BAB I
PENDAHULUAN

A. Latar Belakang

Pada era digital saat ini, teknologi informasi berkembang dengan sangat pesat, termasuk dalam bidang pemilihan umum yang mulai beralih ke sistem elektronik atau e-voting. E-voting menawarkan banyak keunggulan, seperti efisiensi, kecepatan, dan kemudahan akses. Namun, di balik kelebihannya, e-voting juga memiliki tantangan besar terkait keamanan data suara pemilih, terutama dalam proses agregasi data. Agregasi data pada sistem e-voting menjadi titik kritis karena data dari berbagai pemilih harus diakumulasi secara aman dan benar tanpa mengungkapkan preferensi individu.

Keamanan data dalam sistem e-voting merupakan isu krusial yang telah banyak diteliti. Penelitian terbaru menyoroti bahwa salah satu celah utama dalam sistem pemungutan suara daring adalah kerentanan terhadap manipulasi data dan kurangnya transparansi yang dapat menggerus kepercayaan publik [1]. Serangan yang mungkin terjadi antara lain manipulasi data selama agregasi atau serangan replay yang dapat mendistorsi hasil pemilu. Oleh karena itu, diperlukan mekanisme keamanan yang kuat, seperti integrasi protokol komunikasi yang ditingkatkan, untuk melindungi integritas data suara dari serangan siber yang semakin canggih [2].

Salah satu metode kriptografi yang dianggap efektif dalam mengamankan data dalam proses agregasi adalah enkripsi homomorfik. Metode ini memungkinkan operasi matematika, seperti penjumlahan, dilakukan langsung pada data terenkripsi tanpa perlu mendekripsinya terlebih dahulu. Soleh dkk. [3] dalam penelitiannya pada tahun 2024 membuktikan bahwa penerapan enkripsi homomorfik pada sistem e-voting mampu melakukan anonimisasi data secara efektif, sehingga proses pengolahan suara dapat berjalan aman tanpa mengorbankan privasi pemilih. Metode ini sangat sesuai untuk digunakan dalam sistem e-voting karena menjamin kerahasiaan suara individu tetap terjaga selama proses rekapitulasi.

Paillier Cryptosystem adalah salah satu skema enkripsi homomorfik parsial (Partially Homomorphic Encryption - PHE) yang mendukung operasi penjumlahan

pada data terenkripsi [4]. Dengan menggunakan metode ini, data suara dapat dienkripsi dan dijumlahkan secara homomorfik tanpa perlu membuka kunci enkripsi selama proses agregasi, sehingga integritas dan kerahasiaan suara pemilih terjamin mutlak. Penelitian ini akan mengembangkan model e-voting yang menggunakan enkripsi homomorfik tersebut dan menguji keamanannya dalam berbagai skenario.

Berdasarkan penelitian-penelitian terbaru, seperti yang dilakukan oleh Zhan dkk. [5] dan Shahidon dkk. [6], enkripsi homomorfik memiliki keunggulan signifikan dibandingkan metode enkripsi tradisional (seperti RSA) dalam hal fungsionalitas pengolahan data terenkripsi, meskipun memiliki tantangan tersendiri dalam beban komputasi. Zhan dkk. [5] secara spesifik mengusulkan perbaikan pada skema e-voting homomorfik untuk menutup celah keamanan yang memungkinkan pemulihan data oleh otoritas pusat. Oleh karena itu, penelitian ini bertujuan untuk mengimplementasikan dan menguji model e-voting yang aman dengan menggunakan Paillier Cryptosystem, serta mengevaluasi efektivitasnya dalam melindungi data suara dari serangan dan manipulasi di lingkungan nyata.

B. Perumusan Masalah

Bagaimana implementasi algoritma Paillier Cryptosystem pada sistem e-voting dan efektivitasnya dalam mencegah serangan Man-in-the-Middle (MITM) serta Replay Attack?

C. Batasan Penelitian

Agar penelitian lebih berfokus sesuai dengan apa yang ingin dicapai, maka perlu ditetapkan batasan masalah pada penelitian ini yang bertujuan untuk membatasi bidang dan cakupan penelitian yang akan diteliti. Berikut beberapa batasan masalah pada penelitian ini :

1. Penelitian ini hanya akan membahas penggunaan enkripsi homomorfik parsial (Partially Homomorphic Encryption, PHE) dengan Paillier Cryptosystem.
2. Penerapan Paillier Cryptosystem di khususkan pada rekapitulasi perhitungan suara.

3. Simulasi dan implementasi dalam penelitian ini menggunakan data dummy yang dibuat secara manual atau dihasilkan oleh alat pembangkit data untuk keperluan pengujian algoritma..
4. Penelitian ini hanya akan fokus pada dua jenis serangan, yaitu Man-in-the-Middle (MITM) dan Replay Attack. Pembahasan dan pengujian hanya mencakup bagaimana kedua serangan ini mempengaruhi sistem yang menggunakan Paillier Cryptosystem.

D. Tujuan Penelitian

Mengimplementasikan algoritma Paillier Cryptosystem untuk mengamankan proses agregasi data suara secara homomorfik, sekaligus melakukan pengujian ketahanan sistem terhadap serangan Man-in-the-Middle (MITM) dan Replay Attack guna menjamin kerahasiaan data pemilih serta integritas hasil rekapitulasi suara dari ancaman manipulasi jaringan.

E. Manfaat Penelitian

Mengenai manfaat penelitian yang menjadi nilai dalam penelitian ini, baik untuk peneliti, pembaca, maupun pengembang sistem e-voting, berikut adalah kajian manfaat penelitian yang dihasilkan dari penelitian ini :

Manfaat Teoritis

1. Berkontribusi terhadap ilmu pengetahuan dalam penerapan enkripsi homomorfik untuk pengamanan agregasi data pada sistem e-voting.
2. Menambah wawasan literatur bagi peneliti maupun pembaca terkait pentingnya enkripsi dalam melindungi data suara pemilih pada sistem e-voting.
3. Membantu mendalami kajian ilmu terkait pengamanan data selama proses pemilihan menggunakan metode enkripsi homomorfik, khususnya Paillier Cryptosystem.

Manfaat Praktis

1. Memberikan wawasan cara mengimplementasikan enkripsi homomorfik untuk melindungi data suara pemilih dalam sistem e-voting dari manipulasi dan serangan keamanan.
2. Menambah pengetahuan terkait pengamanan agregasi data suara pada sistem e-voting yang dapat diterapkan oleh pengembang dalam membangun sistem yang lebih aman.
3. Mengetahui cara penerapan Paillier Cryptosystem sebagai metode enkripsi dalam konteks penghitungan suara yang aman dan efisien tanpa mendekripsi data..