Achieve Privacy Preserving Priority Classification On Patient Health Data In Remote Ehealthcare System

Pampana Manasa, Smt.K.R.Rajeswari, Sri.V.Bhaskara Murthy
MCA Student, Assistant Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

ABSTRACT

The Wireless Body Area Network (WBAN) has attracted considerable attention and become a promising approach to provide a 24-hour on-the-go healthcare service for users. However, it still faces many challenges on privacy of users' sensitive personal information, confidentiality of healthcare center's disease models. For this reason, many privacy-preserving schemes have been proposed in recent years. However, the efficiency and accuracy of those privacy-preserving schemes become a big issue to be solved. In this paper, we propose an efficient and privacy-preserving priority classification scheme, named PPC, for classifying patients' encrypted data at the WBAN-gateway in a remote eHealthcare system. Specifically, to reduce the system latency, we design a on-interactive privacy-preserving priority classification algorithm, which allows the WBAN-gateway to conduct the privacy-preserving priority classification for the received users' medical packets by itself and relay these packets according to their priorities (criticalities). Detailed security analysis shows that the PPC scheme can achieve the priority classification and packets relay without disclosing the privacy of the users' personal information and confidentiality of the healthcare center's disease models. In addition, the extensive experiments with an android app and two java server programs demonstrate its efficiency in terms of computational costs and communication overheads.

I. INTRODUCTION

With the pervasiveness of smart phones and the wireless body area network (WBAN), the remote e Healthcare system has received considerable attention and become more popular. A variety of WBAN schemes and applications have been proposed [1]–[4] in recent years, including energy-efficient medium access protocol for WBAN using the listen-before transmit manner [2], data forwarding framework between biosensors and the gateway considering the presence of body shadowing [3], prioritized adaptive resource allocation algorithm for WBAN based on patients' medical situation [4]. Considering the limited resource of the sensors, the collected data streams cannot be transmitted directly to the healthcare center.

On the other hand, the disease models are precious intellectual properties of the healthcare center. The healthcare center is not willing to reveal the disease models to the users or the WBAN-gateways. Some attackers may crack the users' smart phones or the WBAN-gateways, and steal the sensitive users' personal information and the healthcare center's intellectual properties. Therefore, a variety of privacy-preserving schemes have been proposed in remote e Healthcare system [5]–[8].

However, the privacy-preserving healthcare schemes based on the encrypted data have some issues like accuracy and efficiency to be solved. We outline the challenges for

privacy-preserving remote e Healthcare system would face as below: Challenges on security and privacy. As discussed above, all the users' physiological data, personal information and the healthcare center's disease models need to be encrypted. An attacker should not recover the sensitive plaintext by observing the cipher text, i.e., secure under cipher text-only attack. Moreover, it is reasonable to assume in some scenarios, the attacker knows some users' information or some disease models.

Even in this context, the attacker cannot recover other plaintext of the corresponding encrypted data. In other words, the system should be secure under know-plaintext attack. Challenges on accuracy. To achieve the security requirements of the remote e Healthcare system, some privacy-preserving schemes based on the encrypted data need to standardize the users' personal information and healthcare center's disease model first. The standardization techniques may compromise the computational accuracy. What's more, some randomization techniques like the differential privacy [9] add some random values to the computational results, which may cause medical disaster in some scenarios [10]. Therefore, the privacy preserving remote e Healthcare system should be accurate for medical analysis. Challenges on efficiency. Most of the privacy-preserving schemes based on the encrypted data are involved with large computational overhead. Recent studies propose some privacy-preserving schemes with multi parties [11],which derives large communication cost. On the other hand, the non-interactive privacy-preserving schemes are always associated with time-consuming techniques, such as fully homomorphic encryption [12]. Thus, the privacy-preserving remote e Healthcare system needs to solve the efficiency issues. In this paper, aiming at solving the above challenges, we propose an efficient and privacy-preserving priority classification (PPC) on patient health data in remote e Healthcare system, which allows authenticated users to periodically send medical packets to the healthcare center through WBAN gate ways.

The WBAN-gateways relay these aggregated medical packets in a non-interactive privacy-preserving way based on the packets' priorities (criticalities). The main contributions of this paper are as following: First, we propose the PPC scheme, an efficient privacy preserving non-interactive priority classification scheme for users' medical packets in WBAN-gateways. Particularly, The WBAN-gateways derive the priorities of the medical packets and relay the packets in a priority heap. Second, we develop an android app and two java server programs to evaluate the performance of the PPC scheme. The results show that the proposed PPC scheme is efficient in both computational cost and communication overhead.

