BAB I
PENDAHULUAN

A. Latar Belakang

Perkembangan teknologi informasi telah mendorong perguruan tinggi untuk mengadopsi dokumen legal dalam bentuk digital, termasuk Sertifikat *English Test Program* (*ETP*). Dokumen elektronik memiliki kekuatan dan akibat hukum yang sah di mata hukum, setara dengan dokumen bertanda tangan manual, asalkan telah memenuhi persyaratan yang berlaku [1]. Oleh karena itu, menjamin keaslian (*authenticity*) dan integritas dokumen digital ini menjadi aspek krusial untuk menjaga kredibilitas institusi dari ancaman manipulasi maupun pemalsuan data [2].

Kebutuhan akan sistem pengamanan dokumen akademik semakin mendesak mengingat maraknya kasus pemalsuan sertifikat kemampuan bahasa Inggris di berbagai wilayah. Ketiadaan jaminan perlindungan keamanan dan kerahasiaan data merupakan celah utama yang memicu terjadinya kebocoran serta manipulasi informasi oleh pihak yang tidak bertanggung jawab [3]. Sebagai contoh, temuan penggunaan sertifikat *TOEFL* palsu oleh kalangan mahasiswa menunjukkan betapa rentannya dokumen terhadap tindakan modifikasi yang merugikan integritas akademik [1]. Dampak dari lemahnya sistem verifikasi ini bahkan berujung pada konsekuensi hukum dan profesional yang fatal, sebagaimana terjadi pada salah satu universitas di Indonesia di mana dua orang pegawai harus menerima tindakan pemecatan akibat keterlibatan dalam sindikat pemalsuan sertifikat. Fenomena ini juga menjadi ancaman nyata di lingkungan internal Universitas Maritim Raja Ali Haji (UMRAH), di mana teridentifikasi celah keamanan yang memungkinkan oknum tertentu mendapatkan sertifikat *ETP* secara ilegal melalui praktik gratifikasi. Kondisi ini menuntut adanya perlindungan data melalui instrumen teknologi untuk menghindari risiko penyalahgunaan data yang kian masif [4].

Dalam konteks Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji, meskipun Sertifikat *ETP* telah diimplementasikan secara digital, permasalahan kritis teridentifikasi pada mekanisme validasinya. Sistem saat

ini masih menggunakan *QR Code* biasa yang proses pembuatannya dilakukan secara manual. *QR Code* tersebut sangat rentan terhadap pemalsuan karena proses pembuatannya masih dilakukan secara manual, sehingga sangat mudah diduplikasi atau dibuat ulang oleh pihak yang tidak berhak secara bebas [1]. Risiko ini secara langsung mengancam legalitas data validasi sertifikat, sehingga menimbulkan kebutuhan mendesak akan solusi keamanan tingkat tinggi yang bersifat *anti-forgery* [5].

Sebagai solusi, sistem baru yang dirancang akan menggantikan peran *QR Code* manual tersebut dengan teknologi *QR Code* terenkripsi untuk menjamin integritas data di dalamnya, digunakan algoritma *Advanced Encryption Standard* (AES-128) yang memiliki kekuatan keamanan tinggi berdasarkan kunci rahasia yang kompleks [6]. Secara eksplisit, data yang akan diproteksi meliputi NIM, Nama Mahasiswa, serta keempat komponen skor *ETP* yaitu *Listening, Structure, Reading,* dan Total skor *TOEFL* yang akan melalui proses enkripsi terlebih dahulu menjadi *ciphertext* sebelum disematkan ke dalam *QR Code*.

Hasil dari proses enkripsi tersebut berupa *ciphertext* yang kemudian disematkan langsung ke dalam *QR Code*. Saat proses verifikasi dilakukan, *QR Code* tersebut dipindai untuk mengekstrak *ciphertext*, yang selanjutnya didekripsi kembali untuk divalidasi dengan database pusat. Implementasi *AES-128* ini telah terbukti efektif dalam memberikan solusi pengamanan dokumen digital di lingkungan lembaga pendidikan [4]. Penggunaan *QR Code* yang berisi *ciphertext AES-128* ini memberikan kontribusi unik dalam menutup celah duplikasi *QR Code* manual yang selama ini terjadi, sekaligus memastikan bahwa seluruh komponen nilai dalam Sertifikat *ETP* benar-benar berasal dari sumber yang sah dan tidak mengalami perubahan [7].

