A Multi-Factor Access Control and Ownership Transfer Framework for Future Generation Healthcare Systems

Vidyadhar Aski[1], Vijypal Singh Dhaka[2], Arjun Singh[3], Anubha Parashar[4],

[1, 2, 3, 4] School of Computing and Information Technology, Manipal University Jaipur, India
{[1*]vidyadharjinnappa.aski,[2]vijaypalsingh.dhaka,[3]anubha.parashar,
[4]arjun.singh} @jaipur.manipal.edu

Abstract. The recent advancements in ubiquitous sensing powered by Wireless Computing Technologies (WCT) and Cloud Computing Services (CCS) have introduced a new thinking ability amongst researchers and healthcare professionals for building secure and connected healthcare systems. The data generated by these systems will be further be analyzed in order to enhance the patient quality of life and minimize the healthcare cost. Major concern of such giant connected systems lies in creating the data handling strategies which is collected from the billions of heterogeneous devices distributed across the hospital network. Edge computing technologies offers the cutting edge solution for such issues by evading latency and storage related complexities. The integration of Internet of Things (IoT) in healthcare services further brings in several challenges with it, mainly including encrypted communication through vulnerable wireless medium, authentication and access control algorithms and ownership transfer schemes (important patient information). Besides, the resource constrained nature of IoT would make these goals difficult to achieve. Motivated by aforementioned deliberations, this paper introduces a novel approach in designing a security framework for edge-computing based connected healthcare systems. An efficient, multi-factor access control and ownership transfer mechanism for edge-computing based futuristic healthcare applications is the core of proposed framework. Data scalability is achieved by employing distributed approach for clustering techniques that analyze and aggregate voluminous data acquired from heterogeneous devices individually before it transits the to the cloud. Moreover, data/device ownership transfer scheme is considered to be the first time in its kind. During ownership transfer phase, medical server facilitates user to transfer the patient information/ device ownership rights to the other registered users. On the other hand, proposed framework overcomes the security gaps of existing authentication and access control schemes. In order to avoid the existing mistakes, we propose a formal and informal security analysis, that ensures the resistance towards most common IoT attacks such as insider attack, denial of distributed service (DDoS) attack and traceability attacks.

Keywords: Internet of Things (IoT), Device Security, Edge Computing, Healthcare Data Security, Access Control, e-health.

1 Introduction

It has been witnessed from the recent past that the profound advancements in Healthcare IoT has significantly improved the standard of livings and quality of services of the patients suffering from chronic illnesses. Smart healthcare communities are the similar beneficiaries of such advancements. As a result, the life expectancy of the patient suffering from long term diseases is seemingly increased. However, these developments have directly or indirectly influenced in increasing the old-age population that required regular medical investigations. Therefore, handling such large patient community at clinical care centers with utmost care might be a real challenge for the doctors with the limited time and hospital resources. These issues needed to be addressed with a potential technological solution at the back end. While it is known that the technology cannot decrease the health service needs but can deliver the solution by involving embedded computing [1]. Many researchers have discussed about the electronic healthcare systems (e-health systems) that are powered by advanced Wireless Computing Technologies (WCTs). These WCTs are establishing the communication between the device layer and cloud layer through the dedicated mobile gateway networks [2,3,4]. These type of e-health systems offer the wide variety of remote services, where patient doesn't have to physically visit hospital for clinical analysis but he/she can use e-health systems from their residential places and get treated by tele-medicines [1, 2]. In these systems, patients are provided with the wireless healthcare device which is equipped with the advanced wireless sensors that can be non-invasively placed on patient's body for transferring the significant biomedical data such as body temperature, ECG, pulse rate etc. to the remote cloud [4, 5, 6]. This cloud may be implemented locally in a desktop computer or remotely into a hospital cloud known as Electronic Health Server (EHS) [7]. Once the data is made available in EHS, finally a doctor or a healthcare professional can access the data and further take decisions about the treatment. As far as consumer connection to EHS is concerned, authentication and verification of user's legitimacy is an important phase in verifying the user at early stages. User verification can be achieved by many ways, generally by means of a RFID tags [8]. Sometimes, the combination between human and machine (H2M) is duplexed direction, where an authorized person like doctor can change the patient device programmatically [9, 10].

