare applications is patient privacy because their vital signs and activities are monitored all the time. To achieve this, authentication and access control must be enforced to ensure that only authenticated healthcare professionals can access, and further can access data that they have privilege for their healthcare services. A public key cryptography called Mutual Authentication and Access Control based on Elliptic Curve Cryptography (MAACE) will be introduced. MAACE provides mutual authentication (a healthcare professional can authenticate to an accessed node (a PDA or medical sensor) and vice versa) and ensures a healthcare professional can only access data that he/she has privilege. By applying elliptic curve cryptography, MAACE provides a public key approach, which is more scalable and requires lesser memory compared to symmetric key-based schemes. Its performance makes it practically feasible to be implemented on sensor platforms. One of the main issues in Elliptic Curve Cryptography is that point multiplication operation takes significant time (810 ms) (and consequently, increases energy consumption) compared with point adding. Reducing the ECC's Point Multiplication operation cost will be our next goal to provide a more secure and energy-efficient scheme for WSNs.

6.REFERENCES

[1] P. Belsis and G. Pantziou. A k-anonymity privacy-preserving approach in wireless medical monitoring environments. Journal Personal and Ubiquitous Computing, 18(1): 61-74, 2014.

[2] D. Bogdanov, S. Laur, J. Willemson. Sharemind: a Framework for Fast Privacy-Preserving Computations. In Proc. ESORICS' 08, pages 192-206, 2008.

[3] R. Chakravorty. A Programmable Service Architecture for Mobile Medical Care. In Proc. 4th Annual IEEE International Conference on Pervasive Computing and Communication Workshop (PERSOMW'06), Pisa, Italy, 13-17 March 2006.

[4] J. Daemen, G. Bertoni, M. Peeters, G. V. Assche, Permutation-based Encryption, Authentication and Authenticated Encryption, DIAC'12, Stockholm, 6 July 2012.

[5] S. Dagtas, G. Pekhteryev, Z. Sahinoglu, H. Cam, N. Challa. Real-Time and Secure Wireless Health Monitoring. Int. J. Telemed. Appl. 2008, doi: 10.1155/2008/135808.

[6] F. Hu, M. Jiang, M. Wagner, D. C. Dong. Privacy-Preserving Telecardiology Sensor Networks: Toward a Low-Cost Portable Wireless Hardware/Software Codesign. IEEE Trans. Inform. Tech. Biomed, 11: 619-627, 2007.

[7]Y. M. Huang, M. Y. Hsieh, H. C. Hung, J. H. Park. Pervasive, Secure Access to a Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks. IEEE J. Select. Areas Commun. 27: 400-411, 2009.

[8]J. Ko, J. H. Lim, Y. Chen, R. Musaloiu-E., A. Terzis, G. M. Masson. MEDiSN: Medical Emergency Detection in Sensor Networks. ACM Trans. Embed. Comput. Syst. 10: 1-29, 2010.

[9] P. Kumar, Y. D. Lee, H. J. Lee. Secure Health Monitoring Using Medical Wireless Sensor Networks. In Proc. 6th International Conference on Networked Computing and Advanced Information Management, pages 491-494, Seoul, Korea, 16-18 August 2010.

[10] P. Kumar and H. J. Lee. Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey. Sensors 12: 55-91, 2012

[11]X. H. Le, M. Khalid, R. Sankar, S. Lee. An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Network in Healthcare. J. Networks 27: 355-364, 2011

[12] H. J. Lee and K. Chen. A New Stream Cipher for Ubiquitous Application. In Proc. ICCIT'07, South Korea, 2007

[13] X. Lin, R. Lu, X. Shen, Y. Nemoto, N. Kato. SAGE: A Strong Privacy-Preserving Scheme Against Global Eavesdropping for eHealth System. IEEE J. Select. Area Commun. 27: 365-378, 2009

[14] D. Malan, T. F. Jones, M. Welsh, S. Moulton. CodeBlue: An Ad-Hoc Sensor Network Infrastructure for Emergency Medical Care. In Proc. MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES'04), Boston, MA, USA,6-9 June 2004

[15] K. Malasri, L. Wang. Design and Implementation of Secure Wireless Mote-Based Medical Sensor Network. Sensors 9: 6273-6297, 2009