BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam era digital saat ini, pengelolaan data menjadi salah satu aspek krusial dalam berbagai institusi, termasuk lembaga pendidikan tinggi. Data mahasiswa yang mencakup informasi pribadi, riwayat akademik, dan data sensitif lainnya memiliki nilai yang tinggi dan perlu dilindungi dari ancaman akses yang tidak sah. Tanpa adanya sistem keamanan yang memadai, data tersebut dapat menjadi target bagi oknum yang berniat jahat yang dapat mengakibatkan kebocoran informasi, pencurian identitas, serta merugikan institusi dan mahasiswa itu sendiri.

Pada tahun 2023, Indonesia mengalami sejumlah insiden kebocoran data yang signifikan, termasuk di sektor pendidikan. Menurut laporan dari Kementerian Komunikasi dan Informatika (KOMINFO) Republik Indonesia, tercatat lebih dari 34,9 juta data pribadi warga, termasuk mahasiswa telah bocor akibat pelanggaran keamanan siber [1]. Sejalan dengan laporan tersebut, Badan Siber dan Sandi Negara (BSSN) menemukan data seperti nomor telepon, NIK, dan NPWP telah bocor ke forum gelap [2]. Kemudian pada tahun 2024, kasus yang mencuri perhatian adalah kebocoran data yang terjadi di Universitas Indonesia, terdapat dugaan kebocoran data yang dilaporkan telah dijual di forum gelap yang bernama *BreachForums* [3]. Sementara itu menurut Setiawan & Najicha (2021), insiden kebocoran data pribadi sebanyak 279 juta orang Indonesia terjadi akibat serangan siber, di mana data tersebut kemudian diperjualbelikan di situs gelap *RaidForums* [4].

Fenomena kebocoran data di sektor pendidikan bukan hanya terjadi di Indonesia, tetapi juga menjadi masalah global yang serius. Menurut laporan Hylender et al. (2024), investigasi Verizon (DBIR) menyebutkan bahwa serangan siber pada sektor pendidikan didorong oleh keuntungan finansial [5]. Seiring dengan laporan di atas, Gregory Rigby (2024) menyampaikan institusi pendidikan di Amerika Serikat mengalami 3.713 kasus pelanggaran data, dengan 60% diantaranya terjadi di universitas [6]. Kejadian ini menunjukkan bahwa sistem keamanan informasi di institusi pendidikan masih rentan dan memerlukan perhatian yang lebih terutama dalam melindungi data.

Sebagai salah satu institusi pendidikan terkemuka di Jawa Timur, Universitas Muhammadiyah Ponorogo (UMPO) telah menerapkan sistem pengelolaan data digital sejak tahun 2005 untuk mengelola informasi mahasiswa [7]. Untuk mendukung pengelolaan data, UMPO menggunakan aplikasi yang dikenal dengan nama SimFT.

SimFT merupakan Sistem Informasi Manajemen Fakultas Teknik Universitas Muhammadiyah Ponorogo. Sistem ini berfungsi untuk mengelola data akademik seperti data pribadi mahasiswa, praktikum, skripsi, Kampus Merdeka dan riwayat akademik lainnya. Mengingat besarnya data yang dimiliki serta risiko terhadap serangan siber, maka data-data perlu diamankan, salah satunya dengan menerapkan enkripsi. Menurut Umam & Muslih (2023), enkripsi adalah proses mengubah data menjadi format yang tidak dapat dibaca disebut *chipertext* tanpa kunci dekripsi yang tepat, sehingga hanyak pihak yang berwenang yang dapat mengakses data tersebut [8]. Salah satu algoritma enkripsi yang populer adalah algoritma *Advanced Encryption Standard* (AES).

