

Common Topic-Based Key Exchange Method for Encrypted Data Transmission in IoT Network

Hyeon Ho Lee*, Won Seok Choi*, Seong Gon Choi *

* Information & Communication Engineering, Chungbuk University, Cheongju-si, Chungcheongbuk-do, Korea
 hhl9438@chungbuk.ac.kr, wschoi@chungbuk.ac.kr, sgchoi@chungbuk.ac.kr

Abstract— We propose a common Topic-based key exchange method for secure data transmission. In the recent years, with the development of artificial intelligence (AI) technology and the rapid increase of AI utilization in various fields, vast amounts of data have become necessary. Data collection using IoT devices is increasing, and in this process, data privacy and security issues are becoming an important challenge. However, existing methods require high computation, such as elliptic curve-based public key exchange methods. Therefore, we propose a simple key exchange method for encrypted data transmission in IoT environments. The proposed key exchange method ensures the security of keys by sharing common topics in advance and exchanging keys based on the topics. After that, the secured key is used to send and receive encrypted data to provide a secure channel. To confirm feasibility of the proposed method, we implemented the proposed method at the laboratory level using python scripts.

Keywords— Key Exchange, Security, Privacy, Internet of Things (IoT), Data Transmission

I. INTRODUCTION

In the recent years, rapid advances in artificial intelligence (AI) technology have led to widespread application of AI in various industries, including the Internet of Things (IoT), security, and healthcare [1]. With its ability to learn and predict patterns based on large amounts of data, AI is revolutionizing industries across the board. In the IoT environment, AI is playing an important role in providing personalized services by analyzing data from many devices in real time.

By 2030, the number of active IoT devices is expected to exceed 25.4 billion, and by 2025, 152,000 IoT devices will be connected to the Internet every minute [10]. In this environment, IoT devices will continuously collect various information such as temperature, humidity, and illumination through sensors, and these data will be stored in public institutions, enterprises, or cloud environments. The vast amount of data collected will be processed differently depending on the type of service and the user's purpose. However, privacy and security are major issues in this situation [2].

IoT devices that can communicate over a network are vulnerable to security attacks and protecting them against attacks is a significant challenge [11]. Data collected in IoT environments can contain sensitive personal information, which can lead to serious privacy breaches if not managed

securely. To ensure that data is transmitted securely, it must be encrypted before it is transmitted. One of the ways to encrypt data is to encrypt the data using a key.

In the IoT network environment, we propose a common topic-based key exchange scheme that can ensure the privacy and security of data while considering the characteristics of resources and environment. The proposed scheme is designed to enable reliable key exchange while protecting privacy based on data held in common by users. By doing so, it attempts to solve the privacy problem by performing encrypted communication based on the exchanged keys during data transmission.

This paper is organized as follows. In Section 2, we review the current state of the art by reviewing related work, and in Section 3, we describe our proposed key exchange method in detail. Section 4 implement the proposed method, and finally, Section 5 concludes the work and presents future research directions.

II. RELATED WORK

In this section, we describe recent research efforts to ensure privacy and security for the secure transmission of IoT data, including key exchange.

Chauhari and Umamaheswari addressed the security issues of IoT-based healthcare data transmission and proposed the Adaptive XOR, hashing and Encryption Key Exchange (AXHE) protocol, an adaptive XOR, hashing, cryptography-based authentication protocol for secure transmission of healthcare data. The AXHE protocol can securely add new IoT devices to a network through a two-factor registration and six-factor authentication process [3].

Chandani and Sharma proposed Secure Data Transmission Scheme (SDTS) based on Elliptic Curve Cryptography (ECC) [7], a lightweight security protocol for securing data transmission in IoT and sensor networks, which provides high security and is suitable for low-power devices. The scheme had the advantages of being simple, secure, and efficient compared to existing schemes, which made it effective in Wireless Sensor Network (WSN) and IoT environments [4].

Bhandari and K. V. B. presented an encryption model that combines symmetric and asymmetric algorithms and uses a public key server to generate an end-to-end key pair, which is then used to securely transmit data over Advanced Encryption

Standard (AES) [8], which defends against man-in-the-middle attacks [5].

Subasini and Raju proposed a lightweight encryption algorithm that combines ECC and Identity-based Encryption (IBE) to generate keys and reduces key length using the Blake2 hashing algorithm [9], making it suitable for constrained IoT environments [6].

However, the existing elliptic curve-based public key exchange method requires high computational effort. Therefore, we propose a simple key exchange method for encrypted data transmission in IoT environments that secures the security of keys by sharing common topics in advance and exchanging keys based on topics.

