Securing BSN's Private Data of Patient's using an Efficient Two Password Authentication Technique

Mamalisa Nayak
Computer Science & Engineering, Bhopal (MP)

Nitin Agrawal
Computer Science & Engineering, Bhopal (MP)

ABSTRACT

Security plays a vital role in the transmission of data from the sender to the receiver whether it will be wired network or wireless network. Wireless body sensor networks are the devices that are embedded in the body of the patient's so that the patient health will be observed by the doctor. Although wireless body sensor network devices are used to sense the data that can be send to the database storage from where the doctor can read the patient's data, but here privacy of the patient's data concerns an important issue when the data send from sensors to storage site and from storage site to doctor.

Here in this paper, providing an efficient technique of securing patient's private data using two password authentication techniques along with the use of IBE-ECIES(Identity based encryption-Elliptic Curve Integrated Encryption Scheme).

1. INTRODUCTION

Wireless Body sensor Network or simply BodyNet are the wireless devices that are used to sense the data and the data read by the sensors can be send to the storage site. Here in the body of the patient's are using multiple sensors such as for the body temperature, Heart rate, Blood Oximeter etc. These sensors are the small storage devices having their internal storage memory and are used to sense the data.

Body Sensor Networks (also known as bodynets or Body Area Networks) have the potential to revolutionize healthcare monitoring. These networks are comprised of wearable devices with attached sensors that can measure various physiological and environmental signals. Bodynet devices communicate wirelessly with networked gateways (mobile phones, computers and PDAs) which store, analyze and communicate vital information in real-time. A Bodynet can be designed to immediately alert emergency personnel to a critical situation like a heart attack or a debilitating fall. Bodynets can also help physicians catch warning signs of a disease earlier or remotely monitor the progress of a recovering surgery patient.

The emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. Applying wireless sensors toward health care monitoring of patient allows for new ways to provide quality health care to patients.

BSN has its own characteristics compared to wireless sensor networks (WSNs):

- It is a network with small-scale structure and super short range of communications.
- Its nodes are limited in their power, computation, and communication capabilities, especially for those implanted into the body.
- It closely surrounds the body which is physiologically and biologically well-known to consist of its own transportation systems.
- It is physiological data that BSN nodes basically detect, collect and transmit.

Security in body sensor networks (BSNs) for medical applications is particularly important because sensitive medical information must be protected from unauthorized usage for personal advantages and fraudulent acts.

Data privacy and security can introduce myriad of problems in body sensor network used for health care. For example, patient health data can be misused by corporations (e.g. in deciding promotions), insurance companies (e.g. in refusing health coverage) etc.. Healthcare applications therefore must meet the stringent requirements of the Health Insurance Portability and Accountability Act (HIPAA) in the US [1]. Bodynet addresses these issues with an infrastructure that enables:

(1) Secure data administration with healthcare providers,

(2) Sound network security,

(3) Secure sensing and monitoring devices, and,

(4) Stronger patient-provider authentication.

1.1 BENEFITS OF BODY SENSOR NETWORK

Important healthcare benefits using Body Sensor Network include:

- **Continuous Monitoring for Chronically-ill patients:** Remote health monitoring enables chronically-ill patients to conform to long-term course of medical treatment that can considerably reduce the crisis and relapse rate for such patients.

- **Better Quality Care and Feedback:** By enabling more effective monitoring of patient's condition, BSN application provides more accurate and useful information to medical personnel. This ultimately leads to better medical advice and feedback to patients. This also leads to better treatment of ailments and an overall improvement in the quality of care for patients.

- **Increased Medical Capacity:** Medical centres using BSN application can treat many more patients. Hospitals often have patients with ailments which require a long recovery period. Using BSN application many such patients can be very effectively monitored and treated in their homes. This offers the potential for increased medical capacity and personalized healthcare.

- **Reduced Medical Cost:** Mobile healthcare using BSN reduce relapse rates of ailments and hospitalization period for patients. Not only it reduces the need for frequent medical consultation, but also by ensuring such reductions, the mobile healthcare system can significantly reduce medical costs.

1.2 WORKING OF BSN

Applying wireless sensors toward health care monitoring allows for new ways to provide quality health care to patients. A diverse array of specialized sensors can be deployed to monitor, for instance, at-risk patients with history of the patient's which is private. These sensors provide continuous, long term monitoring in an unobtrusive manner, allowing doctors to diagnose problems more effectively.

A body sensor network, or BSN, is a network of sensors deployed on a person's body to collect physiological information Figure 3.3. In this thesis, the main focus is on a BSN deployed for medical monitoring. The term person wearing the BSN as the patient, and the person access the data as the doctor. The term "doctor" is used loosely, and refers to any person wanting to access the data. The data collected by the BSN is either stored on the sensors, or forwarded and archived on publicly accessible site known as the storage site.

