Development of Secure IoT System based on Secret Sharing

Hiroyuki Dekihara

The Faculty of Economic Sciences
Hiroshima Shudo University
Hiroshima, Japan 731–3195
Email: hdekihar@shudo-u.ac.jp

***Abstract*—In Cyber Physical Systems based on sensor networks, one of the important requirements is that the data in the system are protected from a variety of incidents. In this study, a secure IoT system is proposed for Cyber Physical Systems using sensor networks, and a prototype was developed on the input side. The novel concept of the proposed method is to apply encryption at the physical layer into the IoT system from input processing to output processing. The system is based on Shamir Secret Sharing, which is a type of encryption using distributed processing. The encrypted data in the system would maintain confidentiality even when a part of the data is browsed by a third party by unauthorized access of a malicious third person or by human operator error. In addition, it is possible for a user to control accessibility by holding key information of the encryption. The prototype system on the input side was created by an Arduino, a Sakura LTE module, and the Sakura IoT Platform.**

Keywords–Internet of Things; Network security; Wireless sensor networks; Encryption; Shamir Secret Sharing.

I. Introduction

In the Fourth Industrial Revolution [1], it is expected that Cyber Physical Systems (CPSs) connecting the real world and virtual world will serve as one advanced system. Usually, the CPS gathers information from the real world using wireless sensor networks. Of course, the CPS must protect the gathered data from a variety of incidents, such as an attack by a malicious third person, a leak due to human error, etc [2], [3]. The objective of this research is to develop a new secure IoT system for the CPS, and the final goal is to proposal the encrypted processes from input to output in CPS, in other words from user side to operator side. The system is based on secret sharing [4], [5], which is a type of encryption using distributed processing. The encryption has been applied at the physical layer into the IoT system from input processing to output processing. The encrypted data by secret sharing can be decrypted when there are more data than the threshold number. Therefore, the encrypted data in the system would be kept confidential even when a part of the data smaller than the threshold number is browsed by a third party by unauthorized access of a malicious third person or by human operator error. In addition, it is possible for a user to control accessibility by holding key information of the encryption. In this paper, the prototype system on the input side was created using an Arduino [6], a Sakura LTE module, and the Sakura IoT Platform [7]. From the prototype, it was verified that the algorithm of Secret Sharing was performed on Arduino, the two paths were connected by Sakura LTE modules, and Sakura LTE modules and a SD card module were performed on a single Arduino together.

In Section 2, the schemes of the proposed system and the prototype system of the input side are explained. Finally, a brief conclusion is presented in Section 3.

II. Proposed System

In this study, a secure IoT system was developed and is proposed for CPSs using wireless sensor networks. In this section, the scheme and prototype of the proposed system are described.

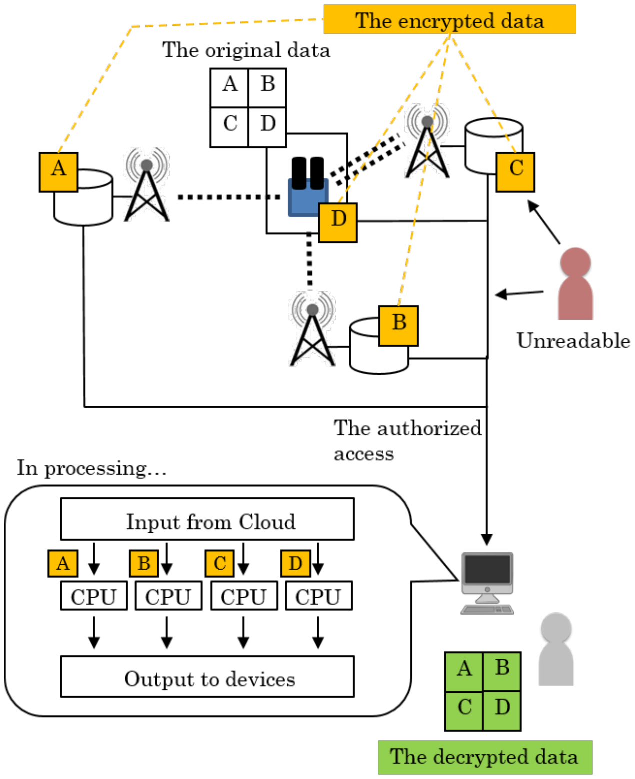

Figure 1. The scheme of the proposed system.

A. Scheme

The scheme of the proposed system is shown in Figure 1. The IoT devices in the CPS receive a signal or stimulus (i.e., heat, light, pressure, motion, etc.). The received data are encrypted and divided by the secret sharing algorithm. Figure 2 illustrates an example graph in Shamir (k, n) secret sharing. Let k = 3 and n = 5 in this case. The secret is the original data, and it is encrypted and divided into five shares. A share is a set of coordinates (x, y). The secret data can be decrypted from three shares out of five. The divided data are transmitted to cloud computing via multiple routes. The key data for the decryption may be held by the IoT device (or the user side). For example, the original data received by a sensor are divided into four data points (A, B, C, and D) in Figure 1. Then the four data points are sent to cloud computing devices and stored there. In authorized access, the original data are decrypted from the four data points on each cloud computing device. The proposed system would maintain data division, even in the computing and output components, by parallel processing using multiple processors and computer vision using mixed reality.

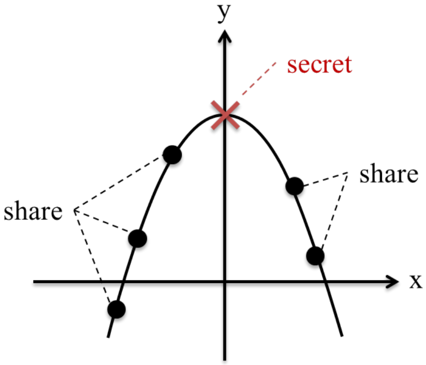

Figure 2. An example of (k, n) secret sharing.