Further, connected healthcare systems offer the remote services in healthcare field for monitoring of patient's vital bio-parameters by Body Sensor Network (BSN) and a medical practitioner can know the patient status remotely. Such systems are called as Internet of Medical Things (IoMT) [11, 12]. Creating connected healthcare infrastructure in a secured way is one of the major challenges in building automated healthcare infrastructure. Maintaining one's biomedical data privacy is crucially important as there's an essence of creating secured environments so that data can be saved securely from being misused for wrong intensions. In the same way, given healthcare service should provide a mechanism to its users so that individual users can access (read) data and chunks of memory from only the allocated segment. Further, the healthcare device

should have the proper access control mechanism implemented into it in order to verify/validate the user access rights. Generally, this access control mechanism is defined in the EHS provided by hospital administrators and users are defined with various access rights according to the policies defined for each user profiles.

Fig. 1 illustrates the various healthcare entities, environments and their interconnections. The community member's biomedical signal is sent to edge mobile gateway after being source encrypted for further analysis in a local storage unit. Thereafter, using a remote gateway the local data is fed to global cloud storage unit for high level analysis. Standard decryption tools are used at the destination for retrieving the original data. Further, secured machine learning algorithms are employed for making clinical decisions and predictive analyses.

On the other hand, the importance of edge computing can also be understood by the fig. 1. Edge computing is another potential computing paradigm that signifies the middle layer computation between physical devices and the cloud computing unit housing computational power closure to device level [13]. The edge computing layer does not only help IoT infrastructure in transforming data locally but also essential in providing the real time services and making intermediate decisions for patient community. Such system enables healthcare professionals to early detection of chronic illnesses thus buy significantly avoiding permanent disabilities and accordingly the medication support can be provided.

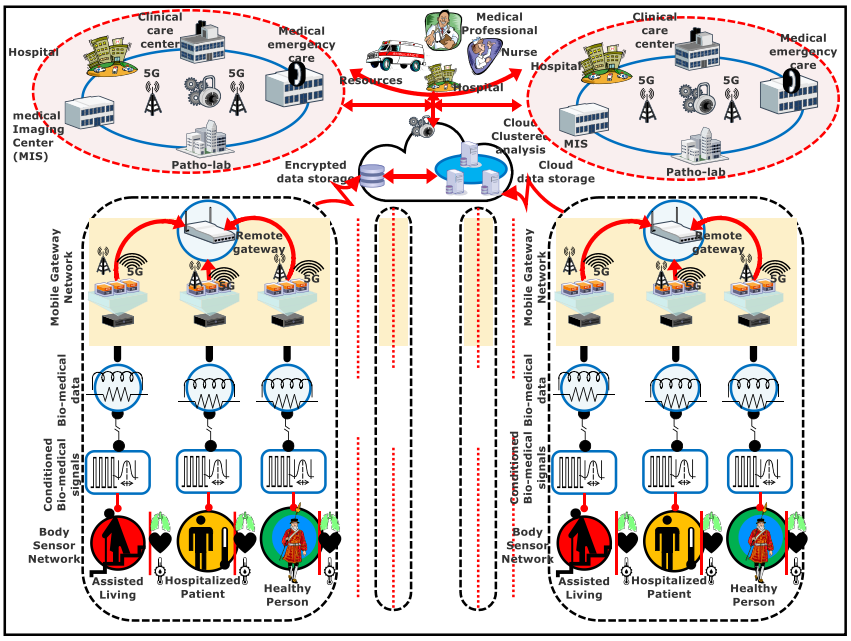

Fig. 1. Overall architecture of the IoMT framework for connected healthcare infrastructure.

1.1 Motivation and Objectives

The authors chosen an attribute based access control model proposed by Zhang et al. [14] for threat analysis. In their model [14], it was observed that, the scheme can preserve the receiver's attribute privacy through ciphertexts that hide the information. However, the adversary can capture the traffic through side channel attack and cold boot attack crypt-analysis models. The adversary can easily manipulate (edit/delete/modify) the captured data through an insecure channel. Authors, assume that the side channel attack is capable enough to steel the RFID card data and data from EHS database. In addition, during the upload time of access control scheme, the sensitive information is at a higher risk of being stolen by intruders.

