BAB I
PENDAHULUAN

1.1 Latar Belakang

Sebagai negara penganut asas demokrasi, pemungutan suara merupakan agenda wajib dalam memilih pemimpin, baik untuk organisasi maupun negara. Metode tradisional yang menggunakan kertas suara telah lama digunakan, namun memiliki beberapa kekurangan, seperti potensi kerusakan pemilihan suara, kesalahan perhitungan, kemungkinan adanya kecurangan, serta lamanya pengumuman hasil. Oleh karena itu, perlu sistem pemungutan suara online yang dirasa aman dan terpercaya. Seiring dengan perkembangan teknologi, berbagai media seperti media sosial dan internet telah digunakan untuk jejak pendapat. Sistem e-voting yang dikembangkan saat ini dirasa aman dan mengikuti kemajuan teknologi saat ini. Untuk meningkatkan keamanannya, sistem ini dapat menggunakan bermacam jenis algoritma dalam kriptografi, seperti algoritma Paillier. Demi menjaga kerahasiaan dan keutuhan data, serta ketiadaan penyangkalan, dan otentikasi, kriptografi merupakan solusi yang efektif. Sistem dalam pemungutan suara elektronik (e-voting) sudah menjadi topik yang banyak diperbincangkan di seluruh dunia, termasuk Indonesia. Di era digital ini, banyak negara yang telah menjadikan sistem e-voting sebagai alternatif yang lebih cepat dan kurang rentan terhadap kecurangan dibandingkan dengan pemungutan suara manual. Pemungutan suara elektronik (evoting) memungkinkan pemilih untuk memberikan hak suara mereka dengan cepat dan mudah, serta berkurangnya kemungkinan kesalahan pada perhitungan suara. (Hermawati, dkk. 2023).

Sistem pada e-voting harus dirancang guna memastikan prinsip-prinsip yang ada dalam pemilu, yaitu langsung, umum, bebas, rahasia (luber), serta jujur dan adil (jurdil), terpenuhi dalam pemilihan langsung. Dalam asas demokrasi, sistem e-voting juga harus dapat menghormati dan menjamin atribut serta kriteria pada pemilihan langsung tersebut, seperti transparansi, kepastian, keamanan, akuntabilitas, dan akurasi (Loura dan Simarmata, 2011).

Namun, sistem pemilihan suara elektronik (e-voting) memiliki tantangan juga, terutama dalam keamanan informasi. Karena bersifat online, sistem evoting bisa rentan terhadap serangan cyber serta kebocoran pada data. Sehingga, penting untuk dipastikan bahwa sistem e-voting yang dipakai aman serta terlindungi dari ancaman siber.

Salah satu serangan yang mungkin terjadi pada algoritma *paillier* e-voting adalah *side-channel attack*. Serangan ini memanfaatkan informasi dari luar system untuk memperoleh informasi tentang kunci rahasia. Informasi tersebut dapat berupa waktu yang dibutuhkan untuk mengenkripsi dan mendekripsi data, penggunaan daya, atau konsumsi memori (Standaert, 2016).

Alasan *side-channel attack* terjadi pada algoritma *Paillier* e-voting adalah karena algoritma ini tidak memiliki mekanisme perlindungan terhadap serangan tersebut. Algoritma *Paillier* menggunakan proses enkripsi dan dekripsi yang membutuhkan waktu berbeda untuk setiap input. Hal ini memungkinkan penyerang memanfaatkan perbedaan waktu tersebut untuk mendapatkan informasi tentang kunci rahasia (Standaert, 2016).

Serangan *Timing* adalah jenis serangan saluran samping yang memanfaatkan waktu eksekusi untuk menargetkan kriptografi. Jika waktu eksekusi algoritma enkripsi bergantung pada kunci atau teks asli, maka serangan *timing* dapat digunakan untuk mengeksploitasi algoritma tersebut. Dengan memanfaatkan perbedaan waktu yang dibutuhkan untuk mengenkripsi dan mendekripsi suara pemilih, penyerang dapat menggunakan perangkat untuk mengukur waktu tersebut. Informasi ini kemudian dapat digunakan oleh penyerang untuk mendapatkan informasi tentang kunci rahasia. (Ariandoko, 2011).

