CCET JOURNAL OF SCIENCE AND ENGINEERING EDUCATION
(ISSN 2455-5061) *Vol. - 3, Page-25-28, Year-2018*

A Review: Security of IOT Based Healthcare System

Kiran Dewangan*, Mina Mishra**

Assistant Professor, Electronics & Telecommunication, Bhilai Institute of Technology, Durg, CG, India,* ***kiran.dewangan@bitdurg.ac.in*

Associate Professor, Electronics & Telecommunication, Christian College of Engineering & Technology, Bhilai, CG, India,* ***minamishraetc@gmail.com

Abstract

Health care is one of the most important application areas of IoT. It provides opportunities to several medical applications such as mobile and remote health monitoring. Recent advances in information and communication technologies and embedded systems have given rise to a new technology: Internet of Things (IoT). Internet of Things (IoT) refers to a recent paradigm that has rapidly gaining ground in the area of modern wireless telecommunications. IoT is then a new technological trend joining new computing and communications paradigms. IoT enables people and objects in physical world as well as data and virtual environments to interact with each other, hence realizing smart environments such as: smart transport systems, smart cities, smart healthcare, and smart energy as part of a prosperous digital society. Intelligence algorithms analyze the m-health data in real-time to identify certain patterns and raise different alert levels such as normal, cautious, emergency, etc., depending upon the condition of the observed patients. In IoT-based healthcare applications, security and privacy are among major areas of concern as most devices and their communications are wireless in nature. Due to direct involvement of humans in IoT-based healthcare applications, providing robust and secure data communication among healthcare sensors, actuators, patients, and caregivers are crucial. Misuse or privacy concerns may restrict people to utilize IoT-based healthcare applications. Conventional security and protection mechanisms including existing cryptographic solutions, secure protocols, and privacy assurance cannot be re-used due to resource constrains, security level requirements, and system architecture of IoT-based healthcare systems. To mitigate the aforementioned risks, strong network security infrastructures for a short or long-range communication are needed.

.

Index Terms: *Internet of Things (IoT), Radiofrequency Identification (RFID), of Machine-to-Machine Communications (M2M), Medical Sensor Network (MSN), and Internet Protocol (IP).*

1. Introduction

The Internet of Things Internet of Things (IoT) refers to a recent paradigm that has rapidly gaining ground in the area of modern wireless telecommunications. IoT is then a new technological trend joining new computing and communications paradigms. Within this new trend, there are intelligent devices that have a digital entity and are ubiquitously interconnected on a network and to the global Internet. Everyday objects may integrate intelligence and the ability to sense, interpret and react to their environment, combining the Internet with emerging technologies such as Radiofrequency Identification (RFID), real-time location and embedded sensors. The IoT concept is based on the idea of a universal presence of 'things' or 'objects', such as RFID tags, sensors, actuators, mobile phones, etc, with digital identification and addressing schemes that enable them to cooperate with neighbours in order to achieve some common goals. In the business sector, the most apparent consequences of IoT may arise in industrial automation and manufacturing, in logistics, in business or process management and in intelligent schemes for transporting people and goods. Therefore, in general, the term Internet of Things refers to any type of devices that are interconnected by means of Machine-to-Machine Communications (M2M), each of which may be identified through a unique ID and defined through a virtual representation within the Internet.

2. Objective

For the purpose of designing a secure and congestion free network, following objectives have been set:

- To emphasize on the security and privacy of the healthcare data with the help of encryption techniques.

- To control congestion in the data and study of various techniques which are helpful for maintenance and safety of the data.
- To develop network design and recovery techniques this can provide solutions for mitigating massive attacks.

