Achieve Privacy-Preserving Priority Classification on Patient Healthcare System

Maheswari Konduru
B.Tech, Department of Computer Science and Engineering, Naryana Engineering College-Gudur, AP, India

N. Yedukondalu
Asst.Professor, Department of Computer Science and Engineering, Naryana Engineering College-Gudur, AP, India

Nikhitha Dasari
B.Tech, Department of Computer Science and Engineering, Naryana Engineering College-Gudur, AP, India

Manasa Aluru
B.Tech, Department of Computer Science and Engineering, Naryana Engineering College-Gudur, AP,

ABSTRACT

The Wireless Body Center's Area Network (WBAN) should provide user-provided health care services for 24 hours and still face many challenges in the confidentiality of users' personal information, confirmation of health care models. Therefore, for this reason, the genius and accuracy of those privacy protection systems become a major problem to be solved. For this project, we are proposing a highly specialized and privately-held privacy system, called PPC, for categorizing data entered into patients at the WBAN gateway at a remote care gate. Specifically, to reduce the system over time, we create interoperable end-user privacy that allows the WBAN gateway to process the privacy of medical packages that users receive and pass these packets according to their priorities. Detailed analysis shows that the PPC system can achieve the saturation of key clusters and packages without revealing the confidentiality of personal information and the robustness of the health care model.

Keywords: Priority, Remote eHealthcare, Privacy, Sensor, User, Disease.

1. INTRODUCTION

With the proliferation of smartphones and the Wireless Body Area Network (WBAN), the long-term eHealthcare system has gained a lot of attention and popularity. Various modes and WBAN applications have been proposed [3], including the centralized WBAN access protocol using pre-transfer listening, data transfer framework between biosensors and gateway for the presence of turnovers of the body [1], an advanced distributed allocation algorithm for WBAN based on patients' medical status [2]. With advances in the wireless network, WBAN became feasible [4]. By considering the finite resource of the sensors, the collected data streams cannot be transmitted directly to the healthcare center[5]. The sensors in each user's wearable health system regularly collect the users' physiological data, send these data to the his/her smartphone for preprocessing. The smartphone assembles a medical packet containing the user's physiological data, and sends it to a WBAN-gateway nearby[5]. The medical packets from different users will be randomly aggregated in WBAN gateways. Then the WBAN-gateways transfer all the medical packets to the remote healthcare center as shown in Figure 1.

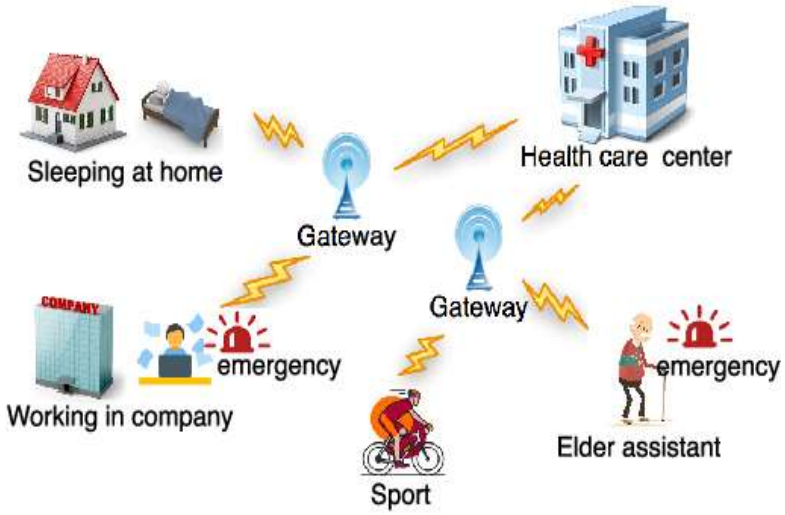

Figure 1. Wearable health monitor system

EXISTING SYSTEM

Access control policies are appropriate strategies used by the PPC. Most of the time, integrated access control policies are adopted to propose ways to control PPC access. It is common to use a combination of control and pseudonymization in a single PPC, which stores user information in an anonymous manner and shares anonymous details with access policy policies. A patient monitoring program was proposed to enable patients to control who can access protected health information. Security systems that protect your privacy based on encrypted data have some problems with accuracy and efficiency that need to be resolved. Higher it raises concerns about leaks and misuse of users' private data. Some attackers may use user smartphones or WBAN gateways, and steal sensitive personal information and intellectual property of a health center.

PROPOSED SYSTEM

Some attackers may disassemble user smartphones or WBAN gates, and steal sensitive personal information and medical packets of the health care center at the entrance of the WBAN gates. First, we propose the PPC system, a privately-held, non-secure operating system for user medical packages in WBAN health packages. In particular, WBAN-drive gates carry significant amounts of medical packages and pass packets at a high volume. The results indicate that the proposed PPC system is applicable to both communication and overhead costs. Security analysis also suggests that our proposed PPC system can maintain the confidentiality of personal data and confidentiality of health care models. The system architecture is shown in Figure 2.

