BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era digital, keamanan dalam transfer data, transaksi digital, maupun pengaksesan suatu akun menjadi salah satu aspek yang semakin penting seiring dengan meningkatnya penggunaan layanan *online*. Ancaman serangan *cyber* seperti pencurian data, peretasan akun, hingga manipulasi autentikasi terus berkembang, mendorong perlunya pengembangan metode autentikasi yang lebih kuat dan andal. Dalam era yang semakin rentan terhadap serangan *brute-force* (percobaan segala kemungkinan), *phishing* (penipuan *online*), dan *man-in-the-middle* (penyadapan komunikasi), metode autentikasi konvensional (*Single-Factor Authentication*) dengan hanya menggunakan *password* menjadi kurang memadai untuk melindungi pengguna.

Guna mengatasi tantangan serangan *cyber*, salah satu metode yang telah diadopsi secara luas adalah *Two-Factor Authentication* (2FA). Pada sistem 2FA, pengguna diharuskan untuk memasukkan dua komponen autentikasi yang berbeda, biasanya berupa *password* (sesuatu yang diketahui pengguna) dan *token* fisik atau kunci privat (sesuatu yang dimiliki pengguna) (Aprilia et al., 2024). Meskipun 2FA meningkatkan keamanan dengan menambahkan lapisan autentikasi tambahan, implementasi ini masih rentan terhadap serangan *cyber* yang canggih jika mekanisme kriptografinya tidak dirancang dengan baik.

Elliptic Curve Digital Signature Algorithm (ECDSA) adalah salah satu algoritma kriptografi yang dapat diterapkan untuk memperkuat lapisan kedua dalam autentikasi 2FA. ECDSA adalah algoritma tanda tangan digital berbasis kurva eliptik yang memiliki keunggulan berupa keamanan tinggi dengan ukuran kunci yang lebih kecil dibandingkan algoritma kriptografi tradisional seperti RSA (Pardosi, 2024). ECDSA memanfaatkan kunci privat untuk menghasilkan tanda tangan digital yang dapat digunakan untuk memverifikasi keaslian dan integritas pesan, memastikan bahwa hanya pengguna yang memiliki kunci privat yang dapat menandatangani pesan yang dikirimkan oleh *server*.

Dalam proses ECDSA, digunakan algoritma *hash* untuk mengubah pesan asli menjadi representasi berukuran tetap. Salah satu algoritma *hash* yang sering

digunakan dalam proses ini adalah *Secure Hash Algorithm 256* (SHA 256). SHA 256 berfungsi untuk menghasilkan nilai *hash* dari pesan yang akan ditandatangani oleh ECDSA. Nilai *hash* ini kemudian digunakan bersama dengan kunci privat ECDSA untuk membentuk tanda tangan digital. SHA 256 dipilih karena menawarkan tingkat keamanan yang tinggi dan *collision-resistant*, artinya memastikan bahwa setiap pesan yang berbeda menghasilkan *hash* yang unik (Judhieputra et al., 2024).

Dalam konteks implementasi kriptografi, terdapat penelitian sebelumnya mengenai implementasi *Elliptic Curve Diffie-Hellman* (ECDH) pada protokol *two-way challenge-response*, yang menunjukkan bagaimana ECDH dapat digunakan untuk pertukaran kunci secara aman antara dua pihak tanpa mengungkapkan kunci privat di jaringan (Fitri, 2022). Penelitian tersebut memberikan wawasan penting tentang penerapan kriptografi kurva eliptik, tetapi lebih fokus pada pertukaran kunci, sementara pada penelitian ini akan mengeksplorasi penerapan ECDSA dan SHA 256 untuk menghasilkan dan memverifikasi tanda tangan digital, yang merupakan bagian penting dari skema autentikasi.

Selain itu, telah ada penelitian yang membahas implementasi ECDSA dan Algoritma SHA 256 pada Autentikasi RESTful Web API. Penelitian tersebut menunjukkan bagaimana kedua algoritma dapat digunakan untuk memperkuat keamanan autentikasi dalam arsitektur layanan *web*, dengan menjamin keaslian dan integritas data yang dipertukarkan (Khan, 2023). Di sisi lain, penulis berfokus pada penelitian terkait penerapan ECDSA dan SHA 256 dalam konteks autentikasi berbasis 2FA, menawarkan pendekatan yang berbeda dan lebih spesifik terhadap pengamanan proses login.

