BAB I

PENDAHULUAN

1.1. Latar Belakang

Pesatnya perkembangan teknologi di era revolusi industri 5.0, baik perangkat keras maupun perangkat lunak telah memungkinkan pengumpulan dan pengolahan data menjadi informasi yang bermanfaat. Perkembangan tersebut dapat mempengaruhi pola kehidupan manusia melaui media elektronik, dengan hubungan perubahan dari pola *paper* ke *paperless* [1]. Namun di balik banyaknya manfaat yang diberikan dalam memenuhi kebutuhan manusia akan informasi dalam melakukan aktivitas hidupnya juga memberikan dampak negatif [2]. Dokumen menjadi aset penting dan merupakan sumber informasi yang diperlukan oleh suatu instansi [3]. Informasi tersebut dapat menjadi sasaran yang sangat berharga bagi para pelaku serangan siber, yang berusaha mencuri atau merusak data penting untuk berbagai tujuan yang tidak sah dan merugikan. Dengan terjadinya kasus manipulasi data yang menyebabkan perubahan tidak sah dan perusakan data pada dokumen, pihak yang tidak bertanggung jawab dapat dengan mudah menyalin, memindahkan, dan memanipulasi data untuk kepentingan tertentu. Oleh karena itu, keamanan data menjadi sangat penting karena kerugian yang ditimbulkan dapat sangat besar, termasuk kerugian finansial maupun reputasi, serta menurunkan tingkat kepercayaan terhadap integritas informasi yang disampaikan, menjadikan keamanan data sebagai salah satu masalah yang sangat penting dalam dunia teknologi informasi [4].

Pada Penerimaan Peserta Didik Baru (PPDB) 2023 jalur zonasi SMA di Makasar terdapat 99 dari 720 data siswa yang bermasalah. Dari 99 data siswa tersebut diantaranya adalah 36 siswa dari SMAN 2 Makassar, 16 siswa dari SMAN 3 Makassar, 30 siswa dari SMAN 5 Makassar, dan 17 siswa dari SMAN 11 Makassar. 99 data siswa yang bermasalah tersebut terdapat peserta didik yang teridentifikasi melakukan mutasi atau berpindah kartu keluarga setelah batas waktu, menggunakan surat keterangan domisili palsu, dan memalsukan data pada

kartu keluarga [5]. Sejak 2019, Kartu Keluarga telah menggunakan tanda tangan berbasis QR code untuk meningkatkan keamanan dan keaslian dokumen, sehingga pemalsuan data seharusnya dapat diminimalkan melalui verifikasi digital. Selain itu kasus pemalsuan tanda tangan di Kepulauan Riau yang melibatkan Lamidi, Kepala Badan Kesatuan Bangsa dan Politik (Kesbangpol). Tanda tangan Lamidi dipalsukan oleh seorang tenaga harian lepas (THL) untuk mengajukan proposal hibah fiktif senilai Rp 1,9 miliar ke Badan Pengelolaan Keuangan dan Aset Daerah (BPKAD). Lamidi mengetahui kasus ini setelah dana dicairkan dan telah melaporkannya kepada Gubernur Kepri sejak Desember 2020. Beliau menegaskan bahwa proposal fiktif tersebut tidak pernah masuk ke dinasnya dan pencairan dilakukan tanpa rekomendasinya.

Dari beberapa kejadian diatas mempunyai persamaan yaitu terjadinya manipulasi data yang menunjukkan betapa lemahnya perlindungan dan keamanan data di Indonesia. Salah satu aspek yang signifikan berkaitan dengan pentingnya informasi atau data adalah kebutuhan akan pembatasan akses untuk menjaga keamanan informasi tersebut atau dengan kata lain dapat di istilahkan dengan *private area* [6]. Kerahasiaan atau privasi dalam mencegah akses tidak sah terhadap data penting atau sensitif oleh pihak yang tidak berhak. Pemalsuan dokumen umumnya dilakukan dengan memanipulasi isi dokumen dan membuat dokumen baru yang memiliki desain dan tampilan yang sama dengan aslinya. Biaya yang diperlukan untuk pemalsuan dokumen juga semakin rendah, sehingga meningkatkan kerentanan terhadap pemalsuan [3].