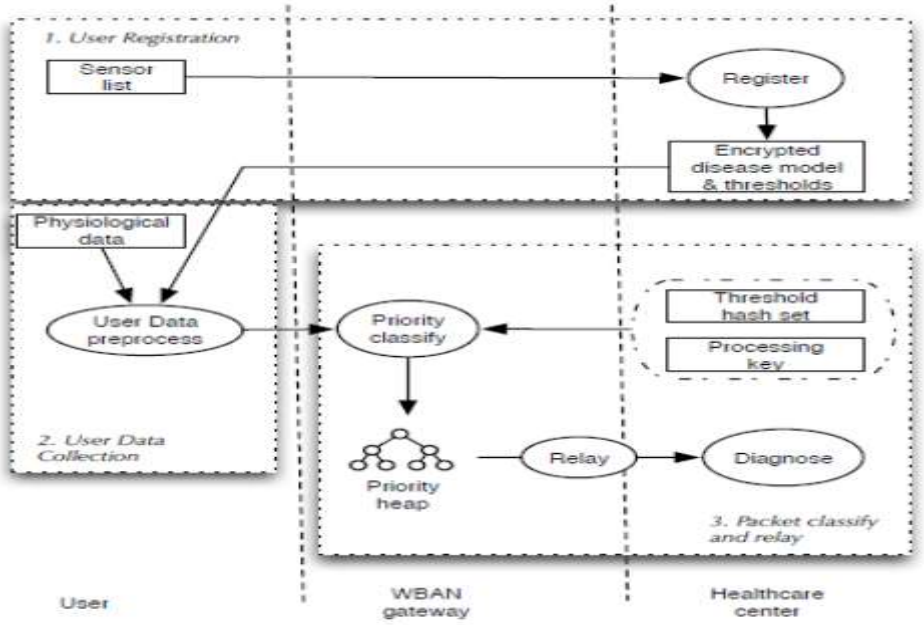

Figure 2. System Architecture

Trusted Authority

In the Admin module, Admin can view all the Data owners and data user's details as shown in Figure 3 and Figure 4. Admin will approve the users and send the signature key and private key to the data owners and data users. Also, the admin will send the search request key to the users. Admin can able to see the files in cloud uploaded by the data owners.

Figure 3. Trusted Authority Login page

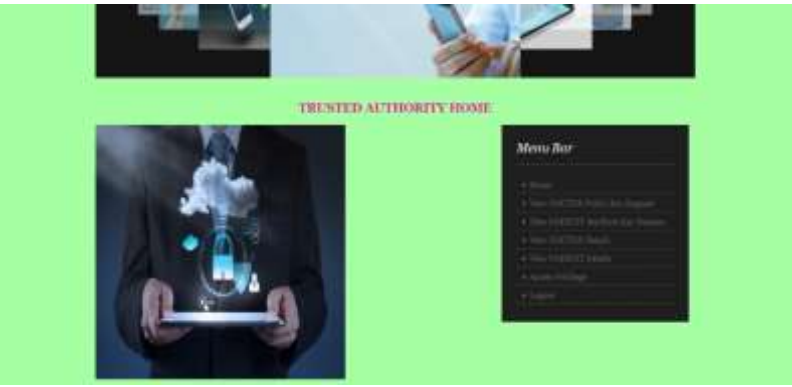

Figure 4. Trusted Authority Home page

User

In the Data User module, initially, Data Users must have to register their detail, and admin will approve the registration by sending signature key and private key through email as shown in Figure 5.

Figure 5. User Registration Form

After successful login, he/she have to verify their login by entering the user ID and password. Data Users can search all the files uploaded by the admin. He/she can send a search request to admin then the admin will send the search key. After entering the search key he/she can view the requested file.

Data Owner

In the Data Owner module, Initially, Data Owner must have to register their detail as shown in Figure 6 and the admin will approve the registration by sending signature key and private key through email. After successful login, he/she have to verify their login by entering a signature and private key.

Figure 6. Owner Registration Form

Then the data Owner can upload files into the cloud server with Polynomial key generation. He/she can view the files that are uploaded in the cloud by entering the secret file key.

CONCLUSION

In this priority, we have proposed an efficient Privacy-Preserving Priority Classification (PPC) scheme on patient healthcare data in the remote eHealthcare 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.

REFERENCES

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

[2] Li Deng "*The MNIST Database of Handwritten Digit Images for Machine Learning Research*. IEEE signal processing Magazine", 29(6), 141-142.

[3] 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.

[4] Aparna A.R., Malini Soman "*Energy-Efficient Medium Access Control Protocols For Wireless Body Area Networks: A Survey*", volume 1, Issue 4, IJSRSET, 2015.

[5] Guoming Wang, Rongxing Lu, And Yong Liang Guan "*Achieve Privacy-Preserving Priority Classification on Patient Health Data in Remote eHealthcare System*" January 9, 2019.