IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

Private and Secured Medical Data Transmission and Wireless Networks using Smart Quick Response QR Code

Lande Vaishnavi Chandrakant, Bedare Apurva Gajanan, Kharat Priyanka Subhash, Hirave Shubhangi Namdev, Prof. Gunjal S.P.
HSBPVT'S GOI, College of Engineering, Ahmednagar, Maharashtra, India

Abstract: *The convergence 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 flourishing of 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. Furthermore, 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. Finally, the prototype implementation of HES is explored to verify its feasibility.*

Keywords: Hospital, Patient, Medical, Doctor

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

II. RELATED DEFINITIONS

Definition 1: A set of nodes is a group of send-receive, if and only if: (1) All the sensor nodes are included within a circle whose radius is R (half of the sensor communication range). (2) The count of nodes in the group is an even number, denoted by 2ξ (ξ=1, 2 ...). (3) Approximately one-half of the nodes (denoted by Ss) only send messages. The other one-half (denoted by Sr) only receive messages. (4) A leader node exists that is elected by one given algorithm in a group.
Definition 2: A node is a GSRM-middle node if and only if the node simultaneously belongs to at least two adjacent groups and can send (or receive) messages from one group to the other or receive (or send) messages in opposite directions. As shown in Fig. 2, two nodes are GSRM-middle nodes, not only in Group A but also in Group B. Generally, there should be more than one GSRM-middle node to make the network unobstructed

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

III. GROUP CONSTRUCTION

When a wireless sensor network is initialized (the procedure can be completed off-line for security considerations), the base station can be considered the origin of a polar coordinate system. A node that can communicate with the base station within one hop, for example Node 1-1 in Fig. 3, calculates the distance d11 between itself and the base station and the departure angle to the base station θ 11, where d11>0, - π ≤ θ 11≤ π . Then, it sends the two parameters d11 and θ 11 to all its neighbor nodes in one hop. Node 2-1 in Fig. 3, for example, also calculates the relative distance d11-21' and the departure angle θ11-21' between itself and the corresponding sender. Then, Node 2-1 can calculate the following: 2 2 21 11 11 11 21 11 21 11 11 11 21 11 21 11 11 11 21 11 21 21 11 11 11 21 11 21 (cos 'cos ') (sin 'sin ') sin 'sin ' arctan( ) cos 'cos ' d d d d d d d d □ (1) However, every node whose GSRM-level is greater than 0 will most likely receive more than one message with distance and angle parameters

IV. KEY DISTRIBUTION

After the execution of Algorithm 1, the leader node of each group will distribute keys for member nodes. If the total number of one group's nodes is 2ξ, the total number of keys that will be distributed is ξ. For example, in a group, when ξ=2 (including two Ss nodes, Ss1 and Ss2, and two Sr nodes, Sr1 and Sr2), two keys will be generated and represented as key1 and key2. Furthermore, a hash function h(x) is chosen to participate in the key distribution. The keys used for different sessions in this example are display.

Based on TABLE I, we can derive other keys when ξ=ξ'>2 from the given recursion rules. If we have learned the key h[key(i, j)] used by Ssi and Srj when ξ=ξ'-1, then we can derive the current key "keyξ'" dispatched for the session between Ssi and Srj when ξ=ξ'□>2. Two random integers r1 and r2 (r1, r2 [1, ξ'-1]) will be generated for the calculation of "keyξ'". Furthermore, when ξ=ξ'+1, the recursion rules will be repeated. All cases of keys used for different sessions in one group are display.

4.1 HEBM for Data Privacy Protection

Not all homomorphic encryption methods can be directly applied to the e-/m-healthcare system based on WSNs, particularly when considering resource constraints and the requirements of the expert system. To better adapt to the privacy-preserving characteristics of HES, HEBM (Homomorphic Encryption Based on Matrix) is proposed. We suppose that a user of HES must submit n medical data items from WBANs via the wireless sensor network infrastructure to WPANs and then obtain the results through the automatic analysis of the expert system. Each type of medical data has a normal region, for example, the normal range of human body temperature (armpit) is between 36 degrees Celsius and 37 degrees Celsius, i.e., [36.00℃, 37.00℃]. If HES can examine a total of l types of medical data, the normal region of the ith medical data item (i=1, 2, ..., l) can be represented as [mini , maxi].

