International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

Enhanced Private and Secured Medical Data Transmission

Mr.K.Nareshkumar thappa[1], Margret.M[2], Preethi.M[3]

[1,2,3] *Department of Electronics And Communication Engineering, Velammal Engineering College*

ABSTRACT: *E-/m-Healthcare still faces many challenges including information security and privacy preservation. To address these problems, a healthcare system (HES) framework is designed that collects medical data from WBANs, transmits them through an extensive wireless sensor network infrastructure and finally publishes them into wireless personal area networks (WPANs) via a gateway. HES involves the GSRM (Groups of Send-Receive Model) scheme to realize key distribution and secure data transmission, the HEBM (Homomorphic Encryption Based on Matrix) scheme to ensure privacy and an expert system able to analyze the scrambled medical data and feed back the results automatically. Theoretical and experimental evaluations are conducted to demonstrate the security, privacy and improved performance of HES compared with current systems or schemes.*

Key Terms— healthcare system, wireless sensor network, security, privacy protection, key distribution

Existing System:

The emergence of wireless body-area networks has become a key enabler of remote and in-home health monitoring. The technology is expected to revolutionize the health and real-time body-monitoring industry. e-/m-healthcare still faces many challenges to its widespread adoption such as privacy breach violations, medical data collection, transmission, processing and presentation has become a critical issue in e-healthcare applications, in which a variety of wireless sensor nodes and terminal devices play important roles in network data aggregation and communications for people to gather information concerning their health status easily, anytime and anywhere using smart mobile devices these medical data consist of personal private information that should not be susceptible to eavesdropping or malicious tampering during transmission.

Proposed System:

The Major contributions can be described as (1) The e-/m-healthcare architecture "HES", based on wireless sensor networks, is proposed. HES incorporates an expert system designed to achieve an automatic analysis of scrambled medical data and "minimal participation" of authorized doctors in general physical examinations. (2) A key distribution scheme based on a group send-receive model "GSRM" is proposed for secure data transmission in wireless sensor networks, and a privacy-preserving strategy of homomorphic encryption based on matrix "HEBM" is advanced to disrupt the original medical data before release onto WPANs. (3) Theoretical analysis and simulation experiments are conducted to verify that the performance of the proposed designs can indeed achieve security, efficiency, feasibility, network delay-toleration and connectivity simultaneously. (4) The implementation of HES includes the development of medical sensors, correlative software and network system.

I.INTRODUCTION:

The rapid technological convergence of Internet of Things (IoT), wireless body-area networks (WBANs) and cloud computing has caused e-healthcare (electronic-healthcare) to emerge as a promising information-intensive industrial application domain that has significant potential to improve the quality of medical care [1]. Therefore, how to achieve medical data collection, transmission, processing and presentation has become a critical issue in e-healthcare applications, in which a variety of wireless sensor nodes and terminal devices play important roles in network data aggregation and communications. Furthermore, the evolution of m-health (mobile-health) technology has made it possible for people to gather information concerning their health status easily, anytime and anywhere using smart mobile devices . However, these medical data consist of personal private information that should not be susceptible to eavesdropping or malicious tampering during transmission. Therefore, the privacy protection and secure transmission of e-/m-healthcare (electronic-/mobile-healthcare) data has drawn more attention from many researchers. A secure and reliable e-/m-healthcare framework to defend against hostile attacks and threats is highlighted for available applications of the informationalized healthcare industry. Moreover, a challenge remains concerning how to effectively process the ever-growing volume of healthcare data and protect data privacy but maintain low sensor network overhead . Due to the resource-strained characteristics (such as limited power) of mobile devices and sensors, the tradeoff between efficiency and privacy or security must be further

balanced for the commercial promotion of e-/m-healthcare. Therefore, a meaningful concern of this paper is the design of a feasible, efficient and privacy-guaranteed e-/m-healthcare information system employing wireless sensor networks.