Penelitian ini bertujuan untuk mengimplementasikan ECDSA dan algoritma SHA 256 dalam skema 2FA guna meningkatkan keamanan proses autentikasi. Dengan memanfaatkan ECDSA untuk menandatangani pesan acak yang dikirimkan oleh *server*, serta menggunakan SHA 256 untuk menghasilkan *hash* dari pesan, sistem diharapkan dapat lebih tahan terhadap berbagai serangan *cyber*. Autentikasi berbasis ECDSA memastikan bahwa hanya pengguna yang memiliki kunci privat yang dapat memberikan tanda tangan digital yang valid, sedangkan penggunaan SHA 256 menjamin integritas pesan.

Berdasarkan pemaparan sebelumnya, penulis tertarik untuk mengkaji proses autentikasi dan verifikasi 2FA menggunakan ECDSA dan SHA 256 yang diimplementasikan dengan menggunakan bahasa pemrograman Python. Oleh karena itu, penulis mengambil judul **"Implementasi *Elliptic Curve Digital Signature Algorithm* dan *Secure Hash Algorithm 256* pada Login Akun dengan Sistem *Two-Factor Authentication*"**.

1.2 Rumusan Masalah

Berdasarkan latar belakang penelitian, maka permasalahan dalam penelitian ini adalah sebagai berikut:

1. Bagaimana rancangan implementasi algoritma ECDSA dan SHA 256 dalam 2FA guna meningkatkan keamanan proses autentikasi dan verifikasi?
2. Bagaimana konstruksi program aplikasi login yang menggunakan sistem 2FA berbasis kombinasi ECDSA dan SHA 256 sehingga dapat memastikan integritas dan keaslian data dengan menggunakan bahasa pemrograman Python?
3. Bagaimana validasi program aplikasi login yang menggunakan sistem 2FA berbasis kombinasi ECDSA dan SHA 256 sehingga dapat memastikan program aplikasi dapat berjalan dengan baik?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah penelitian, maka tujuan dalam penelitian ini adalah sebagai berikut:

1. Merancang implementasi algoritma ECDSA dan SHA 256 dalam 2FA guna meningkatkan keamanan proses autentikasi dan verifikasi.
2. Mengonstruksi program aplikasi login yang menggunakan sistem 2FA berbasis kombinasi ECDSA dan SHA 256 sehingga dapat memastikan integritas dan keaslian data dengan menggunakan bahasa pemrograman Python.
3. Memvalidasi program aplikasi login yang menggunakan sistem 2FA berbasis kombinasi ECDSA dan SHA 256 sehingga dapat memastikan program aplikasi dapat berjalan dengan baik.

1.4 Batasan Masalah

Adapun beberapa batasan dalam penelitian ini adalah sebagai berikut:

1. Fokus pada Prototipe

   Aplikasi yang dikembangkan hanya difokuskan sebagai prototipe untuk menunjukkan konsep dan mekanisme kerja dari ECDSA dan SHA 256 dalam 2FA. Aplikasi ini tidak dirancang untuk digunakan dalam skala industri atau memiliki ketahanan tinggi terhadap berbagai ancaman keamanan yang kompleks.

2. Pengujian Terbatas

   Pengujian sistem hanya dilakukan dalam lingkungan simulasi atau lokal, tidak mencakup pengujian terhadap berbagai situasi dunia nyata, seperti serangan siber tingkat lanjut atau uji coba pada banyak pengguna sekaligus.

3. Penggunaan Data Sederhana

   Dalam prototipe ini, data yang digunakan untuk autentikasi hanya mencakup username dan password sederhana serta kunci privat dan publik ECDSA. Aplikasi tidak melibatkan enkripsi kompleks atau integrasi dengan basis data yang besar.

4. Keterbatasan Fitur

   Aplikasi ini hanya mencakup fitur dasar dari autentikasi dua faktor dengan ECDSA dan SHA 256, yaitu pembuatan akun, login dengan verifikasi, serta proses verifikasi tanda tangan digital. Fitur tambahan seperti pengelolaan pengguna lanjutan atau integrasi dengan perangkat lain tidak dibahas dalam penelitian ini.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat dalam beberapa hal di antaranya adalah sebagai berikut:

1. Memberikan kontribusi dalam bidang kriptografi khususnya dalam ECDSA yang dikombinasikan dengan SHA 256.
2. Meningkatkan keamanan autentikasi untuk *server* dan *client* dengan system 2FA yang mengimplementasikan ECDSA dan SHA 256.