BAB I
PENDAHULUAN

1.1 Latar Belakang

E-voting adalah sebuah metode pemilihan yang mengandalkan teknologi elektronik untuk memfasilitasi proses pencoblosan dan penghitungan suara. Implementasi sistem *e-voting* jika dilakukan di Indonesia sendiri dapat memberikan hal yang positif. Tentu saja, terdapat tantangan yang harus dihadapi, seperti biaya yang besar, ketersediaan sumber daya manusia yang memadai, perbedaan budaya yang beragam dan masalah keamanan yang perlu diperhatikan. Meskipun demikian, manfaat yang bisa diperoleh dari sistem *e-voting* ini memiliki dampak yang jauh lebih besar dibandingkan dengan sistem pemilihan konvensional saat ini. Keuntungan-keuntungan tersebut meliputi efisiensi dalam pengeluaran operasional, proses perhitungan yang cepat dan akurat, serta meningkatnya partisipasi masyarakat dalam pemilihan [1].

Perkembangan keamanan *e-voting* salah satunya adalah penambahan sistem otentikasi yang menggunakan *RFID* dan biometrik *fingerprint*. Penggunaan *e-voting* dengan skema seperti ini membuat pemungutuan suara lebih akurat dan adil karena hanya pemilih yang telah memenuhi syarat saja yang dapat memberikan suara [2].

Penelitian yang berkaitan dengan *e-vote/e-voting* dengan keamanan *RFID* ataupun sidik jari banyak dilakukan misalnya, pada penelitian yang dilakukan Agus Qomaruddin dan Evrita Lusiana Utari pada tahun 2016 dengan judul ***"Pemanfaatan E-KTP untuk Proses Pemungutan Suara Pemilihan Umum di Indonesia Menggunakan Sistem E-vote"*** yang bertujuan untuk memanfaatkan e-KTP sebagai alat pengganti metode pemunguatan suara manual dengan kertas ke sistem *e-vote*.

E-KTP digunakan sebagai otentikasi pada *e-voting* dan hasilnya menyimpulkan bahwa konsep *e-vote* dapat dilakukan dengan memperhatikan beberapa faktor diantaranya adalah *integrity*, *confidentiality* dan *availability* pada prosesnya, serta memberikan kemudahan dalam perhitungan hasil pemilihan [3]. Pada penelitian ini pemanfaatan e-KTP dilakukan sebagai sarana untuk memberikan keamanan pada sistem *e-vote*. Namun, penggunaanya tidak melibatkan proses enkripsi data atau pun tambahan penggunaan biometrik seperti *fingerprint.*

Sementara pada penelitian yang dilakukan P.M. Benson Mansingh, T. Joby Titus, dan V.S. Sanjana Devi pada tahun 2020 dengan judul ***"A Secured Biometric Voting System Using RFID Linked with the Aadhar Database"*** bertujuan untuk membuat sebuah sistem pemungutan suara elektronik dengan menggunakan pemindaian *RFID* dan biometrik *fingerprint* untuk memverifikasi identitas pemilih, dikatakan pada penelitian tersebut bahwa penggunakan sistem ini bagus karena dapat digunakan secara *realtime* dan menghindari suara palsu [2]. Namun, pada penelitian tersebut tidak dilakukan penambahan algoritma kriptografi sebagai sarana pendukung untuk memberikan keamanan lebih.

Penambahan metode otentikasi tersebut tetap memiliki tantangan dalam hal keamanan, terutama dalam menjaga kerahasiaan dalam pengiriman data dari alat. Salah satu cara untuk meningkatkan keamanan pada *e-voting* yang menggunakan sistem otentikasi *RFID*/e-KTP dan biometrik *fingerprint* tersebut adalah dengan menambahkan algoritma kriptografi. Banyak sekali metode keamanan kriptografi yang tersedia salah satunya adalah kriptografi algoritma *Advanced Encryption Standard* (*AES*). Algoritma *Advanced Encryption Standard* (*AES*) ini dipublikasikan pada tahun 2000 oleh *National Institute of Standard and Technology* (*NIST*) yang digunakan sebagai pengganti algoritma sebelumnya yaitu *Data Encryption Standard* (*DES*) dan kemudian ditetapkan sebagai sebuah algoritma kriptografi standar yang baru [4].

Penelitian mengenai penggunaan algoritma enkripsi *Advanced Encryption Standard* (*AES*) yang diterapkan pada perangkat *Internet of Things* salah satunya dilakukan oleh Royyannuur Kurniawan Endrayanto, Adharul Muttaqin dan Raden Arief Setyawan pada jurnal yang berjudul ***"Advanced Encryption Standard (AES) pada Modul Internet of Things (IoT)"*** dengan kesimpulan bahwa algoritma ini dapat melakukan proses enkripsi dengan baik dan cukup cepat dikatakan juga memiliki nilai *Avalanche Effect* di atas 50% untuk beberapa data [5].