2. LITERATURE SURVEY

There are various protocols implemented for the security of the patient's private data and also there are several authentication techniques implemented in these wireless devices.

Advanced Health and Disaster Aid Network (AID-N) [2] is developed at the Johns Hopkins University Applied Physics Laboratory. The system facilitates communication between health providers at disaster scene, medical professionals at local hospitals, and specialist available for consultation from distant facilities.

AMON [3] is the advanced care and alert portable tele-medical MONitor project financed by the EU FP5 IST program. It is a wearable (wrist-worn) medical monitoring and alert system that targets high-risk cardiac/ respiratory patients.

CodeBlue [4] is a wireless infrastructure intended to provide common protocol and software framework in a disaster response scenario. The architecture was developed at Harvard University which allows wireless monitoring and tracking of patients and first responders.

HealthGear [5] is designed as real-time wearable system for constant monitoring, visualizing and analyzing the user's SpO2, HR, plethysmographic signals and location information available in the cell phone.

The LifeShirt [6] System by VivoMetrics [7] is a miniaturized, ambulatory version of an in-patient system. The system consists of the LifeShirt garment, data recorder, VivoLogic analysis and reporting software.

Many attempts have been made to solve the problem of establishing secure communications, from symmetric and traditional public-key cryptography through today's breakthrough technology, Identity-Based Encryption (IBE) [8].

Even though BSN is a comparatively new technology, it has garnered tremendous interest and momentum from the research community. This phenomenon is easy to understand when one remarks that a BSN is essentially a sensor network, or to a broader extent an ad hoc network [9], with characteristics peculiar to mobile health applications. So far, the current trend in BSN research has focused mainly on medical settings [10]. As an ad hoc network, a typical BSN consists of small sensor devices, usually destined to report medical data at varying intervals of time. A typical high-level BSN organization. Each BSN consists of a number of sensors, dedicated to monitoring medical data of the wearer. As noted in [10], for implanted sensors, wireless communication is by far the preferred solution since wired networking would necessitate laying wires within the human body; and for wearable devices, wireless networking is also desirable due to user convenience.

For many years, the discrete logarithm problem has been providing useful tools for key exchange, signatures and encryption. Diffie-Hellman key agreement [11] is describing a scheme that is widely used for key exchange between two parties.

ID-based encryption was proposed by Adi Shamir in 1984[12]. He was however only able to give an instantiation of identity-based signatures. Identity-based encryption remained an open problem from past. IBE as a usage as a research leading up to identity-based encryption is provided in Maurer[13].

The pairing-based Boneh–Franklin scheme[14] and Cocks's encryption scheme[15] based on quadratic residues both solved the IBE problem in 2001.

3. PROPOSED METHODOLOGY

The proposed algorithm works in two stages:

Stage 1

1. Doctor'd' will first request the central authority for the registration.
2. The central authority then responds doctor and ask for the secrete value of doctor.
3. The doctor then send a secrete value to the central authority on the basis of which it will generates a unique key for the doctor.
4. Now if the doctor is authenticated he has to enter his secrete value and password which is then send to the central authority where password matches.

Stage 2

The sensors in the body of patient's start reading data on various parameters and starts encrypting the data by making an identity based on the patientid||sensorname||data||time. The encryption algorithm used here is the identity based encryption using the concept of elliptic curve integrated encryption scheme as given:

INPUT: Message m and public key

OUTPUT: The ciphertext (U,c,r)

1. Choose k € R(1…….q-1)
2. U ← [k]G
3. T ← [k]Y
4. (k1||k2) ← KD(T,l)
5. Encrypt the message c ← Ek1(m)

6. Compute the MAC on the ciphertext r ← MACk2(c).

The doctor that wishes to access the data will have to validate himself on the central authority and can access and decrypt only the reading whose identity is known and be given as:

INPUT: Ciphertext (U,c,r) and a private key r.

OUTPUT: The message m or an 'invalid ciphetext' message.

1. T ← [x]U
2. (k1||k2) ← KD(T,l)
3. Decrypt the message m ← Dk(c).
4. if r ≠ MACk2(c) then output 'Invalid Ciphertext'

4. RESULT ANALYSIS

Public key: The key generated when the sensors starts reading from the patient.

Signature: The sensors when reads the data and encrypted that data using signatures (verification of the sender and the receiver so that the unauthorised user can't access the data) so that data can't be access eavesdropped and the signatures when matched can be decrypted.

