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.**

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

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

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.