

BAB I

PENDAHULUAN

1.1 Latar Belakang Penelitian

Menurut Kusuma dkk [1], sistem demokrasi di Indonesia yang berpijak pada nilai-nilai Pancasila serta konstitusi UUD 1945, menjadikan pemilihan sebagai sarana esensial untuk mewujudkan kedaulatan rakyat. Proses pemilihan memberikan kesempatan bagi masyarakat untuk memilih pemimpin yang akan mewakili aspirasi mereka dalam pemerintahan. Menurut Sri Lumatus Saadah dan Hanif Masruri [2], seiring perkembangan teknologi, metode pemilihan tradisional semakin menghadapi berbagai tantangan, seperti potensi kesalahan penghitungan suara, kerusakan surat suara, dan risiko kecurangan administrasi yang dapat merusak integritas proses demokrasi. Kasus-kasus kecurangan dalam Pilkades, dalam konteks Pilkades Sambimulyo, menunjukkan bahwa integritas proses pemilihan di tingkat desa sangat krusial. Bahkan, dalam pemilihan kepala desa secara konvensional, seringkali terjadi kesalahan seperti adanya daftar pemilih ganda serta pemilih yang melakukan pencoblosan lebih dari sekali, hal ini mengakibatkan banyaknya surat suara tidak sah serta perhitungan suara yang lambat. Menurut Fefiana Diny Hermawati dkk [3], munculnya teknologi informasi menawarkan solusi inovatif untuk mengatasi permasalahan tersebut.

Menurut Fanila Kasmita Kusuma [4], salah satu inovasi yang mendapatkan perhatian adalah *e-voting* atau sistem pemungutan suara elektronik. *E-voting* diharapkan mampu meningkatkan transparansi, efisiensi, serta akurasi dalam proses pemungutan suara, sekaligus mengurangi risiko kecurangan seperti pemilih ganda. Menurut Pradani dan Wahyuni [5], penerapan teknologi ini pada pemilihan, khususnya pada skala lokal seperti pemilihan kepala desa, dapat mempercepat dan mengefisienkan proses tentang pelaksanaan *e-voting* Pilkades. Menurut Chafid dan Soffiana [6], implementasi *e-voting* membawa tantangan besar terkait keamanan data dan integritas suara. Data pemilih dan hasil pemungutan suara harus terjaga keamanannya dari berbagai ancaman seperti manipulasi, peretasan, dan penyalahgunaan.

Menurut Widodo dkk [7], untuk mengatasi isu keamanan tersebut, metode kriptografi menjadi sangat relevan dalam implementasi sistem *e-voting*, terutama yang berbasis *web*.

Algoritma kriptografi asimetris seperti RSA (*Rivest-Shamir-Adleman*) merupakan solusi yang efektif. Algoritma ini memungkinkan perlindungan data suara dengan mengenkripsi informasi menggunakan kunci publik dan mendekripsi dengan kunci privat, sehingga kerahasiaan dan integritas data terjamin. Keamanan dalam sistem pemilihan berbasis teknologi menjadi isu krusial yang terus dibahas dan dievaluasi. Potensi kerentanan yang ada dalam proses pemilihan tradisional maupun digital memberikan argumen kuat untuk pengembangan sistem *e-voting* yang lebih aman dan transparan.

Oleh karena itu, penelitian ini memiliki tujuan untuk menerapkan algoritma RSA sebagai komponen utama dalam menjaga keamanan sistem *e-voting* pada pemilihan kepala desa yang berbasis *web*. Dengan penerapan algoritma ini, diharapkan mampu menjamin aspek kerahasiaan, keutuhan, dan perlindungan data suara selama proses pemilihan berlangsung. Diharapkan hasil penelitian ini dapat memberikan dampak positif yang berarti dalam merancang sistem pemilihan yang lebih terjamin keamanannya dan bersifat transparan di Indonesia, khususnya dalam mendukung proses demokrasi di tingkat desa pada era digital. Berdasarkan latar belakang tersebut, peneliti akan berfokus pada penelitian mengenai **“Implementasi Algoritma RSA (*Rivest Shamir Adleman*) untuk Keamanan Sistem E-Voting Pemilihan Kepala Desa Berbasis Web”**.