Under the presumption of aforementioned threat model, authors proposed a highly secured authentication and access control model for device/data that addresses the issues enlisted above. With this proposal, authors have also considered several important other challenges such as emergency handling, ownership transfer, and access control security. In addition, the sensors used in such medical applications are limited in terms of operating capabilities. As a result, lightweight access control solution must be the possible solution to address these issues and the same is implemented n proposed protocol.

1.2 Protocol Requirements

This section gathers the access control and ownership transfer protocol requirements in terms of three parameters such as functionalities, security and privacy concerns. Here, *Fr* denotes the Functional requirements, *Sr* denotes the Security requirements and *Pr* denotes the privacy requirements.

(Fr0) Access control functionality: This functionality enables all legitimate users to access the healthcare device and data from the allocated space in EHS only. This is carried out by defined access control policies in EHS.

(Fr1) Energy optimization: The proposed scheme is lightweight in nature as it requires less computational and storage spaces and thus it uses the resource constrained sensors utilizes less energy by making the system energy efficient.

(Fr2) Break-glass access control mechanism: The proposed mechanism utilizes te break-glass feature, which is invoked during emergency situations and bypasses the regular access control phases to provide immediate access for the emergency response team members.

(Fr3) Ownership transfer mechanism: Accessibility to patient data can be vertically transferred to another medical professional as and when required. The same can be applied from the patient end as well. Accessibility to doctors can be transferred from one doctor to another doctor as and when patent wishes.

(Sr0) Policy based Authentication: The credibility of each user is verified centrally by attribute based authentication scheme. This attribute is nothing but a session key

generated by the EHS upon the initial request by user. The same session key will be used in allocating the access rights.

(Sr1) Data confidentiality: Only authorized data handlers are entitled to access the data. The data handlers may be the medial practitioners, hospital administrators or the patient.

(Sr2) Information integrity: The data manipulations from unauthorized accesses are strictly prohibited and must the alterations are easily identifiable using back-tracing and efficient cryptographs.

(Sr3) Data availability: All the biomedical data captured by data acquisition system (DAQ) must be timely available to see either by medical practitioners or by patients.

(Pr0) System entity privacy preservation: An intruder must not be able to see the private information of the doctors as well as patients.

(Pr1) User Non-tractability: No hacker or horizontal user will be able to trace the other user information using back tracking methods.

(pr2) Preservation of old owner privacy: Once the ownership of patient information is transferred to new doctor, he/she will not be able to violate the security goals in order to look into the private information of old users.

(pr3) Preservation of new owner privacy: When an ownership is revoked to old owner, the old owner should not be able to access the communication details of current owner.

1.3 Existing work

In this section, the authors describe the holistic literature review of the selected articles that addresses the overall picture of security goals and approaches in healthcare infrastructure. The criteria used in selecting article for literature review is, the policy and attribute based access control mechanisms. In the same way, there are several researchers who proposed numerous security protocols for e-health security recently [15-17]. These articles are mainly focusing to provide solution for shared key problem. The key is shared between sensor, patient and server. Similarly, He et al. [18] provided a deep review on various authentication schemes that are mainly based on Elliptic-curve cryptography (ECC). The authors also demonstrated the unsuitability of these authentication schemes for healthcare scenarios due to their hardbound nature of vulnerabilities to the most common attacks such as insider and side channel attacks.

Le et al. [15] proposed an ECC based lightweight mutual authentication scheme for access controlling of healthcare information. The scheme was seemingly resilient towards the common attacks such as Denial of Service (DoS) and insider attack. Further, Kumar et al. [16] proposed a similar asymmetric-cryptography based access control scheme using two factor authentication process. The authentication scheme is mutual between EHS, user and medical sensor device. In [16], the authors described the security vulnerabilities of [15] in an efficient way. Although, the asymmetric cryptography employment in their scheme is interesting, however, it does not describe the additional feature such as ownership transfer scheme and emergency break-glass access control scheme. Eventually, Chang et al. [18] proposed an authentication scheme for

biometric based healthcare applications that enables its users to access the data/ device using a single-way hash functions. This scheme provides salient features that are resistant towards collision attacks. However, this scheme is vulnerable to many attacks such as insider attack and cold boot attack. In order to enhance this scheme, Das et a. [19] proposed a symmetric cryptography based authentication scheme for access control purpose. A symmetric secrete key is shared between both user and server in order to protect the multi hop communication between them. However, all the aforementioned literature does not support the ownership transfer and break-glass authentication schemes.