III. PROPOSED METHOD

In this section, we provide a detailed description of our proposed target environment and common topic-based key exchange.

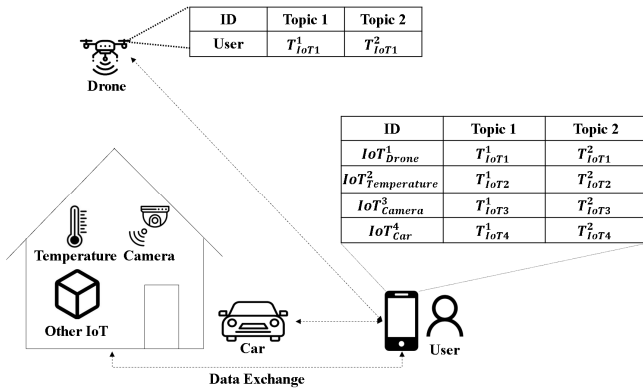


Figure 1. Target Environment

A. Target Environment

Figure 1 shows the target environment in which data collected from IoT devices is exchanged with a user's device. First, users register their IoT devices. The IoT device and the user pre-register two topics known only to them and maintain a table with data from each registered device. The registered topics can contain various metadata known only to the two parties, such as location information, status, registration time, session end time, and so on, and the two topics must be configured so that the exposure of one cannot predict the other.

IoT devices collect data in real time through sensors mounted on the device. Figure 1, the drone collects data such as images and videos in real time, and users can monitor and control the drone's status and data in real time by communicating directly with the drone with a registered device to send and receive data. At this time, the communication between the IoT device and the user device must be encrypted, and the data transmission between each device must be through a secure communication channel. This is to protect data from external attacks and ensure user privacy. In this environment, a common topic-based key exchange procedure is performed to share the keys to be used for

encryption procedures in data transmission. This procedure exchanges keys using a common topic that they have shared with each other. If the key exchange is successful, they can use the exchanged keys to encrypt each other's data and transmit data securely to protect data and ensure privacy.

B. Common Topic-Based Key Exchange Method

TABLE 1. NOTATIONS

Notation	Description
T	Topic
R	Random Number
C	Cipher text

Table 1 describes the notation used in this paper. T denotes a topic that has been shared with the communicator in advance. R is a random number to be used for encryption that each device generates when transmitting data. Then, C is the cipher text generated using R . The encryption function used in our proposed method is XOR.

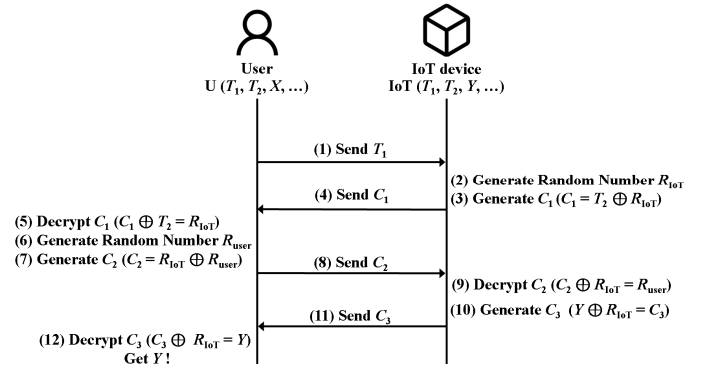


Figure 2. Key Exchange Flow of the proposed method

Figure 2 shows the flow of our proposed user and IoT device to exchange keys with a common topic and transmit encrypted data using the key. Figure 2 assumes that the user sends one of the previously shared topics to the IoT device to exchange keys for data exchange.

The procedure in Figure 2 is as following:

1) Send T_1 : The user sends the pre-registered T_1 to the IoT device.

2) Generate Random Number R_{IoT} : After receiving T_1 , the IoT device generates a random number R_{IoT} to be used as an encryption key.

3) Generate C_1 : The IoT device generates an encrypted Cipher text C_1 using the received T_1 , the mapped T_2 , and the generated random number R_{IoT} .

4) Send C_1 : Send the generated C_1 to the user.

5) Decrypt C_1 : The user decrypts the received C_1 using T_2 to compute a random number R_{IoT} .

6) **Generate Random Number R_{user} :** The user generates a random number R_{user} to be used as an encryption key.

7) **Generate C_2 :** The user encrypts the R_{IoT} obtained by decrypting C_1 to T_2 and the R_{user} generated by the user to generate C_2 .

