BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Internet of Things (IoT) menjadi mode dalam dunia teknologi di masa sekarang, yang memungkinkan berinteraksi melalui semua perangkat yang terhubung satu sama lain melalui jaringan dan kemampuan bertukar informasi tanpa intervensi *Human-Human* dan *Human-Computer*. Sehingga menjadi sangat penting untuk memberikan keamanan pada informasi dengan mengubah informasi yang berguna menjadi yang tidak dapat dipahami dengan menggunakan berbagai algoritma enkripsi [1].

Berdasarkan penelitian M.O'neil tahun 2016, pakar keamanan menjelaskan tentang bagaimana mereka dapat menyerang jaringan dengan mudah untuk menyalakan sebuah lampu otomatis dan mendapatkan *username* dan *password Wi-Fi* dari seorang pemilik rumah. Dilihat dari kinerjanya, mikrokontroler akan mengirimkan serta menerima data dari server melalui internet. Data yang dikirim yang masih berupa *plainteks* yang masih dapat dibaca siapa saja. Jika terjadi serangan data dan *identify Theft* maka diperlukan *sniffing* ke jaringan mikrokontroler. Maka dipastikan bahwa kerahasiaan datanya sudah tidak terjamin [2].

Pada zaman modern saat ini, teknologi dituntut untuk dapat memudahkan segala aktivitas manusia sehingga dapat meningkatkan efisiensi, produktifitas, dan keamanan bagi penggunanya. Namun tidak sedikit dari kelalaian manusia seperti kehilangan kunci fisik yang sudah mulai berganti menjadi akses kontrol elektronik dimana hanya ada orang-orang khusus ataupun yang diberi wewenang

untuk mengakses suatu tempat itu dengan metode yang hanya diketahui oleh beberapa orang, metode yang dimaksudkan antara lain adalah dengan menggunakan kode atau *password* [3].

Kode atau *password* merupakan tautan terlemah dalam keamanan *cyber* yang terus-menerus. Kode menjadi sesuatu yang diketahui, namun rentan terhadap ancaman. Namun, ada sejumlah cara untuk memperkuatnya melalui otentikasi lebih lanjut [4]. Kriptografi menjadi salah satu yang digunakan untuk menjaga suatu kerahasiaan keamanan pesan atau informasi yang dapat dibaca. Pengamanan ini dilakukan dengan cara mengenkripsi informasi dengan suatu kunci yang khusus berupa *password* atau kode [5]. Oleh sebab itu, *password* atau kode dikirimkan melalui aplikasi yang berisi data ringkas namun memiliki informasi yang sangat rahasia, maka harus diperlakukan secara khusus dalam segi keamanan.

Algoritma *Advanced Encryption Standard* (AES) difungsikan sebagai pengamanan data penguncian didalam aplikasi yang terintegrasi dengan mikrokontroler sehingga dapat meningkatkan keamanannya menggunakan kode acak dimana setiap kode yang telah diinputkan akan terus berubah setiap kali di akses dalam jangka waktu tertentu. AES yang merupakan jenis algoritma kriptografi simetris yang menggunakan kunci enkripsi dan kunci dekripsi yang sama [3]. Algoritma ini juga dipilih berdasarkan penelitian oleh A.F Ramdhansya dkk (2014) yang membandingkan algoritma AES dan *serpent* yang diuji berdasarkan parameter yaitu waktu enkripsi dan deskripsi, heap memori dan *avalanche effect* disimpulkan jika AES ini merupakan algoritma yang paling optimal diterapkan dalam pengimplementasian *software* dan *hardware* [6]. AES

digunakan berdasarkan ketahanan terhadap serangan *brute force* [7], dengan karakteristik dan implementasi bersifat terbuka, fleksible, sederhana dan difusi atau *confusion.*

Berdasarkan hal-hal tersebut, dalam penelitian tugas akhir ini akan diarahkan pada judul "Implementasi Keamanan Pada *Internet Of Things* (IoT) Menggunakan Algoritma *Advanced Encryption Standard* (AES)".

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka penyusun dapat merumuskan masalah sebagai berikut:

1) Bagaimana cara merancang dan membangun pengaman pintu menggunakan input kode atau *password*?
2) Bagaimana cara mengautentifikasi masukan dan luaran yang dihasilkan jika kode atau *password* tidak sesuai dengan masukan?
3) Bagaimana kinerja algoritma AES menjadi pengamanan data dalam sistem penginputan kode atau *password*?

