Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Analysis of Security in Various eHealth Networks

Varsha Mary George, P. Blessed Prince
Department of Information Technology
Karunya University, Coimbatore, India

Abstract— Modern healthcare scenario is rapidly changing. The older generation is aging and their population is increasing. Additionally, diseases are becoming diverse and more severe in affecting both the elderly and children. Healthcare is turning out to be complex and expensive. For efficient and constant health monitoring, patients are fitted with sensors on their bodies which are either wearable or implantable, to form body area networks to monitor, record and transmit medical statistics for perusal by physicians. Sensors from different patients are networked or linked together to form health sensor networks. As the devices in these networks work on wireless technologies, their usual vulnerabilities are present in these networks as well. This paper gives insights into the various ways in which several ehealth systems and networks have been employed and tried to be made secure countering their various vulnerabilities.

Keywords— Healthcare, Ehealth, Health networks, Body Area Networks, Security

I. INTRODUCTION

The face of today's healthcare has changed from what it was more than a decade earlier. Physicians and health personnel are looking to technology more than ever to help in taking care of elderly patients, critical infants and others [10]. The care of the elderly, for example those who are afflicted with a serious, incapacitating disease and need care 24/7 can be taken care of by making use of medical sensors which are either wearable or implantable. These sensors monitor and measure required medical readings and then transmit necessary medical information to a remote healthcare facility or centre which is connected to this network. These form what are called Body Area Networks (BANs) or Body Sensor Networks (BSNs) as shown in figure 1. The physician makes use of the data from these networks to keep a constant eye on their patients remotely. This health setup comes very handy in emergency situations where a sudden change in a person's vital statistics might require immediate medical attention and instant communication without the least possible human error.

Biosensors are also employed in healthcare scenarios to the same effect mentioned before [4][5]. RFIDs are another element used in such networks for purposes of tracking and identification of patients and their medication routines [13]. The RFID tags are built into bracelets for example, and worn by patients inside the healthcare facility. The tag has an ID, which is associated with the patient and stored in a database to be read by the RFID reader. Health personnel can also have these RFID tags embedded in their cards to provide them with specific access and privileges when it comes to getting access to patients' rooms and their medical data. This involvement of electronics and information technology in healthcare is what gives rise to the term ehealth. The medical data in such scenario can be stored in electronic form known in different circles by different names such as Electronic Patient Record (EPR) or Patient Information Record (PIR).

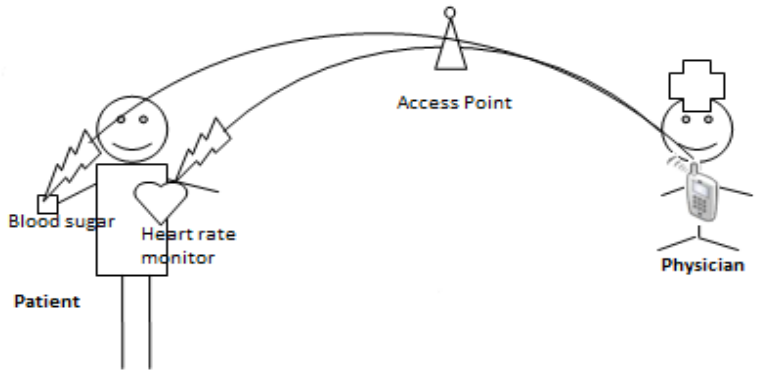

Fig 1. Example scenario of wireless body area network

Given all the good things about such electronic health networks, security is a major issue. This is especially true when critical medical data is transmitted, for instance when EPRs are transmitted through the network. There is a chance for malicious intruders to intercept the data or procure it through unlawful means, and then even manipulate it, which cause harm to the patient. This paper reviews various health networks and the security measures employed.

II. SECURITY REQUIREMENTS

Every wireless network with sensors or other devices handling critical information is vulnerable to many security breaches. This is especially true when there is a wireless transmission channel to be secured against various attacks posed by malicious parties. The presence of patient health information records also needs to ensure the following security properties.

