Secure end-to-end encryption protokol komunikasi IoT dengan kriptografi lightweight berbasis block cipher = A novel secure end-to-end encryption scheme on IoT communication protocol with lightweight cryptography based on block cipher

Agus Winarno, author

Abstrak

Keamanan data pribadi merupakan tren keamanan siber yang menyita perhatian dunia. Pemerintah, praktisi dan akademisi bersama-sama membangun keamanan data pribadi dalam berbagai sistem komunikasi, termasuk IoT. Protokol komunikasi IoT yang banyak digunakan secara luas adalah protokol MQTT. Secara default, MQTT tidak menghadirkan fitur keamanan data berupa data enkripsi. Karena itu, dalam penelitian ini dilakukan desain dan implementasi Secure End-to-End Encryption pada protokol MQTT dengan Kriptografi Lightweight berbasis Block Cipher. Protokol didesain dengan memanfaatkan skema Galantucci secret sharing dan algoritma kriptografi lightweight berbasis block cipher. Algoritma yang diterapkan antara lain adalah AES-128 mode GCM, GIFT-COFB, Romulus N1 dan Tiny JAMBU. Berdasarkan pengujian algoritma dalam protokol Secure End-to-End pada protokol MQTT pada ARM M4 dan ESP8266, diperoleh hasil bahwa algoritma Tiny JAMBU memiliki performa yang tercepat, diikuti AES-128 Mode GCM, GIFT-COFB dan Romulus N1. Pada NodeMCU, Tiny JAMBU memiliki rata-rata enkripsi 314 !" dan rata-rata waktu dekripsi 328 !". AES-128 mode GCM memiliki rata-rata waktu enkripsi 571 !" dan rata-rata waktu dekripsi 584 !". GIFT-COFB memiliki rata-rata waktu enkripsi 1093 !" dan rata-rata waktu dekripsi 1111 !". Sementara itu, Romulus N1 memiliki rata-rata waktu enkripsi 2159 !" dan rata-rata waktu dekripsi 2181 !". Pada STM32L4 discovery, Tiny JAMBU memiliki rata-rata enkripsi 81 !" dan rata-rata waktu dekripsi 85 !". AES-128 mode GCM memiliki rata- rata waktu enkripsi 164 !" dan rata-rata waktu dekripsi 165 !". GIFT-COFB memiliki rata-rata waktu enkripsi 164 !" dan rata-rata waktu dekripsi 166 !". Sementara itu, Romulus N1 memiliki rata-rata waktu enkripsi 605 !" dan rata-rata waktu dekripsi 607.
.....Personal data security is a cybersecurity trend that has captured the world's attention. Governments, practitioners and academics are jointly building personal data security in various communication systems, including IoT. The protocol that is widely used in IoT implementation is MQTT. By default, MQTT does not provide data security features in the form of data encryption. Because of this, a research was carried out on the design of Secure End-to-End Encryption MQTT with Block Cipher-Based Lightweight Cryptography. The protocol is designed by utilizing the Galantucci secret sharing scheme and a lightweight cryptographic algorithm based on a block cipher. The algorithms used include AES-128 GCM mode, GIFT-COFB, Romulus N1 and Tiny JAMBU. Our testing in the Secure End-to-End for MQTT protocol on ARM M4 and ESP8266, show that the fastest performance is produced by Tiny JAMBU, followed by AES-128 Mode GCM, GIFT-COFB and Romulus N1. Our testing in NodeMCU, Tiny JAMBU has an average encryption of 314 microsecond and an average decryption time of 328 microsecond. AES-128 GCM mode has an average encryption time of 571 microsecond and an average decryption time of 584 microsecond. GIFT-COFB has an average encryption time of 1093 microsecond and an average decryption time of 1111 microsecond. Meanwhile, Romulus N1 has an average encryption time of 2159 microsecond and an average decryption time of 2181 microsecond. On STM32L4 discovery, Tiny JAMBU had an average encryption of

81 microsecond and an average decryption time of 85 microsecond. AES-128 GCM mode has an average encryption time of 164 microsecond and an average decryption time of 165 microsecond. GIFT-COFB has an average encryption time of 164 microsecond and an average decryption time of 166 microsecond. Meanwhile, Romulus N1 has an average encryption time of 605 microsecond and an average decryption time of 607 microsecond.