BAB I
PENDAHULUAN

1.1 Latar Belakang

Internet of Things (IoT) bukanlah hal yang baru lagi di era modern ini. 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 (Sudibyo, 2014). IoT dapat memantau pemakaian energi secara real time dalam penghematan energi, dan memantau para penghuninya. Sebagai contoh penggunaan IoT di rumah misalnya saat penghuni masuk rumah di malam hari, maka lampu akan menyala. Kemudian saat penghuni rumah akan tidur, secara otomatis akan mati. Bahkan pada pintu dapat diterapkan IoT, dimana saat pemilik rumah sedang keluar maka pintu akan terkunci secara otomatis. Berbagai perangkat yang terhubung ke Internet of Things tersebut membentuk *Smart Home* (Supendi, 2020).

Smart Home terdiri dari berbagai perangkat yang memiliki sensor berbeda yang terhubung ke internet dengan serangkaian fungsi tertentu. Meski perangkat satu dengan yang lain sangat berbeda, tapi perangkat tersebut memiliki tujuan bersama untuk menyederhanakan tugas sehari – hari penggunanya. *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 (Chang, 2019). 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 sehingga data tersebut tidak dapat dilihat oleh pengguna yang tidak terautentikasi (Alladi et al., 2020).

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. Masing – masing elemen dalam tabel saling ditukarkan minimal sekali. RC4 merupakan algoritma stream cipher yang paling cepat dibandingkan dengan algoritma stream cipher yang lain untuk masalah transmisi. Oleh karena itu algoritma ini sangat cocok digunakan pada perangkat dengan sumber daya terbatas. Dengan penggunaan algoritma RC4, diharapkan dapat meningkatkan keamanan transmisi data tanpa mengurangi performasi secara signifikan (Ariyanto, 2018). Berdasarkan latar belakang tersebut, penelitian ini mengusulkan metode keamanan kriptografi pada IoT yang ada pada smart home dimana data yang diamankan adalah data hasil pemrosesan node sensor yang ditransmisikan web server. Penelitian ini menerapkan algoritma RC4 untuk melakukan enkripsi dan dekripsi. Penulis menggunakan algoritma RC4 karena mudah di implementasikan dengan pemrosesan yang cepat pada perangkat IoT dan menggunakan memori yang sedikit sehingga sangat cocok dengan perangkat IoT dengan sumber daya yang terbatas. Penelitian ini dilakukan dengan menggunakan data yang diperoleh dari node sensor yang selanjutnya data tersebut di enkripsi. Data yang telah di enkripsi ditransmisikan ke web server untuk di dekripsi.

1.2 Ruang Lingkup Penelitian

Berdasarkan dari hasil penelitian yang telah dilakukan, maka ruang lingkup dalam penelitian ini, yaitu :

1. Penelitian ini menggunakan algoritma Rivest Code 4 sebagai enkripsi dan dekripsi.
2. Penelitian ini menggunakan NodeMCU sebagai pengolah data.
3. Penelitian ini menggunakan database pada webserver sebagai media penyimpanan.

1.3 Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah dalam penelitian ini, yaitu:

1. Bagaimana cara implementasi algoritma Rivest Code 4 pada *Smart Home*.
2. Bagaimana kinerja sistem *Smart Home* yang menerapkan algoritma Rivest Code 4.
3. Bagaimana keamanan transmisi data pada sistem *Smart Home*.

1.4 Tujuan Penelitian

Penelitian ini menerapkan metode keamanan data dengan menggunakan algoritma Rivest Code 4 untuk meningkatkan keamanan transmisi data dalam sistem *Smart Home*. Penelitian dilakukan dengan menggunakan data – data hasil pemrosesan node sensor dengan media penyimpanan web server.

1.5 Manfaat Penelitian

Manfaat dari penelitian yaitu :

1. Mengamankan data yang tersimpan pada database server *Smart Home*.
2. Meningkatkan keamanan transmisi data pada sistem *Smart Home*.

1.6 Sistematika Penulisan

Sistematika dalam penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu :

BAB I PENDAHULUAN

Dalam bab ini berisikan latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian dan manfaat penelitian.

BAB II TINJAUAN PUSTAKA

Bab ini berisikan tentang teori – teori yang berkaitan dengan “Implementasi Algoritma Rivest Code 4 untuk Meningkatkan Keamanan pada Sistem *Smart Home*”.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan apa yang akan digunakan dalam uji coba pembuatan alat, tahapan peracangan dari alat, diagaram blok dari alat, dan cara kerja alat tersebut.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi tentang implementasi alur, analisis dan pembahasan dari alur yang dirancang.

BAB V KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan dari pengujian sistem serta saran apakah rangkaian ini dapat digunakan secara tepat dan dikembangkan perakitannya.

DAFTAR PUSTAKA

LAMPIRAN