BAB I

PENDAHULUAN

1.1 Latar Belakang

Pemilihan ketua RW adalah salah satu aspek demokratis yang vital dalam mengatur lingkungan pemukiman. Namun, seringkali proses ini rentan terhadap sejumlah masalah seperti kecurangan, intimidasi, dan pelanggaran privasi pemilih. Melalui wawancara yang saya lakukan dengan beberapa anggota masyarakat dan ketua RW di lingkungan sekitar, saya mendapati bahwa pemilihan ketua RW merupakan momen penting yang sangat diantisipasi oleh seluruh warga. Namun, seringkali mereka menyuarakan keprihatinan terkait rentannya proses ini terhadap kecurangan dan intimidasi. Untuk meningkatkan keamanan dan integritas dalam proses pemilihan, teknologi informasi, terutama e-voting, telah menjadi pilihan yang menarik.

E-voting (*electronic voting*) merupakan sarana yang sering dilihat untuk membuat proses pemilu (pemilihan umum) lebih efisien serta meningkatkan tingkat kepercayaan dalam manajemen proses pemilu[1]. Sejalan dengan perkembangan teknologi dan pengguna smartphone yang pesat, pemungutan dengan cara e-voting tentu sangat membantu dan mempercepat proses suatu pemilihan[2].

Ada banyak masalah dalam sistem pemungutan suara elektronik, seperti kesalahan sistem, keama1nan jaringan, keamanan data, dll. Prosedur untuk menjaga keamanan data dan kerahasiaan data dapat dilakukan dengan menerapkan

algoritma kriptografi[3]. Kriptografi merupakan salah satu teknik untuk menjamin kerahasiaan informasi yang dikomunikasikan. Teknik kriptografi dapat dimanfaatkan untuk mendukung keamanan pada suatu informasi. Aspek keamanan informasi yang dapat didukung oleh kriptografi adalah kerahasiaan (*confidentiality*), keutuhan data (*integrity*), otentikasi penyedia/penerima informasi (authentication) serta penyangkalan (*nonrepudiation*)[4].

Konsep untuk melakukan proses komputasi tertentu pada pesan terenkripsi disebut enkripsi homomorfik. Enkripsi homomorfik merupakan suatu bentuk enkripsi yang memungkinkan dilakukannya komputasi pada *ciphertext* tanpa mendekripsi terlebih dahulu *ciphertext* tersebut. Operasi yang dilakukan pada *ciphertext* yang menggunakan enkripsi homomorfik akan menghasilkan *ciphertext* yang jika didekripsi akan menghasilkan hasil yang sama dengan operasi serupa pada *plaintext*[5]. Paillier cryptosystem, yang diperkenalkan oleh Pascal Paillier pada tahun 1999, adalah contoh sistem enkripsi homomorfik yang menonjol. Dengan menggunakan bilangan prima yang besar dan fungsi eksponensial, sistem kriptografi publik ini memungkinkan enkripsi dan dekripsi yang aman. Salah satu kelebihannya adalah kemampuan untuk melakukan operasi aritmatika langsung pada data terenkripsi, tanpa perlu mendekripsi terlebih dahulu. Namun meskipun konsep kriptografi homomorfik menjanjikan, implementasinya dalam aplikasi e-voting mobile masih memerlukan penelitian lebih lanjut. Beberapa tantangan yang perlu diatasi termasuk kinerja sistem, efisiensi perhitungan, dan keamanan tambahan yang diperlukan untuk melindungi data pemilih dari serangan cyber.

Dengan demikian, penelitian tentang implementasi kriptografi homomorfik menggunakan algoritma *Paillier Cryptosystem* pada aplikasi e-voting mobile menjadi relevan dan penting untuk menjaga integritas, keamanan, dan privasi dalam proses demokratis lokal. Melalui penelitian ini, diharapkan dapat ditemukan solusi yang efektif untuk meningkatkan keamanan dan privasi dalam e-voting serta memperkuat proses demokratis di tingkat komunitas.

1.2 Identifikasi Masalah

Dalam konteks pemilihan ketua RW, terdapat sejumlah masalah yang perlu dipecahkan untuk memastikan integritas dan keamanan proses e-voting. Berikut adalah beberapa tantangan yang dihadapi:

1. Kecurangan dalam proses pemilihan ketua RW, dapat terjadi tindakan curang seperti pembuatan suara palsu, pemungutan suara ganda, atau manipulasi hasil suara. Kurangnya keamanan dalam sistem dapat memperburuk situasi ini.

2. Pelanggaran privasi para pemilih sering kali terancam, terutama dalam sistem e-voting, di mana mereka mungkin harus mengungkapkan identitas atau pilihan suara kepada pihak yang tidak berwenang. Hal ini dapat mengurangi kepercayaan dan semangat partisipasi dalam pemilihan.

3. Ketidaktransparanan dan keraguan pada hasil pemilihan, kurangnya keterbukaan dalam proses pemilihan dapat menimbulkan keraguan tentang keaslian hasil suara. Para pemilih mungkin meragukan keaslian hasil pemilihan jika tidak ada mekanisme yang jelas untuk memverifikasi suara.