B. Prototype System of the input side

The prototype system of the input side was created by an Arduino, a Sakura LTE module, and the Sakura IoT Platform. The Sakura IoT Platform which has been supplied by SAKURA internet Inc. is a service that has integrated the communications environment for IoT and data storage and processing systems. Figure 3 illustrates the prototype component corresponding to the dashed-line area of Figure 1. The Arduino was connected to a sensor on a breadboard by jumper wires, and had several shields mounted, such as the Sakura LTE modules and the SD card shield (shown in Figure 4). The Arduino communicated with the Sakura IoT Platform by LTE to upload data from connected sensors that were encrypted by secret sharing. The Sakura IoT Platform stored the uploaded data from the Arduino. In this step, it is possible for a user to hold key information about the encryption and to control accessibility. In the case of the prototype system, (3, 3) secret sharing was used for encryption, and the original data were divided into three shares. In other words, the original data were decryptable when all three shares were present. One share is stored on the IoT device on the user side. The Arduino connects to the Sakura IoT Platform on the Internet with a dual communication path using LTE and sends three other shares to the Sakura IoT Platform to store. The original data can be decrypted from one share on the user side and two shares on the Sakura IoT Platform. The user side was able to reject unauthorized accesses from a malicious third party. The numbers of data communication media from sensor to cloud are depend on hardware. In the case of the prototype system, it was depended on Sakura LTE modules (max 2). Moreover, SD card module could be added to the Arduino that had attached to the two Sakura LTE modules by solving duplication of used pin numbers among modules. Therefore, it is necessary to notice the duplication of Arduino's pins when the number of physical media storing or sending data of Secret Sharing will be increased.

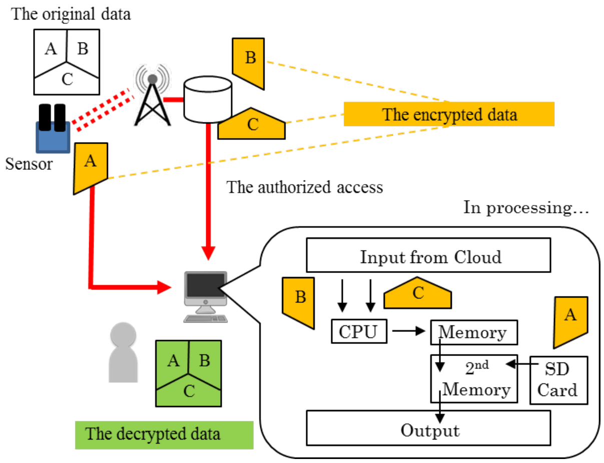

Figure 3. The prototype system of the input component.

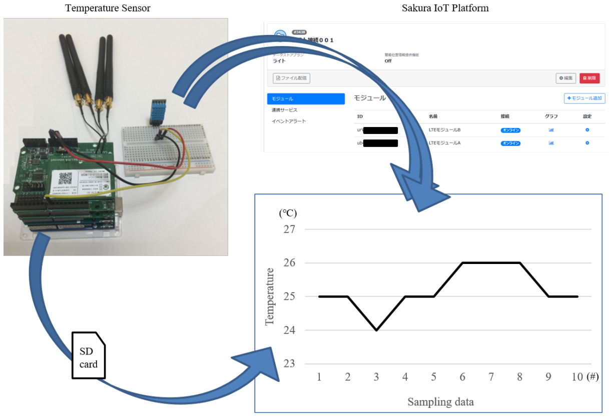

Figure 4. A result of storing data from sensor.

III. Conclusion

In this study, a secure IoT system was proposed for the CPS using wireless sensor networks, and the prototype system of the input component was created using an Arduino, a Sakura LTE module, and the Sakura IoT Platform. The system is based on secret sharing for encryption, and has been applied to encryption at the physical layer into the IoT system from input processing to output processing. It was confirmed that the original data could be decrypted from the divided shares on the IoT device and the Sakura IoT Platform. In addition, it was confirmed that the original data could not be decrypted in the case of a lacking, necessary share.

In the future, the data computing and output components will be developed. Moreover, the developed prototype system will be extended for multi-IoT platforms, adapting to the visualization and calculation of secret sharing, etc., and the data structure will be developed for the proposed system.

References

[1] R. Kenett, R. Swarz, and A. Zonnenshain, Systems Engineering in the Fourth Industrial Revolution: Big Data, Novel Technologies, and Modern Systems Engineering. Wiley, 2019.

[2] R. Gurunath, M. Agarwal, A. Nandi, and D. Samanta, “An overview: Security issue in iot network,” in 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2018 2nd International Conference on, Aug 2018, pp. 104–107.

[3] A. Assiri and H. Almagwashi, “Iot security and privacy issues,” in 2018 1st International Conference on Computer Applications Information Security (ICCAIS), April 2018, pp. 1–5.

[4] G. Blakley, “Safeguarding cryptographic keys,” in Proceedings of the 1979 AFIPS National Computer Conference. Monval, NJ, USA: AFIPS Press, 1979, pp. 313–317.

[5] A. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, Nov. 1979, pp. 612–613. [Online]. Available: http://doi.acm.org/10.1145/359168.359176

[6] “Arduino”, 2019, URL: https://www.arduino.cc/ [accessed: 2019-07-27].

[7] “Sakura IoT Platform”, 2019, URL: https://sakura.io/ [accessed: 2019-07-27].