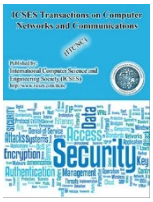
Editorial

ICSES Transactions on Computer Networks and Communications (ITCNC)

Journal Homepage: http://www.i-cses.com/itcnc/



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

Hyunsung Kim[1,2,ǂ,*]

[1] Department of Cyber Security, Kyungil University, Kyungbuk, Korea
[2] Department of Mathematical Sciences, University of Malawi, Zomba, Malawi
[ǂ] This research was supported by NRF funded by the Ministry of Education (NRF-2017R1D1A1B04032598)

* Corresponding Author: kim@kiu.ac.kr

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.

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.

- 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

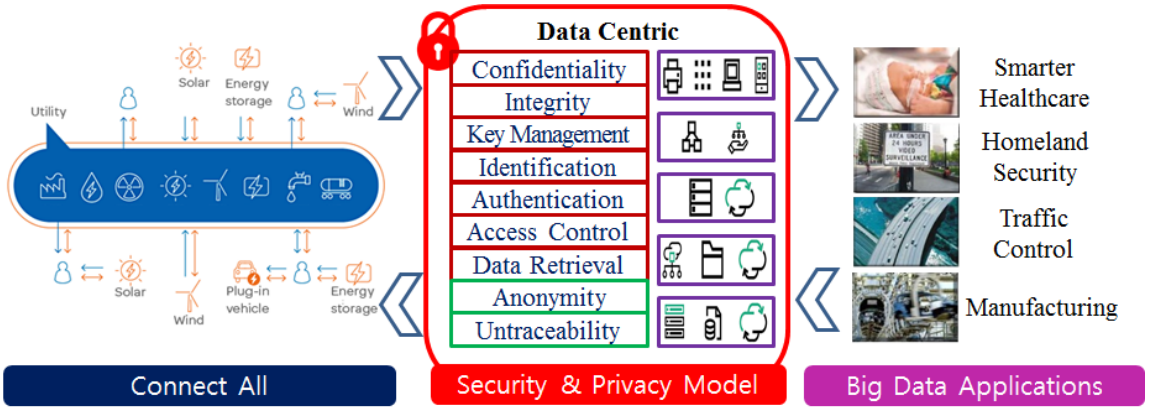


Figure 1. Conceptual diagram of data-centric security and privacy model for intelligent IoT.

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.

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.

With regards,
Prof. Hyunsung Kim, *PhD*
2nd May, 2019

REFERENCES

[1] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Computer Networks*, vol. 153, pp. 113-131, 2019.

[2] M. Nguyen and T. N. Hyu, "Wireless Power Transfer: A Survey of Techniques, and Applications on Communication Networks," *ICSES Transactions on Computer Networks and Communications*, vol. 4, no. 4, pp. 1-5, 2018.

[3] M. Nguyen, H. Nguyen and K. Teague, "Wavelet-based Energy Efficient Data Collection Algorithm in Wireless Sensor Networks," *ICSES Transactions on Computer Networks and Communications*, vol. 4, no. 2, pp. 3-10, 2018.

[4] P. Shah, "Single Healthcare Portal – A Game Changer for the Healthcare Industry," *Biomed J Sci & Tech Res*, vol. 7, no. 3, MS.ID.001515, 2018.

[5] E. Babulak, "Cyber Security Solutions and Challenges in Ultrafast Internet Connecting Ultra-Smart Computational Devices," *ICSES Transactions on Computer Networks and Communications*, vol. 3, no. 1, pp. 1-2, 2017.

[6] S. W. Lee, T. Vallent and H. Kim, "Security and Privacy Measures on Data Mining for Internet of Things," *International Journal of Applied Engineering Research*, vol. 13, no. 14, pp. 11648-11652, 2018.

[7] H. Kim, "Data Centric Security and Privacy Research Issues for Intelligent Internet of Things," *ICSES Interdisciplinary Transactions on Cloud Computing, IoT, and Big Data*, vol. 1, no. 1, pp. 1-2, 2017.

[8] HP News, "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," https://www8.hp.com/ch/de/hp-news/press-release.html?id=1744676, July 29, 2014.

[9] H. Kim, "Freshness-Preserving Non-Interactive Hierarchical Key Agreement Protocol over WHMS," *Sensors*, vol. 14, pp. 23742-23757, 2014.

[10] K. Mtonga, E. J. Yoon and H. S. Kim, "Authenticated Privacy Preserving Pairing-Based Scheme for Remote Health Monitoring Systems," *Journal of Information Security*, vol. 8, no. 1, pp. 75-90, 2017.

[11] H. Yang, H. Kim and K. Mtonga, "An efficient privacy-preserving authentication scheme with adaptive key evolution in remote health monitoring system," *Peer-to-Peer Networking and Applications*, vol. 8, no. 6, pp. 1059-1069, 2015.

[12] D. Ku and H. Kim, "Enhanced User Authentication with Privacy for IoT-Based Medical Care System," *International Journal of Computer Theory and Engineering*, vol. 10, no. 4, pp. 125-129, 2018.

[13] B. P. Kavin and S. Gandapathy, "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications," *Computer Networks*, vol. 151, pp. 181-190, 2019.

[14] H. Tian, F. Nan, C.-C. Chang, Y. Huang, J. Lu and Y. Du, "Privacy-preserving public auditing for secure data storage in fog-to-cloud computing," *Journal of Network and Computer Applications*, vol. 127, pp. 59-69, 2019.

[15] M. Wazid, A. K. Das and J.-H. Lee, "User authentication in a tactile internet based remote surgery environment: Security issues, challenges, and future research directions," *Pervasive and Mobile Computing*, vol. 54, pp. 71-85, 2019.