4.2 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) [5] and its improved algorithm proposed in [6] (short for Imp.qc). We suppose that N sensor nodes are randomly distributed in a range of w×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 2πρR2 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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

B. Network Connectivity

The connectivity of GSRM, qc and Imp.qc is related to the keys stored in sensor nodes. To compare the network connectivity fairly, we assume that each sensor node shares the same average key storage, ranging from 0 to 30. There are 100 nodes in the network. Other relative simulation parameters except for N and ρ are shown in TABLE III.

As shown in Fig. 6, the GSRM algorithm is superior to qc (Imp.qc and qc have the same connectivity) when the numbers of keys stored in each sensor are relatively small. However, when keys reach 20 or more, the network connectivity of these two schemes, in which the isolated nodes have been neglected, is approximately 100%.

C .Security analysis

The security analysis of HES can be divided into two parts: the security of GSRM and that of HEBM.

a. 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 Security 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.

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.

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.

D. System Delay

The system delay of HES for transmission and processing of the medical data remains low due to the following aspects:

1. During the initialization of WSNs, the group division and key distribution can be performed offline; once the initialization is completed, the network can be employed without any delay.
2. The characteristics of GSRM facilitate decreased information exchange between nodes; during the send-receive process of medical data, only three handshakes are required to finish a circle. Thus, a reduced communication frequency means less network delay.

E. Computation Efficiency

To test and verify the computation efficiency of HEBM, similar approaches based on homomorphic encryption are found and analyzed. Consequently, simulation experiments are conducted for comparisons among HEBM, IHC (proposed in [10]) and McEliece (proposed in [11]); all of them achieve data privacy-preservation based on matrix operation. All three methods can be divided into two phases: the initial phase and the encryption/decryption phase (Enc./Dec. phase for short).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

F. Related Work

The emergence of wireless body-area networks (WBANs) 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 [1]. However, e-/m-healthcare still faces many challenges to its widespread adoption such as privacy breach violations [7]. J. Reid et al [12] design a role-based access control scheme that assigns the access authorities in terms of different doctor levels. J. Mirkovic et al [13] also propose a similar access control method. Moreover, an encryption method is frequently selected for the design of secure and privacy-preserving e-/m-healthcare. J.A. Akinyele et al [14] consider attribute-based encryption as an effective approach of protecting the privacy of electronic medical records. L. K. Guo et al [15] find a close relationship between patients' medical records and a sequence of attributes such as existing symptoms and undergoing treatments, and put forward a decentralized m-health system that leverages patients' verifiable attributes to authenticate each other in order to preserve attribute and identity privacy. Furthermore, some approaches based on homomorphic encryption have drawn more focus, although not all of them can be directly utilized in e-/m-healthcare. A. C. F. Chan [10] designs two schemes, which ensure that highly similar plaintexts can be transformed into distinctly different ciphertexts to resist ciphertext-only attacks. C. C. Zhao et al [11] study the homomorphic properties of the McEliece Public-key Cryptosystem and claims that this method can ensure security when data are transmitted in an unsafe environment. These schemes focus mostly on medical data privacy or security; however, some important performance metrics such as computation overhead, network connectivity, delay and power consumption are ignored.

V. CONCLUSION

Aiming at the existing issues 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 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); and (3) enforcing privacy-preserving strategies HEBM and achieving satisfactory performance. The implementation of an expert system that primarily addresses routine physical examinations 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 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.

ACKNOWLEDGEMENT

We are very thankful to our professors and specially to our guide prof .Gunjal S.P for his significant help in completing this project.

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

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

[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.