Mini Review

BIOMEDICAL Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2019.16.002856

Research Issues on Data Centric Security and Privacy Model for Intelligent Internet of Things based Healthcare

Hyunsung Kim*[1,2]

[1]*Department of Cyber Security, Korea*

[2]*Department of Mathematical Sciences, Malawi*

***Corresponding author:** Hyunsung Kim, Department of Cyber Security and Mathematical Sciences, Korea

ARTICLE INFO

Received: March 21, 2019

Published: March 27, 2019

Citation: Hyunsung Kim. Research Issues on Data Centric Security and Privacy Model for Intelligent Internet of Things based Healthcare. Biomed J Sci & Tech Res 16(3)-2019. BJSTR. MS.ID.002856.

ABSTRACT

Various research works are done to design and implement Internet of things (IoT) based healthcare systems. However, there are still several open issues and challenges that are needed to be carefully addressed focused on security and privacy. Especially, data centric solutions should be focused on the intelligent IoT networks. Thereby, the purpose of this paper is to propose research direction on data centric security and privacy model for intelligent IoT based healthcare applications. The author hopes the content could guide researcher future issues and directions on their researches.

Introduction

Recently, as the information technology (IT) environment rapidly changes to the cloud, big data and Internet of things (IoT) era, there are necessity to take much thorough security management not only for storing data but also for encryption, movement, distribution and access of data. Intelligent IoT for healthcare applications has gained attention from vast research fields in recent years. The IoT connects all subjects and the healthcare system seamlessly, which requires secure data transmissions between entities regularly [1-5]. IoT healthcare sector is resourceful and the important should be more focused on security, privacy and authentication. Thereby, data-centric security and privacy strategies are becoming a major research issue because of the variety of data that is generated by the IoT environment. Data-centric security is the key to establish policies that control the access rights of data and apply appropriate security technologies to the entire life cycle of data [6-7].

According to Hewlett-Packard analysis, 70% of IoT connected devices transmit data without applying any security measures, and 6 of 10 devices use vulnerable interfaces [8]. It has been shown that there are various security and privacy vulnerabilities in IoT. In particular, intelligent IoT has the advantage of making life convenient, but privacy issues can arise by recording and using personal private data. Biometric data such as an individual's movement path, heart rate and blood pressure can be considered as highly sensitive privacy information. This paper aims to guide research issues and directions on data-centric security privacy model to overcome security and privacy limitations for realizing future intelligent IoT based healthcare service.

Discussion

IoT plays a vital role in healthcare applications. Healthcare applications should support clinical care, remote monitoring and context awareness. Furthermore, the risks of security and privacy should be removed during data collection from automatic medical data collection in the applications. There are already many researches to solve the issues [9-15]. However, they are not focused on data-centric security and privacy concerns, which are the core concerns on intelligent IoT based healthcare applications.

Intelligent IoT should be capable of collecting and sharing data from interconnecting billions and trillions of heterogeneous objects through Internet. The data privacy and security are the significant open issues in the intelligent IoT based healthcare applications. Especially, data privacy is crucial in the context of IoT based

healthcare, which acquires data from IoT devices. Figure 1 shows a conceptual diagram of data-centric security and privacy model for intelligent IoT. To design a very effective and successful data-centric security and privacy model for healthcare applications, there are a lot of works to be done. We would like to suggest following some research issues and directions, which could be performed sequentially or separately.

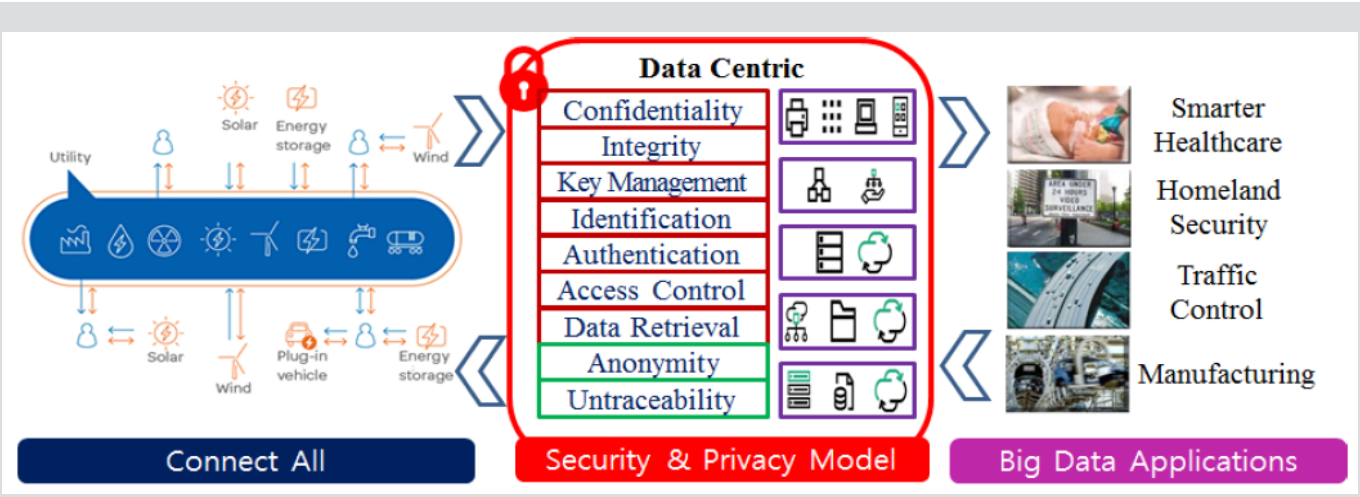

Figure 1: Conceptual diagram of data-centric security and privacy model for intelligent IoT.