Maka dari itu penelitian ini bertujuan untuk menambahkan algoritma enkripsi pada sistem *e-voting* yang menggunakan sistem otentikasi *RFID*/e-KTP dan biometrik *fingerprint* dengan menggunakan algoritma *Advanced Encryption Standard* (*AES*) dengan kunci 128-bit. Pemilihan Algoritma *Advanced Encryption Standard* (*AES*) didasari dengan alasan bahwa algoritma tersebut merupakan algoritma yang cukup sulit untuk dipecahkan saat ini, algoritma yang dikembangkan oleh Rijndael ini terdapat keunggulan lain yaitu kecepatan komputasi dan juga daya memori yang tidak terlalu besar untuk digunakan [3]. Dengan demikian judul yang diangkat dalam penelitian ini adalah ***"Implementasi AES 128 Pada Sistem Otentikasi Berbasis E-Ktp dan Biometrik di E-Voting"***.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diurai di atas, maka dapat dirumuskan sebagai berikut :

1. Bagaimana menerapkan algoritma *Advanced Encryption Standard* (*AES*) 128 dalam sistem otentikasi berbasis e-KTP dan bimoterik *fingerprint*?
2. Bagaimana kinerja *E-voting* menggunakan algoritma *Advanced Encryption Standard* (*AES*) 128?

1.3 Tujuan Penelitian

Adapun tujuan penelitian ini adalah sebagai berikut :

1. Menerapkan algoritma Advanced Encryption Standard (AES) 128 dalam sistem otentikasi berbasis e-KTP dan bimoterik *fingerprint*;
2. Mengetahui kinerja algoritma *Advanced Encryption Standard (AES)* 128 dalam sistem otentikasi berbasis e-KTP dan bimoterik *fingerprint.*

1.4 Batasan Masalah

Berdasarkan rumusan masalah yang dipaparkan di atas, terdapat beberapa batasan masalah yang akan dianalisa pada pembuatan penelitian ini. Adapun batasan-batasan tersebut yaitu :

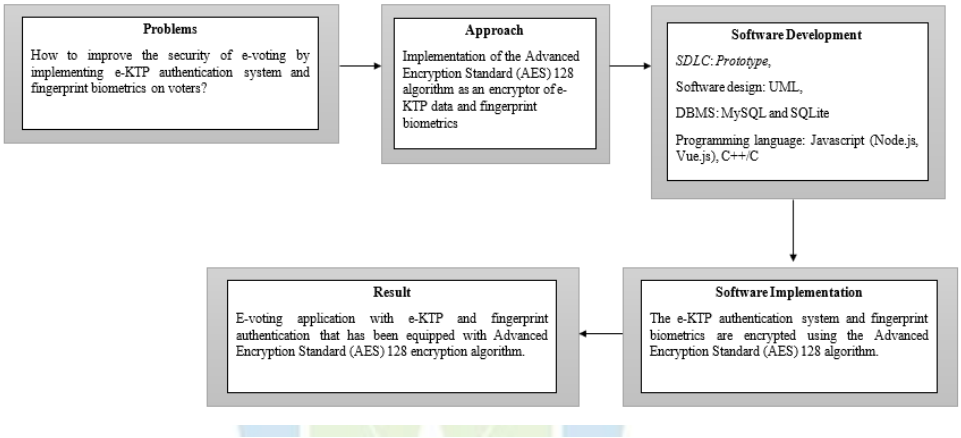
1. Pada bagian *server* menggunakan *runtime environment* Node.js
2. Pada bagian *client* menggunakan *framework UI* Vue.js
3. Aplikasi dibuat dalam bentuk web
4. Hak *super admin* dapat mengelola *admin*, pemilih, dan kandidat
5. Hak *admin* hanya dapat mengelola data pemilih
6. Pemilih hanya dapat melakukan pemilihan satu kali
7. *UID RFID* dan *fingerprint* yang tersimpan ke basis data akan di enkripsi terlebih dahulu menggunakan algoritma *Advanced Encryption Standard* (*AES*) 128
8. Data e-KTP dan sidik jari yang akan diuji pada sistem ini masing-masing berjumlah 33 data

1.5 Manfaat Penelitian

Manfaat pada penelitian ini adalah menghasilkan sebuah sistem pemungutan suara berbasis elektronik yang telah ditambahkan algoritma kriptografi, dengan harapan menambahkan keamanan yang lebih pada sistem tersebut. Sistem ini akan mengimplementasikan algoritma kriptografi *Advanced Encryption Standard* (*AES*) 128 pada data *UID* e-KTP/*RFID* dan biometrik *fingerprint* yang digunakan sebagai otentikasi bagi pemilih.

1.6 Kerangka Pemikiran

Adapun kerangka pemikiran dari pembuatan aplikasi ini yang dilihat pada gambar 1.1 kerangka pemikiran.



Gambar 1. 1 Kerangka Pemikiran

1.7 Metodologi Penelitian

1.7.1 Metodologi Penelitian

Metode yang digunakan dalam pengumpulan data adalah dengan menggunakan sebuah penelitian deskriptif, yakni dengan penelitian yang bertujuan untuk memberikan gambar permasalahan secara lengkap dan objektif. Adapun metode yang digunakan dalam pengumpulan datanya adalah sebagai berikut :

1. Observasi, yaitu mengamati objek penelitian secara langsung terhadap objek pada bidang penelitian untuk mendapatkan data-data yang dibutuhkan.
2. Studi Literatur, yaitu mempelajari pengumpulan data secara tertulis yang didapatkan dari kajian *literature*, studi ilmiah dan laporan penelitian yang berkaitan dengan bidang studi yang diteliti.