8) **Send C_2 :** Send the generated C_2 to the IoT device.

9) **Decrypt C_2 :** The IoT device uses the received C_2 to decrypt it into R_{IoT} and compute the user's random number R_{user} .

10) **Generate C_3 :** After exchanging the random numbers, the IoT device encrypts its own random number R_{IoT} and the sample data Y to be transmitted to generate C_3 .

11) **Send C_3 :** Sends the generated C_3 to the user.

12) **Decrypt C_3 :** The user decrypts the received C_3 using the previously obtained random number R_{IoT} to obtain the sample data Y .

Algorithm1: Generate C_1

Input: T_1

Output: C_1

- 1: $T_2 \leftarrow \text{LookupInTable}(T_1)$
 - 2: **if** $T_2 = \text{null}$
 - 3: Terminate the algorithm
 - 4: **else**
 - 5: $R_{\text{IoT}} \leftarrow \text{GenerateRandomNumber}()$
 - 6: $C_1 \leftarrow T_2 \oplus R_{\text{IoT}}$
 - 7: **end if**
 - 8: **return** C_1
-

Algorithm 1 describes in detail the procedure of generating ciphertext C_1 using T_1 during the procedure in Figure 2. When the IoT device receives T_1 from the user, it checks whether there is a T_2 mapped to T_1 in its topic management table, and if there is not, it terminates the communication. if there is, the IoT device generates a random number R_{IoT} , encrypts T_2 and R_{IoT} by XOR, generates a cipher text C_1 , and sends it to the user who sent T_1 .

Algorithm2: Generate C_2

Input: C_1

Output: C_2

- 1: $R_{\text{IoT}} \leftarrow C_1 \oplus T_2$
 - 2: Update R_{IoT}
 - 3: $R_{\text{user}} \leftarrow \text{GenerateRandomNumber}()$
 - 4: $C_2 \leftarrow R_{\text{user}} \oplus R_{\text{IoT}}$
 - 5: **return** C_2
-

Algorithm 2 describes the procedure to generate C_2 when the user receives C_1 generated in Algorithm 1. After receiving C_1 from the IoT device, it decrypts it with T_2 , calculates the R_{IoT} , and updates the R_{IoT} to the table that manages the key. Then, generate the user's random number, R_{user} , and encrypt it with the R_{IoT} to generate C_2 . If the IoT device and the user do not share T_2 , the random number produced by the IoT device

and the random number computed by the user will be different, and the mutual key exchange will fail.

IV. IMPLEMENTATION

In this section, shows the results of an implementation that utilizes a python script to allow the server and client to each generate random numbers and then exchange them using a common topic.

```
Enter message: 2024-08-28 12:33:02
Enter message:
Received from Alice: LxSLFz6uZsLtROMHHYPwV0+wpM=
Alice_ran_key: 442333143471982903067265243510692799113169126035
Bob Generate random number: 25199364277078031431448448674790909778792498191
Bob Generate Cipher text: SRMd9bWwESLIX867QE4h+h6phpw=

Received from Alice: BR+LGjva+/RpLBOMHHYPwV0+wpM=
Decrypted sample data from Alice: Hello Bob!
Bob sends encrypted sample data (Hello Alice!): TAYW745q6dWXibgWXDgIo0XRA8=
```

Figure 3. Bob (user)

```
Received from Bob: 2024-08-28 12:33:02
Alice Generated Random Number: 442333143471982903067265243510692799113169126035
Alice generate cipher text: LxSLFz6uZsLtROMHHYPwV0+wpM=

Received from Bob: SRMd9bWwESLIX867QE4h+h6phpw=
Bob_ran_key is: 25199364277078031431448448674790909778792498191
Alice sends encrypted sample data (Hello Bob!): BR+LGjva+/RpLBOMHHYPwV0+wpM=

Received from Bob: TAYW745q6dWXibgWXDgIo0XRA8=
Decrypted sample data from Bob: Hello Alice!
```

Figure 4. Alice (IoT device)

Figures 3 and 4 show the python implementation of the procedure in Figure 2. Using a simple topic, it shows how to securely exchange a random number, which is an encryption key, and encrypt sample data using the key, transmit the data, decrypt the data encrypted with the other's key, and securely exchange data. As a result, Alice and Bob use the topic to show how to securely exchange random keys and send and receive encrypted data over a secure channel.

V. CONCLUSIONS

We presented a common topic-based key exchange method. We implemented the proposed method at the laboratory level to verify its behaviour. The results of the implementation confirm the applicability of the proposed method in the IoT environment.