Deriving Data-Centric IoT Features and Characteristics

Data-centric security for intelligent IoT and technical features and characteristics for privacy should be derived after analyzing various standards on IoT and healthcare. Although researches on the characterization of entities in the intelligent IoT environment have been presented, there is no research on prototype development for deriving data-centric features and characteristics.

Definition of Security and Privacy Threat Model

It is necessary to define a data-centric security and privacy threat model by analyzing the various threat models and especially considering the intelligent IoT features and characteristics. It should be together with building testbed based on Arduino, Raspberry Pi, or any latest intelligent IoT devices to guild a prototype of a real experimental environment of the intelligent IoT based healthcare.

Developing Data Centric Security and Privacy Model: It is very difficult to maintain the security and privacy of data collected in the IoT environment and to control users with access rights from the collection phase to the consumption phase. In particular, since the intelligent IoT environment can integrate data that has not been aggregated at all, development of data-centric security and privacy model that considers intelligent IoT features and characteristics is a very important issue that has not yet been attempted.

Designing Data Centric Access Control Scheme: A new access control scheme should be developed based on attribute based encryption. The scheme should minimize sensitive data exposure through least privilege access and should provide privilege user control based on hierarchical key management technique.

Devising homomorphic encryption-based data retrieval technique: Secure and lightweight homomorphic encryption technique should be developed. That should provide data confidentiality and privacy while providing data-centric confidentiality and privacy.

Research on Data Centric Anonymity and Untraceability Techniques: In the intelligent IoT environment, lightweight techniques that can provide conditional anonymity and traceability. They should eliminate the per-session connectivity and suggest selective anonymity by considering the privileges of data users. In the upcoming eras, intelligent IoT based healthcare will be more and more applications because of its widespread adoption of IoT. Security and privacy provision should be the core part for the success of the intelligent IoT based healthcare applications.

Conclusion

Intelligent IoT based healthcare applications have been becoming an interesting field in the medical industry and research. However, the IoT healthcare is resourceful and the most important aspect is security and privacy. This paper gives a brief future research issues focused on data-centric security and privacy model for the intelligent IoT based healthcare applications. The contents would be useful for engineers, researchers, policy makers, health professionals and healthcare technicians for the better understanding of the contemporary research directions and issues.

Acknowledgement

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

References

1. Mrinai M Dhanvijay, Shailaja C Patil (2019) Internet of Things: A survey of enabling technologies in healthcare and its applications. Computer Networks 153: 113-131.
2. LD Stefano, I Rea, P Dardano, M Balestrieri, G Palmieri, et al. (2019) Newer Technologies, Better Healthcare. Biomed J Sci & Tech Res 14(4).
3. Mostafa Rahimnejada (2019) MFC-Based Biosensors Known as an Integrated and Self-Powered System. Biomed J Sci & Tech Res 14(2).
4. Debajani Mohanty, Rajul Rastogi (2018) From Womb to Graveyard: Blockchain in Healthcare. Biomed J Sci & Tech Res 9(4).
5. Parag Shah (2018) Single Healthcare Portal - A Game Changer for the Healthcare Industry. Biomed J Sci & Tech Res 7(3).
6. Sung Woon Lee, Thokozani Vallent, Hyunsung Kim (2018) Security and Privacy Measures on Data Mining for Internet of Things. International Journal of Applied Engineering Research 13(14): 11648-11652.
7. Hyunsung Kim (2017) Data Centric Security and Privacy Research Issues for Intelligent Internet of Things. ICSES Interdisciplinary Transactions on Cloud Computing, IoT, and Big Data 1(1): 1-2.
8. (2014) HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack.
9. Hyunsung Kim (2014) Freshness-Preserving Non-Interactive Hierarchical Key Agreement Protocol over WHMS. Sensors 14(12): 23742-23757.
10. Kambombo Mtonga, Eun Jun Yoon, Hyun Sung Kim (2017) Authenticated Privacy Preserving Pairing-Based Scheme for Remote Health Monitoring Systems. Journal of Information Security 8(1): 75-90.
11. Haomiao Yang, Hyunsung Kim, Kambombo Mtonga (2015) An efficient privacy-preserving authentication scheme with adaptive key evolution in remote health monitoring system. Peer-to-Peer Networking and Applications 8(6): 1059-1069.
12. Donghwan Ku, Hyunsung Kim (2018) Enhanced User Authentication with Privacy for IoT-Based Medical Care System. International Journal of Computer Theory and Engineering 10(4):125-129.
13. Balasubramanian Prabhu Kavin, Sannasi Gandapathy (2019) A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications 151: 181-190.
14. Hui Tian, Fulin Nan, Chin Chen Chang, Yongfeng Huang, Jing Lu, et al. (2019) Privacy-preserving public auditing for secure data storage in fog-to-cloud computing. Journal of Network and Computer Applications 127: 59-69.
15. Mohammad Wazid, Ashok Kumar Das, Jong Hyouk Lee (2019) User authentication in a tactile internet based remote surgery environment: Security issues, challenges, and future research directions. Pervasive and Mobile Computing 54: 71-85.

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2019.16.002856

Hyunsung Kim. Biomed J Sci & Tech Res