Dalam penerapanya, alur penerimaan surat masih terbilang lama karena mahasiswa harus menyerahkan dokumen ke Tata Usaha (TU), yang kemudian diajukan ke dosen berwenang untuk ditandatangani. Banyaknya dokumen yang harus ditandatangani serta ada kalanya pimpinan keluar kantor menyebabkan proses penandatanganan memerlukan waktu yang cukup lama [7]. Selain itu tanda tangan konvensional dapat disalin secara manual atau dengan *scan copy* dan dapat dipergunakan secara berulang [8]. Salah satu strategi yang dapat diterapkan untuk melindungi data adalah penggunaan metode kriptografi [6]. Metode kriptografi

dapat diterapkan melalui penggunaan *digital signature* pada layanan terpadu Fakultas Teknik Universitas Muhammadiyah Ponorogo.

Sistem *digital signature* dengan algoritma RSA dan AES melindungi dokumen elektronik dalam dua tahapan utama yaitu RSA untuk membuat tanda tangan digital unik menggunakan kunci privat pengirim, dan AES untuk mengenkripsi isi pesan. Algoritma RSA menghasilkan kode tanda tangan yang panjang, sehingga sering diubah menjadi kode QR untuk mempermudah verifikasi [9]. Penerima memindai kode QR untuk memperoleh dan memverifikasi tanda tangan digital menggunakan kunci publik pengirim. *Digital signature* memungkinkan dokumen elektronik ditandatangani secara digital, menghasilkan tanda tangan yang unik, tidak dapat dipalsukan, dan mudah diverifikasi.

Berdasarkan uraian informasi diatas akan dilakukan penelitian mengenai implementasi *digital signature* pada surat menyurat yang ada pada layanan terpadu Fakultas Teknik Universitas Muhammadiyah Ponorogo. Diharapkan penelitian ini dapat bermanfaat bagi segenap sivitas akademika Fakultas Teknik Universitas Muhammadiyah Ponorogo.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan pada sub-bab sebelumnya, maka rumusan masalah dalam penelitian ini adalah:

a. Bagaimana implementasi *digital signature* dengan algoritma AES dan RSA pada layanan terpadu Fakultas Teknik Universitas Muhammadiyah Ponorogo?

b. Bagaimana efektivitas algoritma tersebut dalam menjaga keamanan dan keautentikan dokumen?

1.3. Batasan Masalah

Agar penelitian ini lebih terfokus dan terarah untuk menghindari pembahasan diluar permasalahan, maka penulis perlu menggunakan batasan. Adapun batasan masalah pada penelitian ini yaitu:

a. Penelitian ini hanya terfokus pada algoritma AES-256 sebagai pengamaman surat dengan metode enkripsi dan RSA sebagai *digital signature* yang diubah kedalam bentuk QR-code.
b. *Digital signature* hanya diterapkan pada 1 entitas dekan Fakultas Teknik Universitas Muhammadiyah Ponorogo.
c. Fokus penelitian ini hanya pada surat-surat yang memerlukan tanda tangan dekan Fakultas Teknik Universitas Muhammadiyah Ponorogo yang diambil dari Layanan Terpadu.
d. Penelitian ini menggunakan React.js untuk frontend dan Express.js untuk backend.
e. Data surat tersimpan secara otomatis ke dalam database, namun pengelolaan arsip surat tidak terintegrasi dengan sistem penyimpanan data tersebut.
f. Penelitian ini tidak akan mencakup keamanan fisik dari server dan infrastruktur jaringan.
g. Sistem yang dikembangkan tidak mencakup mekanisme pemulihan data apabila terjadi kegagalan sistem atau kehilangan data.
h. QR code yang dihasilkan hanya berfungsi sebagai verifikasi tanda tangan digital tanpa integrasi dengan layanan pihak ketiga untuk validasi eksternal.
i. Waktu enkripsi dan dekripsi yang diukur hanya dilakukan pada tingkat sistem lokal tanpa mempertimbangkan performa dalam skala produksi dengan jumlah pengguna yang lebih besar.

1.4. Tujuan

Tujuan penelitian ini ialah mengimplementasikan *digital signature* untuk memverifikasi keaslian dan integritas dokumen, serta memastikan bahwa dokumen tersebut benar-benar berasal dari pihak yang berwenang.

1.5. Manfaat

Manfaat dari tujuan dilakukannya penelitian ini antara lain:

a. Implementasi *digital signature* memastikan bahwa dokumen memiliki keaslian dan integritas yang terjamin.

b. Memudahkan mahasiswa dengan menghemat waktu karena tidak memerlukan tanda tangan fisik.