Modules:

- A role-based access control scheme
- Security and privacy scheme
- Secure patient data transmission using HMAC (Keyed-Hashing for Message Authentification) algorithm(Enhancement)

A role-based access control scheme:

Most current e-/m-healthcare systems require doctors (or system administrators) to participate in medical information processing, which brings two problems: low effectiveness caused by manual operations and privacy breaches due to doctors' acquaintance with users' private data. A medical expert system that can automatically analyze users' scrambled private data but minimize doctors' participation can address these two problems, current wearable medical devices and nodes cannot be directly linked with smart mobile terminals through 4G or Wi-Fi. Additional network infrastructure or gateway devices are required to enable interconnection between such devices and nodes. Even when the mobile phone has been directly equipped with medical sensors or biometric information-sensing components, current technology limits it to collecting only one or two data items. many e-/m-healthcare architectures fail in terms of the feasibility of data transmission directly from WBANs to wireless personal area networks (WPANs) or the Internet because implementation difficulty and the need for network connectivity are not considered.

Security and privacy scheme:

To ensure the security of medical data transmitted in wireless sensor networks, key distribution schemes and block encryption methods are required. Its can improve efficiency by decreasing the resource consumption of memory, a key distribution scheme based on a group send-receive model (GSRM) and AES is proposed. The base station starts the procedure of building a group from those nodes. The leader node will record the count of its neighbor nodes with the same GSRM-level values and the count of its neighbor nodes whose GSRM-level values are greater than its value by one and dropped nodes will become isolated nodes. To better adapt to the privacy-preserving characteristics of HES, HEBM (Homomorphic Encryption Based on Matrix) also proposed. the medical data of a user can be denoted by an n-dimensional where area is a random number two matrices denoted by M and M' separately are identity matrices. Second, the random number and the random prime number will be generated. Third, three area will be defined. Therefore, HEBM can effectively resist the following attacks. (1) A leakage of privacy by the administrator or anyone who owns the highest authority. (2) Eavesdrop attack. The attacker is unable to access substantive information. (3) Chosen plaintext attack. the attacker has already obtained the entire records of a specific user who utilized medical services from HES times. The HES can be summarized in three areas: (1) using low-cost and easily-deployed wireless sensor networks as the relay infrastructure for GSRM-based secure transmission of medical data from WBANs to WPANs; (2) addressing the problem of achieving direct communications between a user's mobile terminals and embedded (wearable) medical devices (nodes); (3) enforcing privacy-preserving strategies HEBM and achieving satisfactory performance. HES can serve as a significant component of the informationization of medical industries. However, some problems remain unsolved; for example, the diagnosis reliability of the expert system is not perfect, and HES cannot currently monitor or analyze sudden diseases.

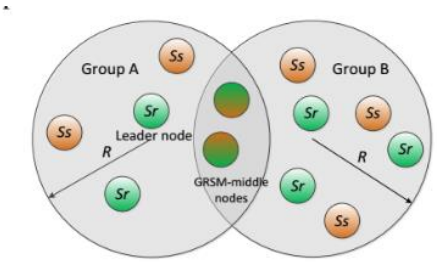


Fig. 2. Group send-receive and GSRM-middle nodes

Algorithm Used:

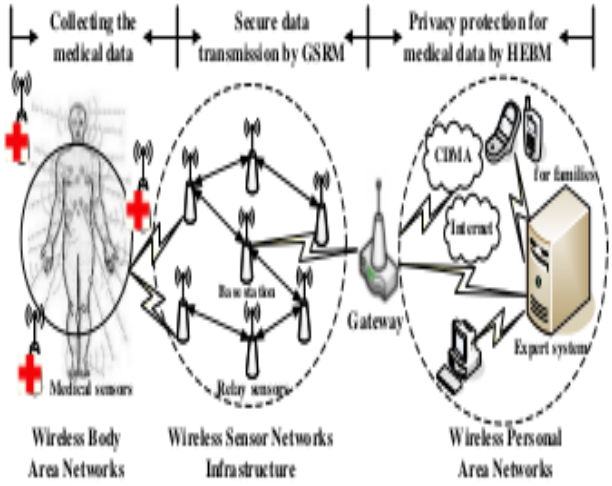
-
- GSRM algorithm

Secure patient data transmission using HMAC algorithm(Enhancement):

MAC algorithms involve the use of a secret key to generate a small block of data, known as a "message authentication code," that is appended to the message. This technique assumes that two communicating parties, say A and B, share K as a secret key. When A has a message to send to B, it calculates the message authentication code as a function

of the message and the key. The message and code are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new message authentication code. The received code is compared to the calculated code we proposed a lightweight and secure system for wireless medical sensor networks (MSN). Each patient area network (PAN) consists of some biosensors and a controller. These biosensors collect his/her personal health information(PHI) like body temperature, blood pressure, heart bear rate, blood glucose level Sensors forward the information to the controller The security techniques are chain key mechanism provide during each and every transmission of medical data from sensor to medical server the chain key gets updated.