1.3 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini yaitu:

1) Merancang dan membangun pengaman pintu menggunakan input kode atau *password.*
2) Mengautentifikasi masukan dan luaran kode atau *password* yang tidak sesuai.

3) Mengimplementasikan algoritma AES dalam pengamanan data dalam sistem *password* atau kode serta menilai kinerjanya.

1.4 Batasan Masalah

Pada penelitian ini ditetapkan beberapa batasan masalah sebagai berikut:

1) Inputan untuk membuka dan mengunci pintu berupa *password* atau kode yang hanya dapat diatur dalam web pengguna.
2) *Password* atau kode yang digunakan terdiri dari 6 digit.
3) Algoritma AES digunakan untuk pengamanan data *password* atau kode yang sudah diacak untuk perintah kepada mikrokontroler.
4) Keluaran yang dihasilkan berupa data tabel *History* pada pengguna *website*.
5) Sistem alat dibangun dengan menggunakan mikrokontroler jenis ATMega328.
6) Sistem penggerak pintu merupakan *motor servo.*
7) Sistem membuka dan mengunci pintu berbasis *Internet of Things* yang diakses secara *real-time.*

1.5 Metodelogi Penulisan

1.5.1 Pengumpulan Data

Metode yang digunakan dalam penelitian ini terdiri dari dua tahap, diantaranya sebagai berikut:

1) Pengamatan

Pengumpulan data dengan cara mengadakan pengamatan atau peninjauan secara langsung ke dalam objek yang sedang diteliti.

2) Studi Literatur

Melakukan pencarian serta pengumpulan referesi seperti jurnal, buku dan bacaan-bacaan yang berkaitan dengan sistem yang akan dibuat atau diteliti.

1.5.2 Pengembangan Perangkat Lunak

Metode pengembangan perangkat lunak yang akan dibuat menggunakan metodelogi *Agile* yaitu *Rational Unifed Process* (RUP). RUP merupakan kerangka kerja proses pengembangan perangkat lunak iterative yang dibuat oleh suatu divisi dari IBM tahun 2003. Adapun tahap pengembangannya sebagai berikut :

1) Permulaan (*Inception)*, merupakan tahap yang digunakan untuk memodelkan proses bisnis serta mengidentifikasi sistem yang akan dikembangkan.
2) Perluasan/perencanaan (*Elaboration*), pada tahapan ini difungsikan sebagai perencanaan atau pemodelan sistem berdasarkan hasil analisis pada tahap *inception*.
3) Kontruksi (*Contruction*), tahap ini berfokus pada implementasi hasil pemodelan dan melakukan pengujian hasil.
4) Transisi (*Transition*), tahap terakhir ini merupakan memberikan pengarahan pada pengguna agar dapat dimengerti.

1.6 Sistematika Penulisan

Untuk memberikan gambaran dan sistematika yang jelas, peneliti akan menyusun penelitian ini menjadi 5 (lima) bab dengan urutan sebagai berikut :

BAB I PENDAHULUAN

Dalam bab ini berisi uraian tentang latar belakang masalah, perumusan masalah, tujuan penelitian, batasan masalah, metodologi penulisan, dan sistematika penulisan.

BAB II LANDASAN TEORI

Dalam bab ini akan diuraikan secara singkat mengenai teori, landasan, paradigma, dan cara pandang serta metode-metode yang telah ada atau akan digunakan dalam penyelesaian laporan pembuatan sistem aplikasi, perangkat keras, dan perangkat lunak yang dibangun.

BAB III PERANCANGAN SISTEM

Bab ini mengungkapkan permasalahan lebih khusus guna mencari alternatif pemecahan masalah serta rancangan suatu pemecahan masalah yang mungkin dilakukan.

BAB IV IMPLEMENTASI SISTEM

Bab ini memuat implementasi dari perancangan yang telah dibuat dan pembahasannya. Bab ini juga mencakup gambar tampilan dari program serta modul program yang mendukung.

BAB V PENUTUP

Dalam bab ini berisi kesimpulan yang merupakan rangkuman keseluruhan isi yang sudah dibahas serta saran seputar perluasan, pengembangan, pendalaman, dan pengkajian ulang.