3. Literature Review

1. Liu. C.H. *et. al* in 2012, proposes secure medical managerial strategies being applied to the network environment of the medical organization information system so as to avoid the external or internal information security events, allow the medical system to work smoothly and safely that not only benefits the patients, but also allows the doctors to use it more conveniently, and further promote the overall medical quality. The objectives could be achieved by preventing from illegal invasion or medical information being stolen, protecting the completeness and security of medical information, avoiding the managerial mistakes of the internal information system in medical organizations, and providing the highly-reliable medical information system. [1]

2. Paschou. M. *et. al* in 2013 uses the Internet of Things concepts in the health domain does not come without extra data and therefore a data transfer cost overheads. To deal with these overheads, novel metrics, and methods are introduced in an attempt to maximize the capabilities and widen acceptance/usage provided by the Internet of Things. Without losing its generality, the method discussed is experimentally evaluated in the paradigm of the Health domain. The focus is on the need for an overview of available data formats and transmission methods and selection of the optimal combination, which can result to reduction/minimization of costs. An analytic methodology is presented backed with theoretical metrics and evaluated experimentally. [2]

3. Ziegeldorf. J. H. *et. al* in 2013 analyzes the privacy issues in the Internet of Things in detail. To this end, this work first discuss the evolving features and trends in the Internet of Things with the goal of scrutinizing their privacy implications. Second, this work classified and examined the privacy threats in this new setting, pointing out the challenges that need to be overcome to ensure that the Internet of Things becomes a reality .[3]

4. Sawand. A., *et. al* in 2015 presented an architectural framework to describe the entire monitoring life cycle and highlight the essential service components. More detailed discussions are then devoted to {em data collection} at patient side, which we argue that it serves as fundamental basis in achieving robust, efficient, and secure health monitoring. Subsequently, a profound discussion of the security threats targeting eHealth monitoring systems is presented, and the major limitations of the existing solutions are analyzed and extensively discussed. Finally, a set of design challenges is identified in order to achieve high quality and secure patient-centric monitoring schemes, along with some potential solutions. [4]

5. Gope. P. *et. al* in 2016 highlights the major security requirements in BSN-based modern healthcare system. Subsequently, this work proposed a secure IoT-based healthcare system using BSN, called BSN-Care, which can efficiently accomplish those requirements. [5]

6. Benssalah. M.. *et. al* in 2016 highlighted the vulnerabilities of the most recent proposed protocol for TMIS in the literature and proposed attacks based on the weaknesses related to the misuse of the timestamp technique, the calculation of the reader request and tag response messages using the one-way hash function, which are not attentively scrutinized. Second, this work proposed an efficient dual RFID-TMIS mobile authentication protocol with high efficiency and security for healthcare systems. Their proposal is an improvement and extension of the protocol of Li et al., where they have proposed to associate the RFID technology with TMIS in the same authentication system to take advantages of both these two promising technologies. The performance analysis shows that our improved protocol could solve security weaknesses of the studied protocol and provide mobility, efficiency and is well suited for TMIS adoption in remote areas and low population density. [6]

7. Alamr. A. A. *et. al* in 2016 propose a new radio frequency identification authentication protocol based on elliptic curve cryptography (ECC) to eliminate these vulnerabilities. In addition, this paper have used an elliptic curve Diffie–Hellman (ECDH) key agreement protocol to generate a temporary shared key used to encrypt the later transmitted messages. In this work a new protocol achieves a set of security properties like mutual authentication, anonymity, confidentiality, forward security, and location privacy, resistance of man-in-the-middle attack, resistance of replay attack and resistance of impersonation attack.

The work have implemented the proposed protocol in real RFID system using Omnikey smartcard reader (Omnikey 5421) and NXP Java smartcards (J3A040). Implementation results shows that the proposed protocol outperform in term of time complexity as compared to other similar protocols and requires less number of operations .[7]