II.ARCHITECTURAL DIAGRAM



III. PERFORMANCE ANALYSIS

a. Average storage cost

The storage cost of HES proposed in this paper primarily comes from the keys stored in sensors. Generally, a more convincing analysis of the average key storage cost is based on comparisons among GSRM, the classic algorithm q-composite (short for qc) and its improved algorithm proposed in (short for Imp.qc). We suppose that N sensor nodes are randomly distributed in a range of $w \times h$, in which these nodes can be divided into groups by GSRM and the average number of nodes in each group is 2ξ. The average storage cost of each node in GSRM can be described as $2\pi\rho R2$ and is positively related to the density ρ. In qc or Imp.qc, network connectivity must be guaranteed; otherwise, nodes cannot communicate with each other by exchanging shared keys. To prevent network connectivity from varying sharply, the density ρ is consistently kept as a constant with the coinstantaneous increase of both node number and region size.

In addition, GSRM has the following properties:

(1) Forward Confidentiality: Once the network detects a node that has suffered from the capture attack, keys updates are performed automatically, thus making it impossible for the captured node to obtain the new keys instantly or to participate in subsequent sessions.
(2) Backward Confidentiality: When key updates occur, due to the lack of previous keys, the fresh nodes are unable to decrypt the data packages generated before they entered the network.

b. security and privacy of HEBM

The HEBM scheme focuses more on the privacy protection of medical data. The matrix permutation and data confusion make it impossible for anyone except the source to obtain the plaintext of private data. Therefore, HEBM can effectively resist the following attacks.

(1) A leakage of privacy by the administrator or anyone who owns the highest authority. Even when the information stored in the WPANs server is decrypted, it remains confused and thus cannot be discriminated even by the administrator.
(2) Eavesdrop attack. The attacker is unable to access substantive information even when a data packet is captured due to the lack of decrypted keys.
(3) Chosen plaintext attack.

We make the following assumptions for the chosen plaintext attack on HEBM: the attacker has already obtained the entire records of a specific user who utilized medical services from HES t times. Each service record can be described as a triple {X, M, C}={Xi, Mi, Mi*Xi}, where X, M and C indicate the real medical data, scrambling matrix and confused medical data, respectively; i=1, 2, ..., t. We shall prove that when the attacker accesses a new medical record Mt+1*Xt+1 from the same user, the posterior probability P(X=Xt+1 | C=Mt+1*Xt+1) that Xt+1 is broken by the attacker equals the prior probability P(X=**X**t+1), where Xi and Mi are mutually independent.

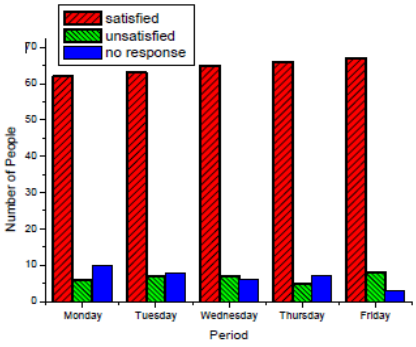


Fig. 3. User's feedback toward HES

IV.CONCLUSION:

We proposed a secure and lightweight system for wireless medical sensor network. The medical data transmission is done in a secure manner using chain key updating mechanism. Fine-grained access control was achieved using chain key technique. The security techniques such as chain key mechanism and achieves the goal i.e. secure patient medical data transmission and access control in the wireless medical sensor network.

References

[1]Sawand, S. Djahel, Z. Zhang, and F. Naït-Abdesselam, "Toward Energy-Efficient and Trustworthy eHealth Monitoring System, " China Commun., vol.12, no. 1, pp. 46-65, Jan. 2015.