1.2 Rumusan Masalah Penelitian

Dari uraian latar belakang, dapat dirumuskan permasalahan penelitian sebagai berikut:

1. Bagaimana mengimplementasikan Algoritma RSA untuk menjaga keamanan sistem *e-voting* pada pemilihan kepala desa yang berbasis *web*?
2. Bagaimana performa Algoritma RSA dalam melindungi sistem keamanan *e-voting* pada pemilihan kepala desa berbasis *web*?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Menerapkan algoritma RSA ke dalam sistem *e-voting* untuk pemilihan kepala desa berbasis *web*.
2. Menganalisis dan mengetahui kinerja Algoritma RSA dalam menjaga keamanan sistem *e-voting* pemilihan kepala desa berbasis *web*.

1.4 Batasan Masalah Penelitian

1. Pada penelitian ini, implementasi keamanan sistem *e-voting* difokuskan hanya pada penggunaan Algoritma RSA.
2. Sistem *e-voting* yang dikembangkan berbasis *web* dan akan disimulasikan untuk studi kasus pemilihan kepala desa.
3. Pemrograman sistem ini akan menggunakan Bahasa pemrograman Python.

1.5 Kerangka Pemikiran Penelitian

Gambar 1.1 menggambarkan alur berpikir yang dijadikan dasar dalam pelaksanaan penelitian ini. Permasalahan utama yang diangkat adalah isu-isu yang sering terjadi dalam proses pemilihan tradisional, seperti adanya daftar pemilih ganda, potensi pemilih mencoblos lebih dari satu kali, banyaknya surat suara tidak sah, serta perhitungan suaran yang lambat. Tantangan ini dapat merusak integritas dan transparansi proses pemilihan.

Untuk mengatasi permasalahan keamanan dan efisiensi dalam sistem pemilihan, khususnya dalam konteks pemilihan kepala desa, penelitian ini mengusulkan pendekatan berbasis teknologi. Pendekatan yang diusulkan melibatkan implementasi algoritma kriptografi. Penelitian ini secara spesifik akan menerapkan Algoritma RSA (*Rivest Shamir Adleman*) digunakan sebagai metode untuk menjaga keamanan data pada sistem *e-voting*. Seluruh tahapan proses implementasinya dirancang menggunakan bahasa pemrograman Python, dengan tujuan guna mengurangi potensi kebocoran informasi dan menjamin aspek kerahasiaan, keutuhan, serta validasi data dalam proses *e-voting* pemilihan kepala desa berbasis *web*.



Gambar 1.1 Kerangka Pemikiran

1.6 Sistematika Penulisan

Sistematika pada laporan tugas akhir ini terdiri atas lima bab utama, yaitu:

BAB I PENDAHULUAN

Membahas dasar pemikiran penelitian, perumusan masalah, tujuan yang ingin dicapai, batasan studi, alur pemikiran yang digunakan, dan format penyusunan laporan.

BAB II KAJIAN LITERATUR

Menjelaskan landasan teori yang mendukung, meliputi pengertian *e-voting*, dasar-dasar kriptografi, serta algoritma RSA, serta ulasan terhadap penelitian-penelitian sebelumnya.

BAB III METODOLOGI PENELITIAN

Menguraikan pendekatan dan metode yang digunakan dalam membangun sistem, mencakup alat, bahan, dan langkah-langkah implementasi.

BAB IV HASIL DAN PEMBAHASAN

Menjelaskan hasil dari penerapan sistem, termasuk proses enkripsi dan dekripsi RSA, serta pengujian fitur sistem yang telah dikembangkan.

BAB V SIMPULAN DAN SARAN

Merangkum hasil penelitian serta memberikan rekomendasi untuk pengembangan lebih lanjut di masa mendatang.