

INTISARI

Implementasi Enkripsi AES-CCM dalam Kunci Rumah Pintar dengan Perangkat IoT Berbasis Wi-Fi

Oleh

Elang Wahab Setyawan
19/439105/PA/18928

Internet of Things (IoT) adalah sebuah sistem yang mengaitkan perangkat komputer dengan objek sehari-hari melalui internet yang memungkinkannya untuk mengirim dan menerima data. Serangan terhadap perangkat IoT dapat terjadi ketika penyerang dapat meretas koneksi perangkat IoT. Salah satu serangan yang umum terjadi adalah *Man-in-the-Middle* (MiM) pada sistem IoT, di mana penyerang dapat membaca dan menggunakan data yang ditransfer pada sebuah sistem IoT. Salah satu sistem IoT yang rentan adalah sistem kunci rumah pintar. *Advanced Encryption Standard* (AES) merupakan sebuah blok cipher yang dipakai dalam mode operasi *Counter with Cipher Block Chaining-Message Authentication Code* (CCM). Menggunakan AES-CCM, sebuah perangkat IoT berupa kunci rumah pintar dapat ditingkatkan keamanannya. Namun, dalam sebuah sistem IoT, juga tidak dapat dipungkiri bahwa kecepatan sistem yang baik sangatlah krusial dalam menjaga pengalaman pengguna.

Penerapan enkripsi AES-CCM pada sebuah sistem kunci rumah bertujuan untuk melindungi data yang dikirimkan dari pengguna ke perangkat kunci tanpa membuat pengalaman pengguna buruk. AES-CCM diterapkan pada gawai pengguna dan perangkat pembuka pintu, dengan gawai sebagai alat enkripsi dan perangkat pembuka pintu sebagai alat dekripsi. Transfer data akan dilaksanakan dengan gawai yang mengirim pesan terenkripsi kepada perangkat pembuka pintu. Penelitian ini membuktikan bahwa dengan AES-CCM, sebuah kunci rumah pintar dapat mengamankan kunci dari serangan MiM dengan memastikan respon sistem berada di dalam standar *real time*.

ABSTRACT

Implementation of AES-CCM Encryption in Smart Home Lock with Wi-Fi Based IoT Devices

by

Elang Wahab Setyawan
19/439105/PA/18928

The Internet of Things (IoT) is a system that connects computer devices to everyday objects via the internet, allowing them to send and receive data. Attacks on IoT devices can occur when attackers manage to hack into the IoT device connections. One of the common attacks is the Man-in-the-Middle (MiM) attack on IoT systems, where the attacker can read and utilize transferred data within an IoT system. One vulnerable IoT system is the smart door lock system. The Advanced Encryption Standard (AES) is a block cipher used in the Counter with Cipher Block Chaining-Message Authentication Code (CCM) mode of operation. Utilizing AES-CCM, an IoT device like a smart door lock can enhance its security. However, in an IoT system, it's undeniable that good system speed is crucial in maintaining user experience.

The implementation of AES-CCM in a door lock system aims to protect transmitted data from the user to the lock device without compromising user experience. AES-CCM is applied to the user gadget and the door opening device, with the gadget serving as the encryption tool and the door opening device as the decryption tool. Data transfer will occur with the gadget sending encrypted messages to the door opening device. This research demonstrates that with AES-CCM, a smart door lock can secure keys from MiM attacks while ensuring the system's response is within real-time standards.