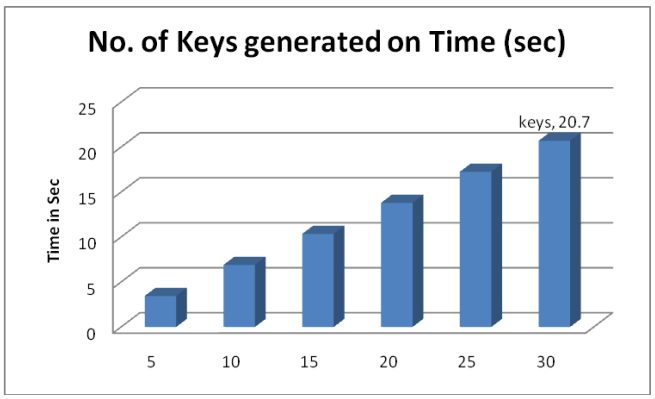
Encrypted Data: The data which is not in actual form but can be converted into another form such that the even if the data is accessed can't understand by the others.

Decrypted Data: The data which is encrypted to provide a security to the data will be decrypted by the same technique used for encryption such that data is correct and readable.

Data storage: The memory required to store a single data from the patient in the sensor.

Public key	**Signature time**	**Time to encrypt**	**Time to decrypt**	**Storage**
0.69 sec	0.70 sec	5.5 sec	2.07 sec	45 bytes

As shown in the above table is the analysis of different parameters when applied ECIES scheme on the security of patient's data.



As shown in the above graph is the comparative analysis of number of keys generated according to the time. Here in IBE using ECIES for the patient's private data contains a number of public/private generated.

5. CONCLUSION

In this paper a new algorithm has been proposed a new way of authenticating the patient's private data from the storage site by the doctor. Here the concept of two password authentication techniques where the person is a doctor or not is validated and then the doctor has to authenticate on the storage site and from where he can only access the patent's data whose identity is known to him. The two password technique implemented here provides various types of security features includes various types of attacks and also provides less storage and computational time.

6. REFERENCES

[1] The US Department of Health and Human Services. Summary of the HIPAA Privacy Rule, 2003.

[2] T. Gao, D. Greenspan, M. Welsh, "Vital sign monitoring and patient tracking over a wireless netowrk", Proceeding of 27th annual international conference of the IEEE EMBS, September 2005.

[3] U. Anliker, J. Ward, P. Lukowicz, "AMON: A wearable multiparameter medical monitoring and alert system" IEEE Transactions on information technology in Biomedicine, Vol. 8, No. 4, Pages 415-427, December 2004.

[4] K. Lorincz , D. Malan, A. Nawoj, G. Mainland, M. Welsh, "Sensor networks for emergency response: challenges and opportunities", IEEE Pervasive Computing, Vol. 3, No. 4, Pages 16- 23, October 2004.

[5] N. Oliver, F. Flores-Mangas, "HealthGear: A Real-time Wearable System for onitoring and Analyzing Physiological Signals" Microsoft Research Technical Report MSR-TR-2005-182. http://research.microsoft.com/ nuria/healthgear/ healthgear.htm.

[6] A. Cardenas, R. Pon, R. Cameron, "Management of streaming body sensor data for medical information systems", The 2003 International Conference on METMBS, Las Vegas Nevada, Pages 186-191, June 2003.

[7] VivoMetrics, http://www.vivometrics.com/site/system techspecs.html.

[8] http://www.voltage.com/technology/ibe.htm

[9] W. R. Heinzelman, A. Chandrakansan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proceedings of the 33rd Annual Hawaii International Conference on SystemSciences (HICSS '00), vol. 2, pp. 3005–3014, Maui, Hawaii, USA, January 2000.

[10] C. C. Y. Poon, Y.-T. Zhang, and S.-D. Bao, "A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health," IEEE Communications Magazine, vol. 44, no. 4, pp. 73–81, 2006.

[11] RSA Data Security, Inc. PKCS #3: Diffie-Hellman Key Agreement Standard, June 1991.

[12] Adi Shamir, Identity-Based Cryptosystems and Signature Schemes. Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7:47--53, 1984

[13] Ueli M. Maurer: Protocols for Secret Key Agreement by Public Discussion Based on Common Information. CRYPTO 1992: 461-470

[14] Dan Boneh, Matthew K. Franklin, Identity-Based Encryption from the Weil Pairing Advances in Cryptology - Proceedings of CRYPTO 2001 (2001)

[15] Clifford Cocks, An Identity Based Encryption Scheme Based on Quadratic Residues, Proceedings of the 8th IMA International Conference on Cryptography and Coding, 2001/