

BAB I

PENDAHULUAN

1.1. Latar Belakang

Rumah merupakan tempat tinggal dan untuk beristirahat yang harus menjamin keamanan dan kenyamanan bagi setiap pemiliknya. Biasanya rumah dilengkapi dengan fasilitas-fasilitas untuk menikmati kenyamanan di dalam dan luar rumah seperti lampu penerangan, televisi dan peralatan elektronik lain.

Ketika pemilik rumah bekerja atau berlibur sehingga rumah dalam keadaan kosong maka dari sinilah mulainya timbul permasalahan. Permasalahan ini muncul karena rumah tidak memiliki kelengkapan standar keamanan rumah. Ada beberapa situasi yang dapat menyebabkan gangguan keamanan rumah, misalnya kunci rumah rusak dan juga masalah lain akibat dari kebakaran maupun pencurian yang dapat timbul setiap saat. Sebagian besar rumah malah belum memenuhi kelengkapan keamanan standar seperti tidak ada sensor pendeteksi api, sensor pendeteksi penyusup dan lain sebagainya [1].

Saat ini, teknologi memegang peranan penting, dimana teknologi telah menjadi bagian yang tidak terpisahkan dalam kehidupan sehari-hari. Penggunaan teknologi untuk keamanan rumah dapat menekan angka kriminalitas pada masyarakat, akibat tindak kejahatan pencurian dan kebakaran [2]. Teknologi *Internet of Things* memungkinkan kita dapat mengakses dan memantau kondisi rumah secara langsung melalui aplikasi android dari jarak jauh dengan memanfaatkan jaringan internet yang tersedia. Situasi dan kondisi rumah dapat dilaporkan melalui pesan notifikasi dari aplikasi android dan jika ada asap yg terdeteksi didalam rumah maka *buzzer* akan berbunyi dan alat juga mengirim pesan ke pemilik rumah melalui notifikasi dari aplikasi android. Serta pada saat pemilik rumah berada dirumah alat tersebut dapat juga dimatikan melalui aplikasi android tersebut.

Pada penelitian ini diterapkan metode kriptografi dengan algoritma *hill cipher*. Dimana Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang

berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, integritas data dan sebagainya [3]. *Hill Cipher* termasuk kepada algoritma kriptografi klasik yang sangat sulit dipecahkan apabila dilakukan hanya dengan mengetahui berkas plaintext maupun ciphertextnya saja. Karena pada *Hill Cipher* tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks baik pada dasar enkripsi dan dekripsinya.

Untuk menjaga kerahasiaan data informasi atau perintah yang dikirimkan, peralatan keamanan rumah berbasis *Internet of Things* (IoT) dapat dilengkapi dengan metode kriptografi, seperti algoritma *hill cipher*. Setiap akses kontrol ke alat keamanan rumah, baik berupa kontrol kunci pintu maupun kontrol on/off pada sensor, dimana perintah atau informasi kontrol tersebut akan di enkripsi oleh aplikasi android sebelum dikirim ke alat. Saat perintah atau informasi tersebut dikirimkan, perintah atau informasi tersebut tidak lagi dalam bentuk aslinya tetapi sudah dalam bentuk sebuah informasi dengan karakter acak. Sehingga informasi tersebut sulit diketahui oleh orang yang berniat jahat.

Untuk mendapatkan sistem atau kelengkapan keamanan dan kenyamanan rumah yang lebih baik dari yang telah ada, maka penulis bermaksud mengangkat judul, "***Rancang Bangun Keamanan Rumah dengan Metode Kriptografi Hill Cipher Berbasis IoT (Internet of Things)***". untuk penelitian pada tugas akhir ini. Sistem keamanan rumah tersebut direncanakan digunakan untuk memonitoring rumah dari jarak jauh dan dapat mengontrol perangkat elektronik dengan menggunakan konsep IoT untuk mengurangi terjadinya tindak kriminalitas pencurian dan menghindari bencana kebakaran.