- *Confidentiality* makes sure that the information is understandable only to that person for whom it was meant.
- *Integrity* guarantees that no malicious alteration has been made to data while in transit or otherwise.
- *Availability* guarantees that data is handy to anyone who needs it at the right time.
- *Authentication* proves to the data receiver that it was indeed sent by the person who claimed to be the sender.
- *Authorisation* guarantees that only those who are authorised to perform certain actions can perform them.
- *Self-organisation* guarantees that the sensors are autonomous in handling sticky situations that arise in the network amongst them.
- *Non-repudiation* makes sure that no one can deny that a message was received or sent by them.
- *Privacy & anonymity* guarantees that no one can be targeted based on their identity or location, which is prevented from exposure [2][3].

III. SECURING DATA EXCHANGE AND STORAGE

Data collected in the health networks are private and critical information belonging to the patients, and should be accessible only to the patients and their respective medical personnel. The data can be stored in electronic form as Electronic Patient Record (EPR) or Patient Information Record (PIR). While passing through the network, these data must be secured from security breaches as they may contain highly sensitive data that patients want to keep private for various reasons, both personal and work related. It is also possible that malicious people who want to harm a person can access these records, if not secured properly.

A. Standard Encryption

Ko et al. proposed MEDiSN, which is a wireless sensor network meant to measure patient vital signs. It carries out 128-bit Advanced Encryption Standard (AES) based symmetric encryption and decryption to protect the data gathered. This application falls behind when it comes to policy violations [5] though. Cherukuri et al. used RC5 [4], a symmetric key block cipher as the encryption algorithm for securing the communication in their biosensor network.

Quirino et al. in regards to asymmetric encryption in WSNs in [15] talked about RSA public key algorithm (1024-bit RSA) being the most commonly used as it is standardized and has relatively better efficiency. Elliptic curve cryptography is also discussed to have potential due to its higher energy efficiency and better performance, provided smaller keys are used. The authors also mention a new scheme that was proposed in 2008 called Multivariate Quadratic Quasigroup (MQQ. 160-bit MQQ which was compared in this paper showed to be magnitudes faster than RSA and ECC in hardware.

[13] talked about the use of hash functions and pseudo random number generators for use in the encryption and re-encryption in the RFIDs. RSA and AES are some of the cryptographic algorithms used in RFIDs for encryption and decryption; lightweight versions are specially designed for use in them.

B. Using Algebraic Signature

In [6], Wang et al. proposed a secure data storage scheme in sensor networks. Initially when the data is stored, the original encrypted data is broken into *n* data shares, each of which consists of a data block generated from (n, k)-erasure coding, and a share of the secret key using (n, k)-secret sharing [6]. Then the shares of data are distributed to *n* neighbour nodes for storage. Here, any modification in data can be detected in the following manner. When a node wants to do an integrity check, all the other storage nodes compute and broadcast an algebraic signature on their data share, and the checking node verifies the integrity by checking its signature against those of other nodes.

C. Using Biometrics

Asymmetric cryptographic algorithm such as RC5 is used in [4] to secure data exchange in the communication links among the biosensors and between the biosensors and the control node outside. The data is encrypted using a suitable key. The key is generated based on biometric readings taken of the patient. These readings taken at different times in different situations result in different and truly random readings. This randomness is highly useful for the cryptographic randomness required when selecting keys. Poon et al. [9] made use of the variations in time found in heartbeat as a unique biometric characteristic for securing data. In [14], the author extracted the key from the fingerprint biometric trait, which was then randomized by applying a genetic operator. In [16], static biometric traits were used to generate authentication keys and dynamic biometric traits to generate encryption keys. 64-bit and 128-bit keys were generated from electrocardiograms, photoplethysmograms and fingerprint images. The hamming distances between the keys were non-zero and their entropy was in the range from 0.662 to 1.

IV. AUTHENTICATION

Without proper authentication anyone can access a patient's private data for malicious purposes. Authentication mechanisms are a necessary security measure to allow only authorised people access to data.