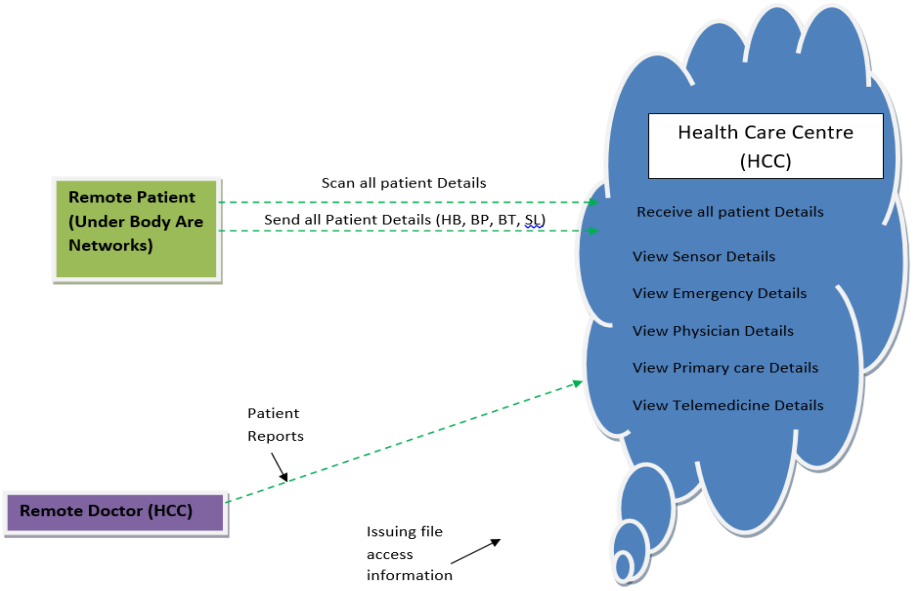
II. LITERATURE SURVEY

The system consists of an unobtrusive wireless body area network (WBAN) and a home health server. The WBAN sensors monitor user's heart rate and locomotive activity and periodically upload time-stamped information to the home server. The home server may integrate this information into a local database for user's inspection or it may forward the information further to a medical server. The prototype may be used for ambulatory monitoring of patients undergoing cardiac rehabilitation or for monitoring of elderly at home by informal caregivers

A network coding scheme for practical implementations of wireless body area networks is presented, with the objective of providing reliability under low-energy constraints. We propose a simple network layer protocol for star networks, adapting redundancy based on both transmission and reception energies for data and

control packets, as well as channel conditions. Our numerical results show that even for small networks, the amount of energy reduction achievable can range from 29% to 87%, as the receiving energy per control packet increases from equal to much larger than the transmitting energy per data packet. The achievable gains increase as a) more nodes are added to the network, and/or b) the channels seen by different sensor nodes become more asymmetric.

III.System architecture

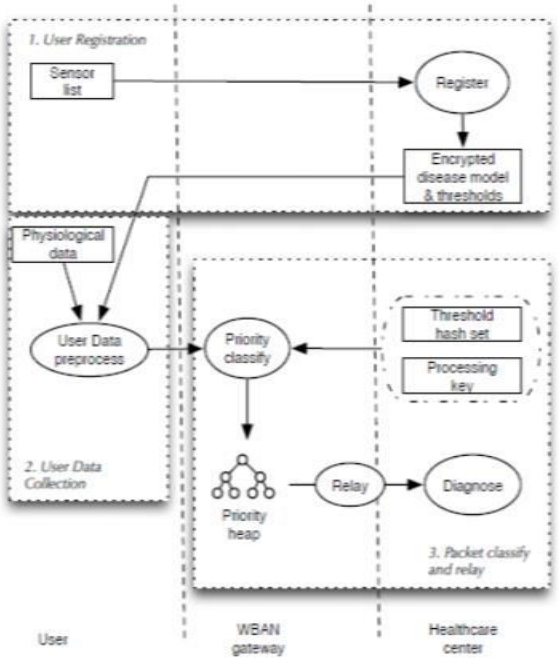


IV.PROPOSED SYSTEM

- The system proposes the PPC scheme, an efficient privacy preserving non-interactive priority classification scheme for users' medical packets in WBAN-gateways. Particularly, The WBAN-gateways derive the priorities of the medical packets and relay the packets in a priority heap.
- The system also develops an android app and two java server programs to evaluate the performance of the PPC scheme. The results show that the proposed PPC scheme is efficient in both computational cost and communication overhead. The security analysis also demonstrates that our proposed PPC scheme can preserve the privacy of the users' personal information and the confidentiality of the healthcare center's disease models.

Advantages

- To achieve the security requirements of the remote eHealthcare system, some privacy-preserving schemes based on the encrypted data need to standardize the users' personal information and healthcare center's disease model first.
- The system gives privacy-preserving schemes based on the encrypted data are involved to give more privacy on data.