[2] M. S. Shin, H. S. Jeon, Y. W. Ju, B. J. Lee, and S. P. Jeong, "Constructing RBAC Based Security Model in u-Healthcare Service Platform," The Scientific World J., vol. 2015, Article ID 937914, 13 pages, http://dx.doi.org/10.1155/2015/937914, 2015.

[3] C. Wang, B. Zhang, K. Ren, J. M. Roveda, C. W. Chen, and Z. Xu. "A Privacy-aware Cloud-assisted Healthcare Monitoring System via Compressive Sensing," in Proc. of 33rd IEEE INFOCOM, 2014, pp. 2130-2138.

[4] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area

Networks," in Proc. of 35th IEEE Symp. on Security and Privacy, 2014, pp. 524-539.

[5] C. Bekara and M. Laurent-Maknavicius, "A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks," in Proc. of 3rd IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), 2007, pp. 59-59.

[6] P. T. Sivasankar and M. Ramakrishnan, "Active key management scheme to avoid clone attack in wireless sensor network," in Proc. of 4th Int. Conf. on Computing, Communications and Networking Technologies (ICCCNT'13), 2013, pp. 1-4.

[7] A. Marcos, J. Simplicio, H. I. Leonardo, M. B. Bruno, C. M. B. C. Tereza, and M. N¨aslund, "SecourHealth: A Delay-Tolerant Security Framework for Mobile Health Data Collection," IEEE J. Biomedical and Health Informatics (IEEE Trans. INF TECHNOL B), vol. 19, no. 2, pp. 761-772, Mar. 2015.

[8] R. X. Lu, X. D. Lin, and X. M. (Sherman) Shen, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency," IEEE Trans. Parall. distr., vol. 24, no. 3, pp. 614-624, Mar. 2013.

[9] A. Amirbekyan and V. Estivill-Castro, "A New Efficient Privacy-Preserving Scalar Product Protocol," in Proc. of Sixth Australasian Conf. Data Mining and Analytics (AusDM '07), 2007, pp. 209-214.

[10] A. C. F. Chan, "Symmetric-Key Homomorphic Encryption for Encrypted Data Processing," in Proc. of 2009 IEEE International Conference on Communications (ICC '09), 2009, pp.1-5.

[11] C. C. Zhao, Y. T. Yang, and Z. C. Li, "The Homomorphic Properties of McEliece Public-Key Cryptosystem," in Proc. of 2012 Fourth International Conference on Multimedia Information Networking and Security (MINES'12), 2012, pp.39-42.

[12] J. Reid, I. Cheong, M. Henrickson, and J. Smith, "A novel use of RBAC to protect privacy in distributed health care information systems," in Proc. of 8th Australasian Conf. on Information Security and Privacy, 2014, pp. 403-415.

[13] J. Mirkovic, H. Bryhni, and C. Ruland, "Secure solution for mobile access to patient's health care record," in Proc. 13th IEEE Int. Conf. e-Health Netw. Appl. Serv., 2011, pp. 296-303.

[14] J. A. Akinyele, M. W. Pagano, M. D. Green, C. U. Lehmann, Z. N. Peterson, and A. D. Rubin, "Securing electronic medical records using attribute-based encryption on mobile devices," in Proc. of 1st ACM Workshop Security Privacy Smart phones Mobile Devices, 2011, pp. 75-86.

[15] L. K. Guo, C. Zhang, J. Y. Sun, and Y. G. Fang, "A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks," IEEE Trans. Mobile Compu., vol. 13, no. 9, pp. 1927-1941, Sep. 2014.

[16] J. J. Yang, J. Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems, vol. 2015, no. 43-44, pp. 74-86, Nov. 2015.

[17] O. Kocabas, T. Soyata, J. P. Couderc, M. Aktas, J. Xia, and M. Huang, "Assessment of cloud-based health monitoring using Homomorphic Encryption," in Proc. of 2013 IEEE 31st International Conference on Computer Design (ICCD'13), 2013, pp.443-446.

[18] A. Page, O. Kocabas, S. Ames, M. Venkitasubramaniam, and T. Soyata. "Cloud-based secure health monitoring: Optimizing fully-homomorphic encryption for streaming algorithms," in Proc. of 2014 Globecom Workshops, 2014, pp.48-52.

[19] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices," In Proc. of ACM Sigcomm'11, Aug. 2011, pp. 2-13.