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas, beberapa rumusan masalah berikut dapat ditetapkan:

1. Bagaimana cara memberikan keamanan dan kenyamanan rumah yang lebih baik dari kondisi yang sudah ada?
2. Bagaimana cara memonitoring dan mengendalikan perangkat yang terkoneksi pada Keamanan Rumah berbasis *Internet of Things* (IoT)?
3. Bagaimana menerapkan metode kriptografi algoritma *hill cipher* ke dalam sistem keamanan rumah.

1.3. Tujuan

Adapun tujuan dari pembuatan tugas akhir ini adalah :

1. Memberikan solusi permasalahan keamanan dan kenyamanan rumah melalui penerapan teknologi berbasis IoT
2. Meneliti dan menghadirkan alat keamanan rumah berbasis IoT yang berfungsi untuk *memonitoring* dan mengendalikan perangkat elektronik yang terkoneksi pada alat tersebut.
3. Memahami penggunaan metode kriptografi dengan algoritma *hill cipher* dalam proses pengamanan data dan kontrol pada sistem keamanan rumah.
4. Menyediakan literatur praktis terkait penerapan teknologi IoT dan pengetahuan kriptografi.
5. Membangun aplikasi dan perangkat keras untuk perlindungan dan keamanan rumah.

1.4 Manfaat Penelitian

Manfaat penelitian pada tugas akhir ini adalah untuk:

1. Monitoring dan kendali sistem keamanan dari jarak jauh sebagai antisipasi tindak kriminal dan peningkatan keamanan rumah.
2. Peningkatan keamanan dan kenyamanan pemilik rumah.

3. Penerapan pengetahuan kriptografi pada peralatan keamanan rumah berbasis IoT.

1.5. Ruang Lingkup dan Batasan Masalah

Untuk membatasi ruang lingkup masalah yang akan dibahas, maka dalam penulisan tugas akhir ini maka penulis lebih menekankan pada:

1. Dasar-dasar dan penerapan IoT untuk peralatan keamanan rumah.
2. Perancangan monitoring dan kontrol dari aplikasi.
3. Penerapan kriptografi menggunakan metode algoritma *hill cipher* dalam proses pengamanan data kontrol pada peralatan keamanan rumah.
4. Penerapan dan cara kerja sensor.

1.6. Metode Penulisan

Untuk mempermudah penulisan dalam penyusunan tugas akhir maka penulis menggunakan metode-metode sebagai berikut:

1. Metode Studi Pustaka

Yaitu pengumpulan data mengenai sistem *monitoring* keamanan rumah secara *real time* yang menggunakan teknologi dari beberapa sensor yaitu: sensor asap MQ-2 sebagai pendeteksi kebakaran, sensor PIR sebagai pendeteksi pergerakan serta perangkat *solenoid door lock* yang digunakan untuk membuka/ mengunci pintu rumah.

2. Metode Perancangan

Yaitu tahap perancangan alat yang akan dibuat terdiri dari *flowchart*, perancangan rangkaian yaitu berupa bangun sistem dengan *input*, proses dan *output*.

3. Metode Observasi

Yaitu metode pengamatan terhadap alat yang dibuat sebagai acuan pengambilan informasi.

4. Metode Konsultasi / Wawancara

Metode wawancara dilakukan untuk sampel beberapa data dengan bertanya kepada para dosen khususnya dosen pembimbing serta pihak yang berhubungan dengan judul yang Penulis bahas.

1.7. Sistematika Penulisan

Adapun sistematika penulisan yang digunakan dalam penulisan laporan tugas akhir ini sebagai berikut :

BAB I PENDAHULUAN

Pada bab ini berisi uraian singkat mengenai latar belakang permasalahan, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, metode penelitian serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini membahas tentang teori-teori pendukung pembahasan masalah serta teori pendukung lainnya berdasarkan referensi yang berkaitan dengan judul laporan akhir ini.

BAB III METODELOGI PENELITIAN

Pada bab ini akan membahas kerangka penelitian, perancangan perangkat, persiapan data, pengembangan metoda dan tes kinerja sistem

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi hasil perancangan perangkat keras, perangkat lunak, hasil penerapan kriptografi *hill cipher* serta berisi pembahasan dari penelitian.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari penelitian yang telah dilakukan dan saran-saran mengenai apa saja yang harus ditambahkan untuk penelitian selanjutnya.

DAFTAR PUSTAKA

LAMPIRAN