Proposed architecture

V.IMPLEMENTATION

- **Body Area Network Provider**

  The Wireless body area network (WBAN) has been recognized as one of the promising wireless sensor technologies for improving healthcare service. This network will detect human diseases like sugar, BP, Heart Beat, temperature and send to the particular solution provider (emergency center, physician, telemedicine server and primary care provider) with their tags such as patient name, patient ID, sugar level, blood pressure, temperature and heart beat through via internet or Earth net or GSM.

- **HCC**

  In this module, the HCC has to login by using valid user name and password. After login successful he can do some operations such as add hospitals, Sensor details, view emergency, view physician, view primary care, view telemedicine, view queries, view complains, view opinions, view patient details, results, change password and logout. The admin can view sensor details with the particular patient details, and then server will give response to the admin with their tags such as patient name, patient number, sugar level, blood pressure, temperature, heartbeat, status, date and time. The admin can view emergency patient details, view the physician details, view the primary care details, view the telemedicine details, view query in a query status is accepted means solution is given to the patient and also admin can view the patient details.

VI.CONCLUSIONS

In this paper, we have proposed an efficient privacy preserving priority classification (PPC) scheme on patient healthcare data in remote

Healthcare system. The proposed PPC scheme achieves the priority classification and packets relay tasks, while preserving the privacy of the users and the confidentiality of the healthcare center's disease models. Because it is a non-interactive procedure, the communication cost is low. We have also implemented an android app and two java programs to demonstrate that our PPC scheme is efficient in computational cost and communication overhead.

REFERENCES

[1] C. A. Otto, E. Jovanov, and A. Milenkovic, "A wban-based system for health monitoring at home," in Ieee/embs International Summer School on Medical Devices and BIOSENSORS, 2006, pp. 20–23.

[2] O. Omeni, A. Wong, A. J. Burdett, and C. Toumazou, "Energy e_cient medium access protocol for wireless medical body area sensor networks,"IEEE Transactions on Biomedical Circuits & Systems, vol. 2, no. 4, p. 251, 2008.

[3] A. Argyriou, A. C. Breva, and M. Aoun, "Optimizing data forwarding from body area networks in the presence of body shadowing with dualwireless technology nodes," Mobile Computing IEEE Transactions on, vol. 14, no. 3, pp. 632–645, 2015.

[4] S. Rezvani and S. A. Ghorashi, "Context aware and channel-based resource allocation for wireless body area networks," Iet Wireless Sensor Systems, vol. 3, no. 1, pp. 16–25, 2013.

[5] N. Mcdonald, D. Atkinson, Y. Khmelevsky, and S. Mcmillan, "Sport wearable biometric data encrypted emulation and storage in cloud," in Electrical and Computer Engineering, 2016, pp. 1–4.

[6] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," IEEE Wireless Communications, vol. 17, no. 1, pp. 51–58, 2016.

[7] Z. Chen, H. Hu, and J. Yu, "Privacy-preserving large-scale location monitoring using bluetooth low energy," in International Conference on Moile Ad-Hoc and Sensor Networks, 2016, pp. 69–78.

[8] C. Y. Chou, E. J. Chang, H. T. Li, and A. Y. Wu, "Low-complexity privacy-preserving compressive analysis using subspace-based dictionary for ecg telemonitoring system," IEEE Transactions on Biomedical Circuits & Systems, vol. PP, no. 99, pp. 1–11, 2018.

[9] C. Dwork and M. Naor, "On the di_culties of disclosure prevention in statistical databases or the case for di_erential privacy," Journal of Privacy & Confidentiality, 2008.

[10] M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page, and T. Ristenpart,"Privacy in pharmacogenetics: an end-to-end case study of personalized warfarin dosing," in Usenix Conference on Security Symposium, 2014, pp. 17–32.

[11] B. Dan and M. Zhandry, "Multiparty key exchange, e_cient traitor tracing, and more from indistinguishability obfuscation," in Cryptology Conference, 2014, pp. 480–499.

[12] M. V. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, Fully Homomorphic Encryption over the Integers. Springer Berlin Heidelberg, 2010.

[13] B. Dan, E. J. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts,"in International Conference on Theory of Cryptography, 2005, pp. 325–341.

[14] D. Harrison, S. Boyce, P. Loughnan, P. Dargaville, H. Storm, and L. Johnston, "Skin conductance as a measure of pain and stress in hospitalized infants," Early Human Development, vol. 82, no. 9, pp. 603–608, 2006.

[15] G. Wang, R. Lu, and C. Huang, "Pguide: An e_cient and privacypreserving smartphone-based pre-clinical guidance scheme," in IEEE Global Communications Conference, 2015, pp. 1–6.