Private and Secure Medical Data Transmission using QR Code

Harshada S. Nichit[1], Mitali J. Gadge[2], Pallavi S. Sonawale[3], Sneha S. Gadekar[4], Prof. Rote R. R.[5]

Students[1,2,3,4] and Guide[5]

Samarth Group of Institution College of Engineering, Belhe, Maharashtra, India

Abstract: *The concurrence of Internet of Things (IoT), cloud computing and wireless body-area networks (WBANs) has greatly promoted the industrialization of e-/m-healthcare (electronic-/mobile-healthcare). However, the further brandish of e-/m-Healthcare still faces many challenges including information security and privacy protection. To address these problems, a healthcare system (HES) framework is designed that collects medical data from WBANs, transmits them through an large wireless sensor network infrastructure and finally issue them within wireless personal area networks (WPANs) via a gateway. Furthermore, HES involves the GSRM (Groups of Send-Receive Model) scheme to realize key classification and secure data transmission, the HEBM (Homomorphic Encryption Based on Matrix) scheme to ensure privacy and an expert system able to analyze the clamber medical data and feed back the results automatically. Theoretical and experimental estimate are conducted to display the security, privacy and improved performance of HES compared with current systems or schemes. Finally, the prototype implementation of HES is explored to verify its possibility.*

Keywords: Internet of Things, medical management, wireless sensor network, safety, privacy protection, key distribution

I. INTRODUCTION

The rapid technological concurrence of Internet of Things (IoT), wireless body-area networks (WBANs) and cloud computing has caused e-healthcare (electronic-healthcare) to emerge as a good information-intensive industrial application domain that has importance potential to improve the grade of medical care . Therefore, how to achieve medical data collection, transmission, processing and presentation has become a critical matter in e-healthcare applications, in which a variety of wireless sensor nodes and terminal devices play important roles in network data collection and connection. Furthermore, the evolution of m-health (mobile-health) technology has made it possible for people to together information about their health status easily, anytime and anywhere using smart mobile devices . However, these medical data consist of personal private information that should not be exposed to overhear or bitter tampering during transmission. Therefore, the privacy protection and secure transmission of e-/m-healthcare (electronic-/mobile-healthcare) data has drawn more observation from many researchers. A safe and good e-/m-healthcare framework to defend against hostile attacks and risk 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 trade off between efficient and privacy or safety must be further balanced for the commercial promotion of e-/m-healthcare. Therefore, a meaningful concern of this paper is the design of a possible, effectively and privacy-guaranteed e-/m-healthcare information system employing wireless sensor networks.

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 violation due to doctors' contact with users' private data. A medical expert system that can automatically analyze users' clamber private data but reduce doctors' participation can address these two problems, particularly for the application of general physical examinations. Even with perfect access control mechanisms, frequent human intervention will always cause a higher risk of privacy reveal in e-/m-healthcare. As a major component of e-/m-healthcare systems, the development of a medical specialist system is another focus of this paper.

DOI: 10.48175/568

II. SECURITY OF GSRM

In a key management system, an attacker can obtain a large number of keys by capturing a small fraction of sensor nodes, which enables him (or her) possibly to take control of the entire network by deploying a replicated mobile sink to preload some compromised keys for authentication and then initiate data communication with any sensor node. Here, we make the following assumptions:

1. The attacker can randomly capture nodes from any network area.
2. The attacker has the ability to read the memory information of a captured node and obtain all its secret keys.
3. The attacker is unable to capture or attack the base station.
4. We use the ratio of the number of keys originating from those nodes captured by the attacker to the total keys as the metric of anti-capturing attacks. We assume that the keys stored in each node range from 2 to 5, with 2000 nodes in the network and 1000 keys in the key pool.The ratio increases approximately linearly with the rise of captured nodes. GSRM has a stronger anti-capturing ability than Imp.qc and qc because the keys carried by each node are dispersed in groups, resulting in less information being obtained by the attacker even when he (or she) has controlled the whole group.

III. SECURITY AND PRIVACY OF HEBM

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

1. A beginning of privacy by the administrator or anyone who owns the highest power. Even when the information reserve in the WPANs server is decrypted, it remains confused and thus cannot be separate even by the administrator.
2. Intrude attack. The attacker is unable to access certain information even when a data packet is captured due to the lack of decrypted keys.
3. Select plaintext attack.
4. Replay attacks. During each handshaking session, the disarrange medical data send in channels at one specific moment differs from that at another moment because the matrix M is randomly generated, and such an inconformity is uncertain. Therefore, the attack is unable to conduct a fake inquiry by replay attacks.
5. Camouflage trust strike. If a fake server claims to be an expert system, it is impossible for it to obtain the plaintext because the data packet is encrypted. Moreover, it remains impractical for the fraud server to acquire the results even when the data packet is decrypted because the data remain confused.

IV. IMPLEMENTATION OF HES

To verify the possible of HES, we have designed a prototype system and realized the fundamental functions. Wearable medical nodes add the HK-2000H digital pulse sensor, the DS-100A oxygen finger clip and the DS-18B20 temperature sensor. Many temperature sensor nodes based on the CC2420 conversation module are self-organized as relay networks. The gateway node make the protocol transformation between ZigBee and CDMA2000 or publishes the medical data to the specialist system and other mobile devices within WPANs through Wi-Fi. We developed healthcare applications for handy mobile devices based on Android 4.1 and an specialist system based on Ubuntu OS. We deployed our medical nodes and convey nodes in one particular hospital, end the integration of HES software and hardware with the network system, and installed the APP on the mobile phones of a few patients, doctors and nurses.

To verify preliminarily the dependability and possible of the specialist system, we tested 78 patients using HES (only body temperature, heart rate and blood oxygen) for a time of one week. Note that one main feature of HES is that it is available for the families and guardians to access health status information of these 78 patients via their mobile phones' APP, which also caters to the scenario of remote healthcare for senior people. The analysis of questionnaires of their families and guardians. Three situations are possible: satisfied with the results provided by the expert system, disappointed and no response. We see a relatively high approval of results provided by the specialist system.

DOI: 10.48175/568

V. CONCLUSION

Aiming at the existing point of e-/m-healthcare systems, a distinct framework "HES" is proposed in this paper. The features of HES can be summarized in three areas:

1. Using low-cost and easily-deployed wireless sensor networks as the relay infrastructure for GSRM-based fixed transmission of medical data from WBANs to WPANs;
2. Addressing the problem of achieving direct conversation between a user's mobile terminals and embedded (wearable) medical devices (nodes); and
3. Enforcing privacy-preserving plan HEBM and achieving satisfactory performance. The implementation of an specialist system that primarily addresses routine physical inspection can greatly reduce a doctor's or administrator's involvement and enable families and guardians to access users' health information anytime and anywhere. Therefore, HES can serve as a importance component of the informationization of medical industries. However, some problems remain unsolved. For example, the diagnosis reliability of the specialist system is not perfect, and HES cannot currently monitor or analyze sudden diseases.

VI. REFERENCES

[1]. A. 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 AreaNetworks," 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.