2 Conceptual framework of proposed architecture

This section provides the brief overview of implementation and overall scheme is discussed with the relevant diagrams. The proposed architecture diagram is depicted in the fig. 2. As shown in fig. 2, the overall architecture is categorized in three entities namely patient entity (Pi), healthcare professional entity (Hi) and electronic healthcare server (EHR) entity (Si). Patient entity is made of numerous healthcare sensor nodes attached on patient body. EHR entity is made of servers, base stations that connect user devices to the server and cloud computing infrastructure. Similarly, healthcare professional entity comprised of doctors, nurses, chemist and lab technicians. The set of Hi and Pi must be registered in EHR as per their service plans through the radio cards.

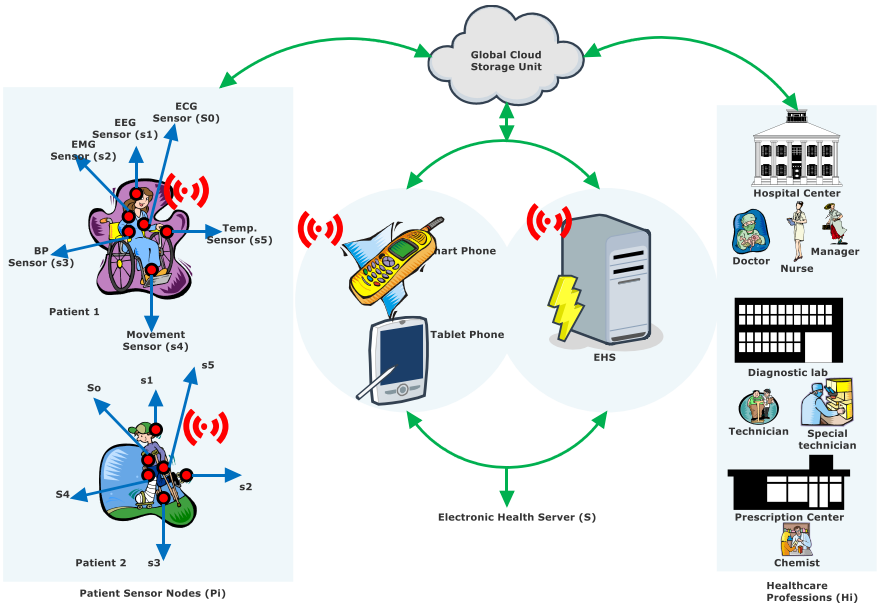

Fig. 2. Proposed framework of Multi-factor authentication scheme in Access Controlling applications

The proposed framework will be implemented in the following phases.

2.1 Enrollment phase (E):

During this phase, user (Hi) (doctor) will be able to register for the e-health services. Following steps are followed by the Hi in order to register for the authentication services.

(E0): The healthcare user (Hi) uses his/her preassigned identity number Ide_1 and user generated access credential (Ac_i) in order to generate a random number x_1. The healthcare professional then extracts the biometric information for computing the same random number. The random number is generated by the accumulative concatenation operation (||).

(E1): After receiving the enrollment request from the medical user, the EHS invokes its master key for computing intermediate access key M.

(E2): Upon the reception of smart radio card by healthcare professional, the data holder is computed and stored in the smart radio card. Thus the enrollment of user to the system is carried out. Therefore, the smart RFID card has the details such as Biometric trait that belongs to the medical user and related flags.

2.2 Sign-In Phase (S):

During Sign-In phase, if Hi needs to access the patient details from the medical server, he/she inserts the smart card in the dedicated hardware terminal and continues in Sign-In phase as follows. To be specific, the doctor enters his/her user id (U_{ID}) and ($Pw_{i)}$ in the portal and extracts the biometric details (BM_i) by means of biometric reading sensor terminal. Now, that the server performs the computation of matching biometric data and rejects the user from sign-in process if it doesn't find a match. In other words, the accepted card data will be stored in server along with the time stamp.