1.3 Batasan Masalah

Penelitian ini memiliki beberapa batasan masalah, antara lain sebagai berikut:

1. Fokus penelitian ini terbatas pada penerapan kriptografi homomorfik dalam aplikasi e-voting mobile untuk pemilihan ketua RW. Penelitian ini tidak akan memperhitungkan teknologi e-voting lainnya atau penggunaan kriptografi homomorfik dalam konteks yang berbeda.
2. Penelitian ini akan menitikberatkan pada peningkatan keamanan dan privasi dalam proses pemilihan ketua RW. Ini mencakup enkripsi suara pemilih, keamanan transmisi data, dan perlindungan dari serangan siber.
3. Evaluasi kinerja sistem e-voting yang menggunakan kriptografi homomorfik akan dilakukan, tetapi tidak akan menyelidiki secara mendalam. Pengukuran akan difokuskan pada waktu eksekusi dan penggunaan sumber daya komputasi dalam konteks aplikasi e-voting.
4. Penelitian ini akan membatasi diri pada penggunaan kasus khusus pemilihan ketua RW. Tidak akan meluas ke pemilihan lain atau tingkat pemilihan yang lebih tinggi, seperti pemilihan nasional.

1.4 Rumusan Masalah

Berdasarkan latar belakang penelitian, masalah yang akan dibahas dalam penelitian ini adalah sebagai berikut:

1. Bagaimana penerapan kriptografi homomorfik pada aplikasi e-voting mobile untuk pemilihan ketua RW dapat meningkatkan tingkat keamanan dan menjaga privasi pemilih?
2. Apa dampak dari penggunaan kriptografi homomorfik dalam meningkatkan integritas serta keamanan dalam proses pemilihan ketua RW melalui teknologi e-voting?

1.5 Tujuan Penelitian

Penelitian ini bertujuan untuk memfasilitasi interaksi antara masyarakat dan calon ketua RW dengan adanya aplikasi voting mobile. Tujuan spesifik penelitian ini adalah:

1. Meningkatkan tingkat keamanan dan menjaga privasi dalam proses pemilihan ketua RW dengan menerapkan teknologi kriptografi homomorfik dalam aplikasi e-voting mobile.
2. Mengevaluasi kinerja dan efisiensi sistem e-voting mobile yang memanfaatkan kriptografi homomorfik.
3. Mengidentifikasi langkah-langkah tambahan yang diperlukan untuk memperkuat keamanan dan integritas suara dalam sistem e-voting mobile yang mengadopsi kriptografi homomorfik.

1.6 Manfaat Penelitian

Berdasarkan latar belakang tersebut dapat disimpulkan manfaat penelitian adalah sebagai berikut:

1. Peningkatan Keamanan E-Voting penerapan kriptografi homomorfik dalam e-voting mobile untuk pemilihan ketua RW dapat meningkatkan keamanan sistem dan mengurangi risiko kecurangan, serta memperkuat kepercayaan masyarakat pada proses pemilihan.

2. Perlindungan Privasi Pemilih penggunaan kriptografi homomorfik dapat menjaga privasi pemilih melalui enkripsi yang kuat, meningkatkan kepercayaan dalam memberikan suara tanpa khawatir tentang privasi yang terganggu.

3. Efisiensi Proses E-voting dan kriptografi homomorfik dapat meningkatkan efisiensi pemilihan ketua RW dengan mempersingkat waktu pemrosesan suara dan meningkatkan partisipasi pemilih.

4. Kontribusi pada Kriptografi penelitian ini dapat memberikan kontribusi penting pada pemahaman tentang kriptografi homomorfik dalam konteks e-voting, membantu pengembangan aplikasi yang lebih baik dalam praktiknya.

1.7 Sistematika Penulisan

Sistematika Penulisan dalam penelitian skripsi ini terdiri dari lima bab, dengan sistematika penelitian sebagai berikut:

BAB I PENDAHULUAN

Dalam bab ini akan membahas latar belakang, identifikasi masalah, rumusan masalah, tujuan dan manfaat, batasan masalah, sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Menguraikan tentang konsep dan penjelasan metode yang digunakan. Selain itu terdapat hasil-hasil penelitian yang telah dilakukan sebelumnya oleh peneliti lain yang terkait dengan penelitian yang dilakukan.

BAB III METODOLOGI PENELITIAN

Dalam bab ini menjelaskan secara detail tentang perancangan dan analisis program, mulai dari gambaran rancangan secara umum dan analisa kebutuhan perangkat lunak yang digunakan dalam pembuatan aplikasi ini.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas mengenai hasil perancangan dan implementasi algortima dari aplikasi mobile untuk pemilihan e-voting ketua RW.

BAB V PENUTUP

Berisi tentang beberapa kesimpulan yang didapatkan dari hasil pembahasan bab bab sebelumnya, serta saran-saran yang dapat di kembangkan atau dilakukan sebagai penerapan untuk perusahaan kedepannya.

DAFTAR PUSTAKA

LAMPIRAN