Berdasarkan permasalahan diatas, pada proposal ini akan membahas tentang "Analisis *Side Channel Attack* Pada Pengamanan Aplikasi e-voting Menggunakan Algoritma *Paillier*".

1.2 Rumusan Masalah

Dari latar belakang yang telah dipaparkan, rumusan masalah dari penelitian ini yaitu: pengaruh *Side Channel Attack* pada performa keamanan aplikasi e-voting menggunakan algoritma *paillier*.

1.3 Batasan Masalah

Terdapat batasan-batasan masalah yang terdapat pada penelitian ini yaitu, sebagai berikut:

1. Sistem e-voting yang digunakan adalah sistem e-voting berbasis website yang diakses dari *localhost* dan serangan dilakukan berdasarkan waktu yang digunakan untuk mengeksekusi algoritma.
2. Penelitian ini dibatasi untuk mengetahui performa algoritma *paillier* terhadap salah satu *side channel attack* yaitu *timing attack.*
3. *Side channel attack* hanya berfokus pada pembacaan isi basis data tanpa meretas sistem. Hal ini melibatkan akses ke basis data terenkripsi tanpa menyadap informasi selama proses transmisi.
4. Sistem e-voting ini dapat digunakan untuk pemilihan dengan skala lebih kecil seperti dilingkungan desa, sekolah maupun tingkat universitas.

1.4 Tujuan Penelitian

Tujuan dalam penelitian ini yaitu untuk menganalisis serangan *side channel attack* pada aplikasi e-voting yang menggunakan algoritma *paillier*. Penelitian ini dilakukan untuk mengetahui seberapa kuat algoritma *paillier* terhadap serangan *side channel attack* serta mengidentifikasi potensi kebocoran informasi pada aplikasi e-voting menggunakan algoritma *paillier*.

1.5 Manfaat Penelitian

1. Hasil penelitian ini dapat digunakan untuk meningkatkan keamanan pada aplikasi e-voting yang menggunakan algoritma *paillier*.
2. Dapat berkontribusi dalam mendesain atau mengembangkan aplikasi e-voting yang lebih tahan terhadap serangan *side channel attack*

3. Meningkatkan kesadaran pengguna terkait risiko *side channel attack* pada aplikasi e-voting.
4. Mengetahui cara pengimplementasian *paillier* sebagai enkripsi homomorfik sebagian.
5. Aplikasi berbasis website yang telah dibuat dapat dipergunakan maupun dikembangkan untuk melakukan pemungutan suara dalam skala kecil seperti pemilihan dilingkungan sekolah, desa serta universitas.

1.6 Sistematika Penulisan

Penulisan penelitian ditulis secara sistematis. Adapun sistematika penulisan skripsi terstruktur sebagai berikut:

BAB I PENDAHULUAN

Bab ini akan mengulas latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, keaslian penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan penelitian-penelitian sebelumnya yang diperoleh dari jurnal terkait, yang digunakan untuk mendukung analisis dan pengembangan sistem baru.

BAB III METODE PENELITIAN

Bab ini mengulas metode penelitian yang digunakan, termasuk materi penelitian, prosedur penelitian, metode pengumpulan data, serta tahapan dalam pengolahan, analisis, dan perancangan data.

BAB IV ANALISIS DAN PEMBAHASAN

Bab ini akan memuat hasil pengujian dan pembahasan dari sistem e-voting yang telah dibuat.

BAB V PENUTUP

Pada bagian ini berisi penjelasan tentang kesimpulan dan saran pada penelitian yang dilakukan.

DAFTAR PUSTAKA

Bagian ini berisi sumber-sumber yang digunakan sebagai bahan referensi dan pendukung kajian terdahulu.

LAMPIRAN

Pada bagian ini memuat lampiran yang digunakan sebagai pendukung pada penelitian ini.