2.3 User authentication and Key exchange phase (AKE):

During this phase the doctor executes the following steps as part of user verification and proving legitimacy towards the EHS. Upon successful authentication, the Hi shares the shared secrete key to all its entities as and when required.

AKE0: During this step, server receives the message (msg1) from the sign-in phase, then server compute ΔT. It is the normalized difference between T1 and T2. If ΔT is greater than |T1-T2|, then server suspend the connection. Otherwise the consequent elements are computed from the database.

AKE1: During this step, the output from the previous steps are considered as elementary components in to drive the AKE1. The msg2 validity is sequentially checked with allotted timestamp. If T2 is found out of margin, then the server abrupt the secured

connection else relation member (Pj) maps its corresponding memory value (Mj) to the specific user.

AKE2: During this step, the msg3 is received and checked against its validity with the help of associated timestamp. If timestamp |T3-T4| produces the greater results than the original delta, then the connection is aborted by the server, otherwise the server extracts the session key and share across its entities.

2.4 Transferring ownership from one user to other (OTP):

The objective of this phase is to transfer the target sensor data access rights from one legitimate user to another. After few steps getting executed, the fresh user will have an access to the allocated sensor data and the previous user will be deprived from the access rights. Proposed scheme also provides an access revoking capability, where previous user can resume his access rights back.

OTP0: A new medical professional (H2) who wants to replace an access right with already existing user, he\she inserts the smart card into the device terminal and provide the acquired credentials from the hospital administration. Then H2 retrieve his/her biometric data $BM2^{'}$ by the help of biometric device. Now the sever calculates the biometric feature difference ($Y2^{'}$). IF $Y2^{'}$ is observed as a match found from the server then it continues, else server aborts the secure communication.

OTP1: After the OTP0, the H1 user will receive the deregistration notification and H1 user details are still saved in EHS in order to have the future revocation process if required. This step is important since the deregistration process is crucial in any database services. After this the new user will have the access rights to the target sensor data from electronic health server.

3 Crypt analysis of the proposed scheme

In this session, authors produce the informal attack reports for the proposed scheme. The security analysis is partially based on the Dolev security model [20].

3.1 Theft card threat attack:

In this attack, if the user loses his/her smart card, he intruder need to acquire the essential parameters from the non-tamperable electronic card. However, the card cannot have the user ID and PWi. Therefore, during the absentia of these credentials, the adversary cannot calculate the real-time communicative messages in order to establish the new connection request with EHS. In addition, the hash function used in implementing the cards are irreversible. Meaning, using one side of the function equator, it’s not possible

to guess the other part. Hence the card has the standard robust embedded encryption. Hence, the proposed scheme is secure against the stolen card attack

3.2 Offline password supposition attack

Generally, in any communication system, if an adversary finds a cryptographically contaminated message packet that has the information about all the essential parameters except the user ID and password details, he/she will be easily able to guess the password using dictionary attack model. In the proposed model, all the parameters are additionally encrypted by biometric details. Therefore, using dictionary attack an adversary cannot guess the password details.

4 Conclusion

Nowadays, healthcare IoT systems are changing the traditional ways of medical treatment and diagnosis of chronic diseases. However, these systems are facing the challenges in implementing phase such as secure communication, authentication of legitimate users at server level etc. The obvious reason for such challenges are resource limitations and wireless network vulnerabilities. In this paper, authors presented a unique way of authenticating system user and key agreement challenges are addressed with the help of access control mechanism. The major contribution lies in creating ownership transfer strategy. Authors evaluated the scheme with security analysis and observed the better efficiency in terms of resiliency towards most common attacks such as insider attack and cold boot attacks formally and theft card threat attack and offline password supposition attack informally. On the other hand, proposed framework overcomes the security gaps of existing authentication and access control schemes. In order to avoid the existing mistakes, we propose a formal and informal security analysis, that ensures the resistance towards most common IoT attacks such as insider attack, denial of distributed service (DDoS) attack and traceability attacks.

