

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi, khususnya dalam bidang jaringan komputer dan internet, mengalami perkembangan yang sangat cepat. Jika dahulu komputer umumnya digunakan secara mandiri, kini hal tersebut sudah jarang ditemui. Kebutuhan untuk melakukan pertukaran data secara cepat dan efisien menjadikan jaringan komputer sebagai hal yang sangat penting. Namun, di balik kemudahan tersebut, muncul berbagai risiko yang berkaitan dengan pengamanan sistem informasi. [1]

Pengamanan sistem merupakan langkah penting untuk mendeteksi sekaligus mencegah berbagai aktivitas yang bisa merugikan sistem. administrator jaringan memiliki tanggung jawab besar untuk memastikan jaringan tetap aman dari upaya peretasan dan menjaga layanan agar tetap tersedia bagi pengguna. Tantangan utama yang dihadapi adalah serangan bisa terjadi kapan saja. Maka konsekuensinya bisa sangat serius. Oleh karena itu, diperlukannya pelapis pertahanan sistem. [2]

Perkembangan teknologi informasi dan komunikasi saat ini mendorong peningkatan *volume* transaksi data, khususnya melalui internet, karena proses pengiriman, penerimaan, dan penyimpanan data kini dapat dilakukan secara cepat dan praktis. Situasi ini menjadikan isu keamanan data semakin krusial, sebab integritas dan kerahasiaan data harus terjamin sejak proses pengiriman hingga sampai ke penerima yang berhak. Dalam ranah ilmu pengetahuan, muncullah bidang kriptografi dan steganografi sebagai solusi untuk menjaga keamanan data, yakni melalui teknik penyandian dan penyembunyian informasi agar isi pesan tetap

terlindungi dari pihak yang tidak berwenang. [3]

Terdapat berbagai macam algoritma dalam kriptografi, salah satunya adalah *Caesar Cipher*. *Caesar Cipher* dikenal sebagai salah satu metode tertua dalam dunia kriptografi dan termasuk dalam kategori *cipher* substitusi. Teknik ini bekerja dengan mengganti setiap karakter dalam plainteks melalui pergeseran huruf sebanyak sejumlah langkah tertentu yang sama untuk seluruh teks. [4]

Oleh karena itu, peneliti melakukan pengembangan solusi berbasis OTP menggunakan algoritma *Caesar Cipher* yang efektif diperlukan untuk menciptakan sistem autentikasi yang mampu menjamin keamanan dan kenyamanan pengguna secara bersamaan.

1.2 Identifikasi Masalah

Berdasarkan Kuesioner yang telah disebar, maka diperoleh identifikasi masalah yang dihadapi adalah:

1. Tindakan yang disengaja seperti pencurian data merupakan ancaman nyata terhadap keamanan sistem informasi.
2. Meningkatkan autentikasi dan otorisasi agar sistem informasi menjadi lebih kuat dan aman.
3. Kerentanan Perangkat Lunak (*Software Vulnerabilities*) yang sering kali memiliki celah keamanan yang dapat dimanfaatkan pihak tidak berwenang.

1.3 Rumusan Masalah

Berdasarkan latar belakang di atas, maka dapat dirumuskan permasalahan yang akan diteliti sebagai berikut :

1. Bagaimana penerapan lapisan perlindungan tambahan, seperti autentikasi dapat memperkuat sistem?
2. Bagaimana agar lapisan keamanan sistem akan sulit dipecahkan?

1.4 Batasan Masalah

Untuk tidak memperluas area pembahasan pada penelitian ini diperlukan batasan-batasan masalah untuk menyederhanakan permasalahan, yaitu :

1. Sistem dikembangkan secara spesifik pada modul akun *user*.
2. Sistem hanya merekomendasikan persiapan *email* pribadi saat daftar
3. Karena keterbatasan waktu pembuatan aplikasi *mobile* hanya sampai tahap aktivasi email dan password.

1.5 Tujuan dan Manfaat Penelitian

1.5.1 Tujuan

Adapun tujuan utama dari penelitian ini yaitu:

1. Mengembangkan sistem keamanan pada aplikasi berbasis Android dengan menggunakan algoritma *Caesar Cipher* untuk mengenkripsi kode *One Time Password* (OTP).
2. Memberikan lapisan keamanan tambahan dalam proses registrasi akun agar data pengguna tetap terlindungi dari risiko penyadapan.
3. Menyediakan mekanisme pengiriman dan validasi OTP yang efisien, aman, dan mudah digunakan pada aplikasi berbasis Android.

1.5.2 Manfaat

Berikut adalah manfaat dari penelitian yang dilakukan :

1. Memberikan keamanan tambahan saat melakukan registrasi akun melalui penggunaan kode OTP yang terenkripsi, sehingga data pribadi pengguna terlindungi dari risiko penyadapan atau akses tidak sah.
2. Menyediakan referensi dan solusi untuk meningkatkan keamanan proses registrasi akun dengan menggunakan algoritma enkripsi seperti *Caesar Cipher*

1.6 Sistematika Penulisan

Penelitian ini akan dibagi dalam empat bab, gambaran masing-masing bab akan dijelaskan dibawah ini :

BAB I PENDAHULUAN

Dalam bab ini berisi penjelasan tentang latar belakang masalah, maksud dan tujuan penelitian, rumusan masalah, pembahasan masalah, metode pengumpulan data dan sistematika penulisan.

BAB II LANDASAN TEORI

Dalam bab ini menjelaskan tentang memuat tinjauan dan ulasan singkat mengulas pentingnya penelitian yang dilakukan dan menyampaikan teori yang berhubungan dengan permasalahan yang dibahas sebagai dasar analisa permasalahan yang diteliti.

BAB III METODOLOGI PENELITIAN

Dalam bab ini membahas tentang pendekatan studi dan dapat berupa analisis teori, metode eksperimen, kombinasi, rancangan, spesifikasi sistem baik perangkat

keras maupun perangkat lunak.

BAB IV HASIL DAN PEMBAHASAN

Pada bab ini berisi tentang hasil dan pembahasan yang diperoleh dari perancangan sistem, dan implementasi pada penelitian yang dilakukan.

BAB V PENUTUP

Pada bab ini merupakan bab terakhir yang berisi kesimpulan, dan saran dari penelitian yang dilakukan untuk pengembangan sistem lebih lanjut agar tercapai hasil yang lebih baik.