8. Choi. J. *et. al* in 2016 proposed a secure IoT framework to ensure an End-To-End security from an IoT application to IoT devices. The proposed IoT framework consists of the IoT application, an IoT broker and the IoT devices. The IoT devices can be deployed along a board line or a boundary of the area of IoT broker. The IoT broker manages their own devices and aggregates their sensing data. The IoT application provides users with IoT services. To use the IoT services, it needs to access to sensing data. Especially, the case of real-time healthcare services should consider intermediate security issues because medical information of patients is one of very sensitive privacy information. However, most of IoT protocols such as CoAP and MQTT have no concern about the End-To-End security; they only depended on the security of DTLS. Therefore, this paper proposed a new IoT framework to satisfy the End-To-End security feature under the CoAP communication. The proposed framework encrypts sensitive data by a symmetric encryption and an attribute-based encryption for efficiencies of communication and computation costs. In addition, each IoT device has a unique identification used as one of their attributes. Consequently, although the IoT broker is one of the intermediate nodes, it decrypts and shows data only if it satisfies all attributes. [8]

9. Ko. H. *et. al* in 2016 has presented a Secure User Profiling Structure which has the patient information including their health information. A patient and a hospital keep it at that same time, they share the updated data. While they share the data and communicate, the data can be leaked. To solve the security problems, a secure communication channel with a hash function and an One-Time Password between a client and a hospital should be established and to generate an input value to an OTP, it uses a dual hash-function. This work presents a dual hash function-based approach to generate the One-Time Password ensuring a secure communication channel with the secured key. In result, attackers are unable to decrypt the leaked information because of the secured key; in addition, the proposed method outperforms the existing methods in terms of computation cost. [9]

10. Suciu. G. *et. al* in 2016 analyzes existing components and methods of securely integrating big data processing with cloud M2M systems based on Remote Telemetry Units (RTUs) and to propose a converged E-Health architecture built on Exalead CloudView, a search based application. Finally, this work discussed the main findings of the proposed implementation and future directions. [10]

11. Sajid. A. *et. al* in 2016 helped in setting research directions for the techniques and mechanisms that are needed to address the patient's data privacy concerns in a balanced and light-weight manner by considering all the aspects and limitations of the cloud-assisted healthcare systems. [11]

12. Tahmasbi. A. *et. al* in 2016 presented a software architecture for development of healthcare systems based on pervasive computing concepts, and then models the behavior of described system. A set of solutions are then proposed to improve the design's qualitative characteristics including, availability, interoperability and performance. [12]

13. Xu. H. *et. al* in 2016 worked on a secured electrocardiogram (ECG) signal transmission scheme to prevent further injuries for patients with heart diseases from human emotional stress. This paper proposed a dynamic encryption method via biometric information among frequency spectrums of ECG signals, which can guarantee both high classification rate (>90 %) and system energy efficiency. At the same time, cooperative relays are applied for an additional spatial diversity gains. Simulation results show that the improved transmission rate and signal power capacity can lower the probability of data intercept (LPI) and detection (LPD) by taking the advantages of both temporal and spatial diversities. The network security thereby can be further improved. [13]

14. Zhang. Y. *et. al* in 2015 proposed a remote mobile health monitoring system with mobile phone and web service capabilities. It provides an end-to-end solution; specifically, (1) physiologic parameters, including respiration rate and heart rate, are measured by wearable sensors and recorded by a mobile phone which presents the graphical interface for the user to observe his/her health status more easily; (2) it

provides doctors and family members with necessary data through a web interface and enables authorized personnel to monitor the patient's condition and to facilitate remote diagnosis; and (3) it supports real-time alarming and positioning services during an urgent situation, such as a tumble or a heart attack, so that unexpected events can be handled in a timely manner. Experimental results show that the proposed system can reliably monitor the physiologic parameters and conveniently report the user's position. [14]

4. Conclusion

Security is a major concern wherever networks are deployed at large scales. IoT-based healthcare systems deal with human-related data. Although collected from innocuous wearable sensors, such data is vulnerable to top privacy concerns. In IoT-based healthcare applications, security and privacy are among major areas of concern as most devices and their communications are wireless in nature. An IP-enabled sensor in a Medical Sensor Network (MSN), for instance, can transmit medical data of patients to a remote healthcare service. In healthcare IoT, security and privacy of patients are among major areas of concern. In this regard, the authentication and authorization of remote healthcare centers/caregivers and end-to end data protection are critical requirements as eavesdropping on sensitive medical data or malicious triggering of specific tasks can be prevented . Due to direct involvement of humans in IoT-based healthcare applications, providing robust and secure data communication among healthcare sensors, actuators, patients, and caregivers are crucial.