References

1. Hamidi, Hodjat. "An approach to develop the smart health using Internet of Things and authentication based on biometric technology." Future generation computer systems 91 (2019): 434-449.
2. Hossain, Mahmud, SM Riazul Islam, Farman Ali, Kyung-Sup Kwak, and Ragib Hasan. "An Internet of Things-based health prescription assistant and its security system design." Future generation computer systems 82 (2018): 422-439.
3. Yang, Geng, Li Xie, Matti Mäntysalo, Xiaolin Zhou, Zhibo Pang, Li Da Xu, Sharon Kao-Walter, Qiang Chen, and Li-Rong Zheng. "A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box." IEEE transactions on industrial informatics 10, no. 4 (2014): 2180-2191.

4. Gope, Prosanta, and Tzonelih Hwang. "BSN-Care: A secure IoT-based modern healthcare system using body sensor network." IEEE Sensors Journal 16, no. 5 (2015): 1368-1376.
5. Yeh, Kuo-Hui. "A secure IoT-based healthcare system with body sensor networks." IEEE Access 4 (2016): 10288-10299.
6. Wu, Taiyang, Fan Wu, Jean-Michel Redouté, and Mehmet Rasit Yuce. "An autonomous wireless body area network implementation towards IoT connected healthcare applications." Ieee Access 5 (2017): 11413-11422.
7. Dimitrov, Dimiter V. "Medical internet of things and big data in healthcare." Healthcare informatics research 22, no. 3 (2016): 156-163.
8. Catarinucci, Luca, Danilo De Donno, Luca Mainetti, Luca Palano, Luigi Patrono, Maria Laura Stefanizzi, and Luciano Tarricone. "An IoT-aware architecture for smart healthcare systems." IEEE Internet of Things Journal 2, no. 6 (2015): 515-526.
9. Camara, Carmen, Pedro Peris-Lopez, and Juan E. Tapiador. "Security and privacy issues in implantable medical devices: A comprehensive survey." Journal of biomedical informatics 55 (2015): 272-289.
10. Yang, Yang, Ximeng Liu, and Robert H. Deng. "Lightweight break-glass access control system for healthcare Internet-of-Things." IEEE Transactions on Industrial Informatics 14, no. 8 (2017): 3610-3617.
11. Rani, Shalli, Syed Hassan Ahmed, Rajneesh Talwar, Jyoteesh Malhotra, and Houbing Song. "IoMT: A reliable cross layer protocol for internet of multimedia things." IEEE Internet of things Journal 4, no. 3 (2017): 832-839.
12. Jan, Mian Ahmad, Muhammad Usman, Xiangjian He, and Ateeq Ur Rehman. "SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT." IEEE Internet of Things Journal 6, no. 2 (2018): 1576-1583.
13. Rahmani, A. M., Gia, T. N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 78, 641-658.
14. Zhang, Yinghui, Dong Zheng, and Robert H. Deng. "Security and privacy in smart health: Efficient policy-hiding attribute-based access control." IEEE Internet of Things Journal 5, no. 3 (2018): 2130-2145.
15. Le, Xuan Hung, Murad Khalid, Ravi Sankar, and Sungyoung Lee. "An efficient mutual authentication and access control scheme for wireless sensor networks in healthcare." Journal of Networks 6, no. 3 (2011): 355.
16. Kumar, Pardeep, Sang-Gon Lee, and Hoon-Jae Lee. "E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks." Sensors 12, no. 2 (2012): 1625-1647.
17. Y.-F. Chang, S.-H. Yu, D.-R. Shiao, A uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care, J. Med. Syst. 37 (2) (2013) 9902, http://dx.doi.org/10.1007/s10916-012-9902-7.
18. Das, Ashok Kumar, and Adrijit Goswami. "A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care." Journal of medical systems 37, no. 3 (2013): 9948.
19. He, Debiao, and Sherali Zeadally. "An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography." IEEE internet of things journal 2, no. 1 (2014): 72-83.
20. Dolev, Danny, and Andrew Yao. "On the security of public key protocols." IEEE Transactions on information theory 29, no. 2 (1983): 198-208.