Lu et al. in [8], discussed about a mobile healthcare social network in which elderly patients can communicate with other elderly patients with similar symptoms. In order to prevent other people from knowing their symptoms and to identify those with the same symptoms, they have proposed a secure same symptom-based handshake (SSH) scheme. In the scheme, every patient is provided with a pseudo-ID and a private key corresponding to his/her symptom. So, if two

patients meet, if they have the same symptom, they can use their respective private keys to mutually authentication each other. The paper also explained about patient health information delivery through this connection among patients. Liang et al. proposed an attribute-oriented authentication scheme in [1]. They explained about a health social network in which the users are each assigned attributes based on certain characteristics by the attribute trusted authority. Each of the HSN users have the ability to generate an attribute proof for themselves, whereby the sensitive attributes can be anonymized if they so choose. Only by verifying the provided attribute proof (figure 2), will the other users be able to know what attributes an HSN user has and thus can authenticate themselves to access others' personal medical data.

Recently, D. He et al. proposed an authentication protocol for wireless medical sensor networks. It helps to authenticate the health professional in order to access a patient's physiological data. The protocol in [7] consists of professional registration and patient registration phases, followed by the login and authentication phase. The authentication is performed by inserting a smart card in a card reader, which inputs the professional's id and password, followed by using random numbers and checking timestamps for authenticating. This protocol provides user anonymity as well.

Althobaiti et al.'s [17] is an example of a biometric trait being used for authentication in wireless sensor network. They used the iris of the user to regenerate the user's key every time the user needs be authenticated which considerably enhances the security. After extracting the iris's features, the biometric encryption is performed by using a fuzzy commitment scheme, the biometric data is then stabilised. This stabilised data is bound with the user's random generated key during registration phase. The saved hash value of the encryption key is used during the remote authentication process.

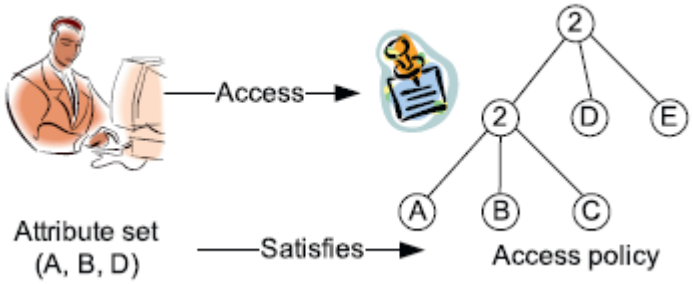

Fig 2. User generates attribute proof for verification, and thus authenticates [1]

V. ACCESS CONTROL AND PRIVACY

Restricting access to a patient's private medical information data is an important facet of security.

Massacci et al. in [10] discussed about accessing resources based on two things, one being that a person should be given rights explicitly to access that resource and second being that there should be a specific purpose for using it, hence their principle is stated as no purpose, no data. There are specific goals, roles and goals-roles assignments in this system based on which resources can be accessed; this access is provided by the access control manager. The predefined security policies in the system determines if there is any danger based on which emergency requests are sent to the medical centre.

In [11], Mohan et al. explained MedVault, a framework for sharing electronic health records. The EHRs are kept in a source verifiable repository. Identity agents and an authorisation module are also present. The request for a particular record from a user is met with compliance to associated access policies. The amount of information requested, even if by an authorised individual is considered so as to help protect a patient's privacy. This system provides fine-grained patient control over information disclosure thus safeguarding privacy, and data integrity and verifiability to both patients and health care providers. The use of attributes facilitates role based access control as well.

Memon [12] described role based access control in healthcare ad hoc networks. In RBAC, users are granted membership into roles based on their assigned responsibilities in the organization. Policies are defined for each group and role so the user is automatically assigned access rights to various data within the organisation. Each functional role has a set of permissions once it is activated for a particular session, and remains active for that session unless explicitly specified otherwise. RBAC is described as policy neutral and is said to support security policy objectives, and the static and dynamic separation of duty limitations which might come as a result of change in roles themselves or the policies associated with those roles.

VI. CONCLUSION

Health monitoring networks are rampant these days. With the massive amount of medical data amassed in these networks and the transmission of these medical records over numerous communication links, security is an important issue. Securing the data exchanged and stored by authenticating those people who access the data and restricting access to those who are not authorised to do so, are some of the aspects that come under security for such health networks.