Acknowledgement

This work would not have been possible without the support and cooperation of the management of Bhilai Institute of Technology, Durg. I am grateful to all of those with whom I have had the pleasure to work during my work.

References

[1] Chia-Hui Liu, Yu-Fang Chung, Tzer-Shyong Chen & Sheng-De Wang, 2012, The Enhancement of Security in Healthcare Information Systems, Journal of Medical System. 36, 1673–1688.

[2] Mersini Paschou, Evangelos Sakkopoulos , Efrosini Sourla and Athanasios Tsakalidis, 2013, Health Internet of Things: metrics and methods for efficient data transfer, Simulation Modelling Practice And Theory Elsevier, 1569-190X.

[3] Jan Henrik Ziegeldorf, Oscar Garcia Morchon and Klaus Wehrle, 2013, Privacy In The Internet Of Things: Threats And Challenges, Security And Communication Networks, 1002/sec.795.

[4] Ajmal Sawand, Soufiene Djahel, Zonghua Zhang and Farid Nait-Abdesselam, 2015, Toward Energy-Efficient and Trustworthy eHealth Monitoring System, China Communications.

[5] Prosanta Gope and Tzonelih Hwang, 2016, BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network, IEEE Sensors Journal, 16, NO. 5.

[6] Mustapha Benssalah, Mustapha Djeddou and Karim Drouiche, 2016, Dual cooperative RFID-telecare medicine information system authentication protocol for healthcare environments, Security And Communication Networks, 1002/sec.1665.

[7] Amjad Ali Alamr, Firdous Kausar, Jongsung Kim and Changho Seo,2016, A secure ECC-based RFID mutual authentication protocol for internet of things, Journal of Super Computing, 1,1227-016-1861-1.

[8] Jongseok Choi, Youngjin In, Changjun Park, Seonhee Seok, Hwajeong Seo and Howon Kim, 2016, Secure IoT framework and 2D architecture for End-To-End security, Journal of Super Computing, 1227-016-1684-0.

[9] Hoon Ko and MoonBae Song, 2016, A Study on the Secure User Profiling Structure and Procedure for Home Healthcare Systems, Journal of Medical System, 10916-015-0365-5.

[10] George Suciu, Victor Suciu, Alexandru Martian, Razvan Craciunescu, Alexandru Vulpe, Ioana Marcu, Simona Halunga and Octavian Fratu, 2016, Big Data, Internet of Things and Cloud Convergence – An Architecture for Secure E-Health Applications, Journal of Medical System, 0916-015-0327-y.

[11] Anam Sajid and Haider Abbas, 2016, Data Privacy in Cloud-assisted Healthcare Systems: State of the Art and

[12] Arezoo Tahmasbi, Sahar Adabi and Ali Rezaee, 2016, Behavioral Reference Model for Pervasive Healthcare Systems, Journal of Medical System, 0916-016-0632-0.

[13] Hansong Xu and Kun Hua, 2016, Secured ECG signal transmission for human emotional stress classification in wireless body area networks, EURASIP Journal on Information Security, 3635-015-0024-x.

[14] Yunzhou Zhang, Huiyu Liu, Xiaolin Su, Pei Jiang and Dongfei Wei, 2015, Remote Mobile Health Monitoring System Based on Smart Phone and Browser/Server Structure, Journal of Healthcare Engineering, Vol. 6 · No. 4 Page 717–738. Future Challenges, Journal of Medical System, 0916-016-0509-2.