1.7.2 Metodologi Pengembangan

Metode pengembangan yang digunakan dalam pembuatan sistem perangkat lunak ini adalah model prototype. Metode ini memiliki tahapan percobaan tanpa harus menunggu sistem terselesaikan. Adapun tahapan yang gunakan sebagai berikut :

1. *Requirement Gathering*

   Tahap ini adalah tahap proses menganalisa kebutuhan yang akan digunakan dalam membangun sistem, seperti *hardware* dan *software* apa saja yang akan diperlukan.

2. *Quick Design*

   Pada tahap ini dilakukan perancangan desain *user interface* yang nantinya akan digunakan.

3. *Building Prototype*

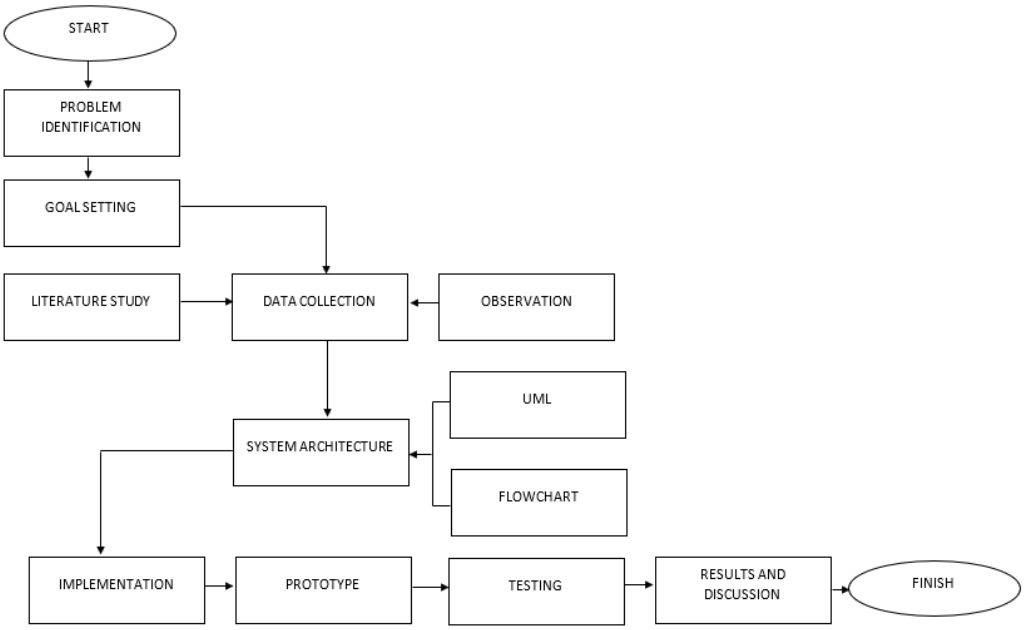
   Tahap ini adalah tahap pengerjaan perangkat lunak yang telah dirancang pada lalu semuanya diimplementasikan, tahapan yang terdapat pada tahapan ini contohnya ialah pembuatan kode program hingga selesai lalu diuji tingkat keberhasilannya.

4. *Evaluation of Prototype*

   Tahap ini adalah tahapan terakhir dimana terdapat evaluasi atau pengujian dari sistem perangkat lunak yang telah dibangun dan kemudian perbaikan *bug* yang masih ditemukan.

1.7.3 Alur Penelitian

Berikut alur penelitian yang digambarkan pada Gambar 1.2 alur penelitian.



Gambar 1. 2 Alur Penelitian

1.8 Sistematika Penulisan

Sistematika penulisan merupakan gambaran umum yang terdapat dalam penulisan penelitian ini berikut susunannya :

BAB I PENDAHULUAN

Bab I berisikan tetang latar belakang masalah, perumusan masalah, batasan masalah, maksud beserta tujuan, manfaatnya, metode penelitian dan sistematika penulisan.

BAB II STUDI PUSTAKA

Bab II menerangkan teori yang berhubungan dengan penelitian yang dibuat mulai proses hingga impelementasi. Pada bab ini juga berisikan pemaparan mengenai penelitian terdahulu yang berhungan dengan penelitian ini.

BAB III METODE PENELITIAN

Bab III berisikan analisis dan rancangan perangkat lunak yang dibangun berdasarkan permasalahan yang sudah dirumuskan dibab II.

BAB IV HASIL DAN PEMBAHASAN

Bab IV menjelaskan tentang implementasi sistem seperti basis data, interface atau antarmuka, serta pengujian sistem melalui metode *blackbox* dan kesimpulan dari pengujian

BAB V PENUTUP

Bab V ini berisikan kesimpulan dan saran dimana dibahas juga didalamnya tentang penelitian yang dilakukan secara garis besar dan saran untuk pengembangan penelitian di masa mendatang.