Algoritma *Advanced Encryption Standard* (AES) merupakan algoritma enkripsi populer yang telah digunakan oleh lembaga dan perusahaan besar seperti *Amazon Web Service* (AWS) dan *Google Cloud* [9]. Di Indonesia, salah satu perusahaan yang menerapkan algoritma AES untuk pengamanan data adalah PT PLN (Persero) [10] . Menurut Radus Batau (2024), algoritma AES adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris saat ini [11]. Sejalan dengan hal tersebut, Nova et al. (2023) menyebutkan bahwa algoritma AES digambarkan sebagai algoritma simetri yang sering digunakan karena keamanannya yang tinggi [12]. Sementara itu, Teng et al. (2020) menjelaskan algoritma AES telah diakui secara luas keamanannya karena memiliki panjang kunci sebesar 256 bit [13]. Kemudian dalam pandangan Laayu et al. (2020), AES adalah sistem kriptografi simetris bertipe *blockcipher* dengan spesifikasi panjang blok 128 bit [14]. Irawan et al. (2024) mengatakan bahwa algoritma AES, proses enkripsi dilakukan berulang kali dalam serangkaian tahapan yang disebut ronde, di mana banyaknya ronde yang dilakukan tergantung pada panjang kunci yang digunakan [15]. Berdasarkan karakteristik tersebut, algoritma AES 156 bit merupakan algoritma kriptografi

simetris yang cocok untuk mengamankan data karena kemampuanya untuk melakukan proses enkripsi dan dekripsi yang baik, sehingga mampu melindungi data yang ada pada SimFT Universitas Muhammadiyah Ponorogo.

Dengan isu yang ada dan kerentanan yang terjadi, maka diperlukannya pengamanan data mahasiswa dalam SimFT Universitas Muhammadiyah Ponorogo, penelitian ini bertujuan untuk mengimplementasikan algortima AES 256 bit sebagai enkripsi data dalam *database* pada fitur pendaftaran mahasiswa Kampus Merdeka. Dengan pendekatan ini, diharapkan sistem ini dapat menjamin keamanan informasi mahasiswa dan meningkatkan kepercayaan dari pihak-pihak terkait, termasuk mahasiswa, dosen, dan staf akademik.

Penelitian ini berfokus pada implementasi algoritma *Advanced Encryption Standard* (AES) 256 bit untuk enkripsi data mahasiswa Kampus Merdeka pada SimFT. Diharapkan penelitian ini tidak hanya memberikan kontribusi dalam pengembangan sistem manajemen fakultas, tetapi juga menjadi referensi untuk penelitian lebih lanjut di bidang keamanan data.

1.2. Perumusan Masalah

Bagaimana merancang sistem pendaftaran Kampus Merdeka pada SimFT menggunakan algoritma *Advanced Encryption Standard* (AES) 256 bit dalam *database* berbasis web?

1.3. Tujuan Penelitian

Menerapkan algoritma *Advanced Encryption Standard* (AES) 256 bit dalam *database* pada sistem pendaftaran Kampus Merdeka berbasis web.

1.4. Batasan Masalah

Dalam penelitian ini, terdapat beberapa batasan yang perlu diperhatikan agar fokus penelitian tetap terjaga. Batasan masalah tersebut adalah sebagai berikut:

1. Sistem yang dirancang akan difokuskan pada aspek enkripsi data pribadi dan data akademik mahasiswa yang mendaftar pada program Kampus Merdeka.
2. Enkripsi hanya diterapkan pada sisi *database*, bukan pada proses pengiriman data (transmisi) atau komponen sistem lainnya.

3. Tabel-tabel yang dienkripsi dibatasi hanya pada tabel yang berhubungan langsung dengan program Kampus Merdeka, seperti tabel pendaftaran, program, persetujuan, dan sebagainya.
4. Penelitian ini tidak akan membahas topik keamanan lainnya di luar enkripsi data, seperti pengamanan jaringan atau keamanan sistem secara keseluruhan.

1.5. Manfaat Penelitian

Penelitian ini memberikan kontribusi dalam meningkatkan keamanan data mahasiswa pada SimFT Universitas Muhammadiyah Ponorogo khususnya pada fitur pendaftaran mahasiswa Kampus Merdeka melalui implementasi algoritma *Advanced Encryption Standard* (AES) 256 bit.

Selain itu, penelitian ini dapat membantu Fakultas Teknik Universitas Muhammadiyah Ponorogo dalam mengelola dan menyimpan data yang diperlukan untuk keperluan administrasi mahasiswa yang mendaftar pada program Kampus Merdeka.