ABSTRAK

IMPLEMENTASI ALGORITMA RIVEST CODE 4 UNTUK MENINGKATKAN KEAMANAN PADA SISTEM SMART HOME

Oleh
Bambang Fitriadi Wiansyah
wiansyahb@gmail.com

Penerapan *internet of things* memiliki banyak manfaat untuk mempermudah kehidupan manusia. Salah satu manfaat dari *IoT* adalah memantau dan mengontrol sistem mekanis, elektrik, dan elektronik yang digunakan didalam rumah. Berbagai perangkat yang terhubung ke *Internet of Things* didalam rumah tersebut membentuk *Smart Home. Smart home* memberi pengguna akses yang luas ke banyak aspek di rumah mereka, bahkan dari lokasi yang jauh. Misalnya, pengguna dapat memantau rumah mereka secara *real-time* melalui aplikasi seluler atau antarmuka web. Berbagai perangkat di dalam rumah yang terhubung ke internet dan berkomunikasi satu sama lain dengan *web server* memiliki ancaman dimana data sensor tersebut dapat diakses oleh pengguna yang tidak terautentikasi. Terutama data sensor pada *smart home* yang bersifat rahasia. Dibutuhkan suatu metode untuk mengamankan data yang ditransmisikan ke *web server*.

Algoritma kriptografi *Rivest Code 4* (RC4) merupakan salah satu algoritma kunci simetris dibuat oleh *RSA Data Security Inc* (RSADSI) yang berbentuk *stream chipper*. RC4 menggunakan panjang kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang 256 byte. Tabel ini digunakan untuk generasi yang berikut dari pseudo random yang menggunakan XOR dengan plainteks untuk menghasilkan cipherteks. Algoritma ini sangat cocok digunakan pada perangkat dengan sumber daya terbatas seperti perangkat *IoT* pada sistem *smart home*. Dengan penggunaan algoritma RC4, diharapkan dapat meningkatkan keamanan transmisi data tanpa mengurangi performasi secara signifikan.

Kata Kunci: *Rivest Code 4*, RC4, *Internet of Things*, *IoT*, Sensor, web, *server*, *real-time*. DHT11, ESP8266, NodeMCU.

ABSTRACT

IMPLEMENTATION OF THE RIVEST CODE 4 ALGORITHM TO IMPROVE SECURITY IN SMART HOME SYSTEMS

By

Bambang Fitriadi Wiansyah

wiansyahb@gmail.com

The application of the internet of things has many benefits to make human life easier. One of the benefits of IoT is monitoring and controlling the mechanical, electrical and electronic systems used in the home. Various devices connected to the Internet of Things in the house form a Smart Home. Smart homes give users extensive access to many aspects of their home, even from remote locations. For example, users can monitor their home in real-time via a mobile app or web interface. Various devices in the house that are connected to the internet and communicate with each other with a web server have the threat that sensor data can be accessed by unauthenticated users. Especially sensor data on smart homes is confidential. A method is needed to secure the data transmitted to the web server.

The Rivest Code 4 (RC4) cryptographic algorithm is a symmetric key algorithm created by RSA Data Security Inc (RSADSI) in the form of a stream chipper. RC4 uses key lengths from 1 to 256 bytes which are used to initialize a 256 byte long table. This table is used to generate the following from pseudo random which uses XOR with plaintext to produce ciphertext. This algorithm is very suitable for use on devices with limited resources such as IoT devices in Smart Home systems. By using the RC4 algorithm, it is hoped that it can increase data transmission security without reducing performance significantly.

Key Words: *Rivest Code 4*, RC4, *Internet of Things*, *IoT,* Sensor, web, *server*, *real-time*. DHT11, ESP8266, NodeMCU.