Penggabungan *AES* dengan skema validasi visual, seperti *QR Code*, telah teruji efektivitasnya dalam menjamin keamanan informasi. Penelitian menunjukkan bahwa penerapan *AES* ke dalam URL atau data yang dikonversi menjadi parameter keaslian pada kartu identitas berhasil menjamin integritas data secara signifikan [8]. Teknologi *QR Code* dipilih karena mampu menyimpan informasi terenkripsi dalam

kapasitas yang lebih besar serta memiliki fitur perbaikan kesalahan (*error correction*) yang lebih baik dibandingkan *barcode* konvensional [9].

Meskipun telaah pustaka menunjukkan keberhasilan *AES-128* dalam pengamanan data dan legalisasi umum, posisic masalah yang diteliti ini berfokus pada kekosongan solusi *anti-forgery* spesifik terhadap pemalsuan *QR Code* manual pada Sertifikat *ETP* yang beredar di lingkungan akademik. Berbeda dengan studi lain yang sering menggunakan skema super-enkripsi hibrida untuk *digital signature* [8], penelitian ini secara langsung menciptakan lapisan keamanan (*anti-forgery*) untuk menghilangkan risiko duplikasi *QR Code* manual yang sebelumnya mudah dibuat secara bebas [1]. Model implementasi ini menyematkan *ciphertext* hasil enkripsi *AES-128* ke dalam *QR Code* sebagai parameter keaslian utama. Dengan demikian, penelitian ini memberikan solusi praktis yang terfokus pada pencegahan pemalsuan spesifik Sertifikat *ETP* melalui pembuktian pesan acak yang hanya dapat dikembalikan ke data awal secara sempurna melalui kunci yang tepat [7].

B. Perumusan Masalah

Dari latar belakang yang telah dipaparkan di atas, maka bisa ditarik rumusan masalah yang akan menjadi tujuan pada proposal penelitian ini adalah bagaimana merancang dan mengimplementasikan sistem pencegahan pemalsuan *QR Code* manual pada Sertifikat *ETP* dengan mengintegrasikan enkripsi data validasi menggunakan Algoritma *AES-128* ke dalam *QR Code* di UPA Bahasa UMRAH?

C. Batasan Penelitian

Dari konteks latar belakang proposal dan perumusan masalah, ada beberapa batasan yang diperlukan, antaranya adalah:

1. Penelitian ini dibatasi pada implementasi di Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji (UMRAH).
2. Penelitian ini tidak mencakup pengujian atau perbandingan dengan varian *AES* lainnya (*AES-192* atau *AES-256*), atau algoritma hibrida kunci asimetris (seperti *RSA* atau *DSA*).

3. Penelitian tidak mencakup analisis kerentanan jaringan, aspek legalitas tanda tangan elektronik secara mendalam, atau dampak *QR Code* pada kualitas *file* dokumen (PDF/DOCX).
4. Penelitian ini hanya berfokus pada dokumen digital dalam format PDF, sistem tidak dirancang untuk memproses dokumen hasil *scan*, foto, maupun sertifikat fisik yang sudah dicetak.

D. Tujuan Penelitian

Tujuan utama dalam penelitian ini adalah membuat purwarupa aplikasi berbasis *web* yang mampu menerapkan mekanisme enkripsi data validasi menggunakan Algoritma *AES-128* yang terintegrasi dengan *QR Code,* serta membuat modul verifikasi yang mampu mendekripsi data tersebut, sebagai solusi pencegahan pemalsuan Sertifikat *ETP*.

E. Manfaat Penelitian

Berikut adalah beberapa manfaat dari hasil penelitian yang diharapkan oleh penulis:

1. Manfaat untuk Institusi, hasil penelitian ini dapat menjadi kontribusi praktis dalam mengatasi celah keamanan *QR Code* manual yang rentan pemalsuan, sehingga meningkatkan keamanan dokumen dan menjaga reputasi serta kepercayaan publik terhadap UPA Bahasa dan Universitas Maritim Raja Ali Haji.
2. Manfaat untuk Pembaca, diharapkan pembaca dapat memperoleh pemahaman mendalam mengenai implementasi kriptografi (*AES-128*) dalam pengamanan dokumen akademik digital dan dapat dijadikan referensi untuk penelitian serupa di institusi pendidikan lainnya.
3. Manfaatnya untuk Masyarakat, diharapkan hasil penelitian ini dapat menjamin keaslian dan keabsahan Sertifikat *ETP* yang mereka miliki di mata pihak ketiga (perusahaan atau institusi lain), serta memfasilitasi proses verifikasi keaslian dokumen secara cepat dan mudah melalui pemindaian *QR Code*.