REFERENCES

[1] X. Liang, M. Barua, R. Lu, X. Lin and X. Shen, "HealthShare: Achieving secure and privacy-preserving health information sharing through health social networks," *Elsevier Computer Communications*, Vol.35, Iss.15, pp. 1910–1920, Sep. 2012.

[2] A. Aldini, G. Barthe, R. Gorrieri, Ed., *Foundations of Security Analysis and Design V*, ser. Lecture Notes in Computer Science. Berlin, Germany: Springer, 2009, Vol.5705.

[3] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks", *IEEE Commun. Surveys Tutorials*, Vol.8, pp. 2 -23, 2006.

[4] S. Cherukuri, K. K. Venkatasubramanian and S. K. S. Gupta "BioSec: A Biometric based Approach for Securing Communication in Wireless Networks of Biosensors Implanted in the Human Body", in *Proc. IEEE ICPPW'03*, 2003, pp. 432-439.

[5] J. Ko, J. H. Lim, Y. Chen, R. Musvaloiu-E, A. Terzis, G. M. Masson, T. Gao , W. Destler, L. Selavo, R. P. Dutton, "MEDiSN: Medical emergency detection in sensor networks", *ACM Transactions on Embedded Computing Systems (TECS)*, Vol.10 No.1, pp. 1-29, Aug. 2010.

[6] Q. Wang , K. Ren , W. Lou and Y. Zhang, "Dependable and secure sensor data storage with dynamic integrity assurance", *ACM Transactions on Senor Networks*, Vol.8, No.1, Article 9, 24 pages, Aug. 2011.

[7] D. He, N. Kumar, J. Chen, C. Lee, N, Chilamkurti, S. Yeo, "Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks", *Multimedia Systems*, Springer, Dec. 2013.

[8] R. Lu, X. Lin, X. Liang, X. Shen, "Secure handshake with symptoms-matching: the essential to the success of mhealthcare social network", *Mobile Network Applications*, Springer, Nov. 2010.

[9] C. C. Y. Poon, Y. Zhang, S. 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, Sep. 2006.

[10] F. Massacci, V. Nguyen, A. Saidane, "No purpose, no data: goal oriented access-control for ambient assisted living", *ACM workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS)*, pp. 53-58, 2009.

[11] A. Mohan, D. Bauer, D. Blough, M. Ahamad, B. Bamba, R. Krishnan, L. Liu, D. Mashima, B. Palanisamy, "A patient-centric, attribute-based, source-verifiable framework for health record sharing", *Technique Reports*, 2009.

[12] Q. A. Memon, "Implementing Role Based Access in Healthcare Ad Hoc Networks", *Journal of Networks*, Vol.4, No.3, pp. 192-199, 2009.

[13] Y. Xiao, X. Shen, B. Sun, L. Cai, "Security and Privacy in RFID and Applications in Telemedicine", *IEEE Communications Magazine*, Vol.44 , Iss.4, pp. 64-72, April 2006.

[14] B. Shanthini, S. Swamynathan, "Genetic-based Biometric Security System for Wireless Sensor-based Health Care Systems", *RACSS 2012*, April 2012, pp. 180-184.

[15] G. S. Quirino, A. R. L. Ribeiro and E. D. Moreno, "Asymmetric Encryption in Wireless Sensor Networks", Wireless Sensor Networks - Technology and Protocols, Dr. M. Matin (Ed.), ISBN: 978-953-51-0735-4, InTech, DOI: 10.5772/48464. Available from: http://www.intechopen.com/books/wireless-sensor-networks-technology-and-protocols/asymmetric-encryption-in-wireless-sensor-networks

[16] G.H. Zhang, C.C.Y. Poon, Y.T. Zhang, "A biometrics based security solution for encryption and authentication in tele-healthcare systems", *ISABEL 2009*, Nov. 2009, pp. 1-4.

[17] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, "An Efficient Biometric Authentication Protocol for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, vol.2013, Article ID 407971, 13 pages, 2013. doi:10.1155/2013/407971