In further study, we plan to analyze the implementation and performance based on real IoT devices.

ACKNOWLEDGMENT

This work was partly supported by the MSIT (Ministry of Science and ICT), Korea, under the Grand Information Technology Research Center support program (IITP-2024-2020-0-01462, 50%) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation). This work was partly supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2020R1A6A1A12047945, 10%). This work was partly supported by Institute of Information & Communications

Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No. RS-2024-00397979, Development of tera-level ultra-precision transmission network system technology, 40%)

*corresponding author is S.G. Choi(choisg@cbnu.ac.kr).



Hyeon Ho Lee received B.S. degree in college of Information & Communication Engineering from Chungbuk National University in 2024. He is currently pursuing the M.S. degree in Radio Communication Engineering, Chungbuk National University. His research interests include network security, blockchain, IoT.

REFERENCES

- [1] S. H. Sim and Y. S. Jeong, "Multi-Blockchain-Based IoT data processing techniques to ensure the integrity of IoT data in AIoT edge computing environments," *Sensors*, vol. 21, no. 10, p. 3515, May 2021, doi: 10.3390/s21103515.
- [2] K. Seyhan, T. N. Nguyen, S. Akleylek, K. Cengiz, and S. K. H. Islam, "Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security," *Journal of Information Security and Applications*, vol. 58, p. 102788, May 2021, doi: 10.1016/j.jisa.2021.102788.
- [3] D. A. Chaudhari and E. Umamaheswari, "A new adaptive XOR, hashing and encryption-based authentication protocol for secure transmission of the medical data in Internet of Things (IoT)," *Biomedical Engineering / Biomedizinische Technik*, vol. 66, no. 1, pp. 91–105, Aug. 2020, doi: 10.1515/bmt-2019-0123.
- [4] P. Chandani and M. Sharma, "Secure Data Transmission using Cryptography for Internet of Things and Sensor Networks Applications," *2023 2nd International Conference for Innovation in Technology (INOCON)*, Bangalore, India, 2023, pp. 1–7, doi: 10.1109/INOCON57975.2023.10101069.
- [5] R. Bhandari and K. V. B., "Enhanced encryption technique for secure IoT data transmission," *International Journal of Power Electronics and Drive Systems/International Journal of Electrical and Computer Engineering*, vol. 9, no. 5, p. 3732, Oct. 2019, doi: 10.11591/ijece.v9i5.pp3732-3738.
- [6] A. Subashini and P. K. Raju, "Hybrid AES model with elliptic curve and ID based key generation for IOT in telemedicine," *Measurement Sensors*, vol. 28, p. 100824, Aug. 2023, doi: 10.1016/j.measen.2023.100824.
- [7] D. Vidakovic, "Generating keys in elliptic curve cryptosystems," *arXiv (Cornell University)*, vol. 4, no. 1, Aug. 2013, [Online]. Available: <https://arxiv.org/pdf/1309.0245>
- [8] S. Heron, "Advanced Encryption Standard (AES)," *Network Security*, vol. 2009, no. 12, pp. 8–12, Dec. 2009, doi: 10.1016/s1353-4858(10)70006-4.
- [9] J. P. Aumasson, W. Meier, R. C. w. Phan, and L. Henzen, *The hash function BLAKE*. 2014. doi: 10.1007/978-3-662-44757-4.
- [10] B. Ivanovic, Internet of Things statistics for 2024—Taking things apart, Feb. 2024, [online]. Available: <https://dataprot.net/statistics/iot-statistics/>.
- [11] W. S. Choi, S. Y. Lee, and S. G. Choi, "Implementation and design of a Zero-Day Intrusion detection and Response system for responding to network security blind spots," *Mobile Information Systems*, vol. 2022, pp. 1–13, Apr. 2022, doi: 10.1155/2022/6743070.



Won Seok Choi received B.S. and Ph.D. degree in the College of Electrical and Computer Engineering, Chungbuk National University, Korea in 2008 and 2014 respectively. He is currently researcher in Research institute of Computer and Information Communication, Chungbuk National University. His research interests include vehicle network, energy saving network, SDN, NFV and NGN.



Seong Gon Choi received B.S. degree in Electronics Engineering from Kyungpook National University in 1990, and M.S. and Ph.D. degree from KAIST in Korea in 1999 and 2004, respectively. He is currently a professor in College of Electrical & Computer Engineering, Chungbuk National University. His research interests include V2X, AI, smart grid, IoT, mobile communication, high-speed network architecture and protocol.