BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi mendorong terjadinya transformasi digital di berbagai bidang, termasuk dalam dunia pendidikan dan pelatihan. Salah satu bentuk implementasinya adalah penggunaan sertifikat sebagai bukti bahwa seseorang telah menyelesaikan suatu program pembelajaran atau pelatihan tertentu. Sertifikat tidak hanya berfungsi sebagai dokumen administratif, tetapi juga menjadi bentuk pengakuan atas kompetensi yang dimiliki seseorang. Sertifikat sering digunakan dalam berbagai keperluan seperti melamar pekerjaan, melanjutkan pendidikan, maupun sebagai portofolio profesional. Maka dengan demikian keberadaan sertifikat harus dapat dipertanggungjawabkan keasliannya agar tidak menimbulkan keraguan bagi pihak yang menggunakan dokumen tersebut (Zulkarnaim & Mansyur, 2024).

Our Learning Center (OLC) Kampung Inggris Kuningan merupakan lembaga pendidikan nonformal yang bergerak di bidang pelatihan bahasa Inggris yang berlokasi di Jl. Kelurahan, Cirendang, Kecamatan Kuningan, Kabupaten Kuningan, Jawa Barat. Dalam setiap program pembelajaran, OLC menerbitkan Certificate of Completion sebagai bukti bahwa peserta telah menyelesaikan proses pembelajaran. Setiap program terdiri dari tiga level pembelajaran, sehingga peserta akan memperoleh sertifikat pada setiap level yang berhasil diselesaikan. Sertifikat yang diterbitkan memuat beberapa informasi penting seperti nama peserta, nama program, tanggal penyelesaian, nilai, serta nomor sertifikat yang dikeluarkan oleh lembaga.

Berdasarkan hasil wawancara yang telah dilakukan, proses verifikasi sertifikat di OLC masih memiliki beberapa keterbatasan. Data peserta yang telah memperoleh sertifikat saat ini disimpan menggunakan layanan Google Drive dengan informasi yang tersimpan relatif terbatas seperti nama dan alamat peserta. Proses verifikasi keaslian sertifikat juga masih dilakukan secara

manual dengan memeriksa cap lembaga dan tanda tangan yang terdapat pada sertifikat atau dengan melakukan konfirmasi langsung kepada pihak OLC. Metode tersebut memiliki keterbatasan karena belum didukung oleh sistem teknologi yang mampu menjamin keaslian serta keutuhan data sertifikat. Kondisi ini menyebabkan sertifikat yang diterbitkan berpotensi mengalami manipulasi atau perubahan data. Hal ini sejalan dengan laporan mengenai dokumen hasil pemindaian yang mengalami perubahan isi setelah dipindai ke dalam bentuk digital. Berdasarkan hasil kuesioner pra-penelitian terhadap 28 responden, sebanyak 83,1% menyatakan bahwa proses verifikasi keaslian sertifikat masih membutuhkan cara yang lebih mudah dan cepat dibandingkan metode yang digunakan saat ini.

Keterbatasan tersebut menyebabkan keaslian sertifikat sulit untuk dipastikan oleh pihak lain yang membutuhkan dokumen tersebut. Padahal, sertifikat seharusnya memiliki mekanisme verifikasi yang memungkinkan pengguna umum memeriksa keaslian dokumen secara langsung sehingga dapat dipastikan apakah sertifikat tersebut benar-benar otentik atau tidak (Lorien & Wellem, 2021). Selain itu, maraknya kasus pemalsuan dokumen seperti ijazah maupun sertifikat kompetensi juga menunjukkan bahwa sistem verifikasi yang hanya mengandalkan pemeriksaan secara manual sudah tidak lagi efektif. Hal ini menunjukkan bahwa dokumen masih dapat mengalami perubahan apabila tidak dilengkapi dengan mekanisme verifikasi yang efektif (Amaludin & Rahmatulloh, 2024).

Salah satu pendekatan yang dapat digunakan untuk menjaga keaslian dokumen adalah dengan memanfaatkan teknologi kriptografi melalui penerapan digital signature. Digital signature memungkinkan suatu dokumen memiliki identitas autentik yang dapat diverifikasi serta memastikan bahwa isi dokumen tidak mengalami perubahan setelah diterbitkan (Arwah et al., 2024). Dalam implementasinya, teknologi ini sering dikombinasikan dengan QR Code untuk mendukung proses verifikasi dokumen. QR Code merupakan kode dua dimensi yang mampu menyimpan informasi dalam jumlah lebih besar

dibandingkan barcode serta dapat dimanfaatkan pada sertifikat untuk mempermudah proses verifikasi sertifikat (Mulyawan & Asmunin, 2024).

Salah satu algoritma yang banyak digunakan dalam penerapan digital signature adalah Elliptic Curve Digital Signature Algorithm (ECDSA). Algoritma ini merupakan algoritma digital signature yang memanfaatkan kurva eliptik dan memiliki kekuatan keamanan yang tinggi pada setiap bit kuncinya dibandingkan algoritma kriptografi konvensional (Arwah et al., 2024). Selain itu, ECDSA mampu memberikan tingkat keamanan yang setara dengan algoritma digital signature lainnya meskipun menggunakan panjang kunci yang lebih pendek (Mallouli et al., 2025). Karakteristik tersebut menjadikan ECDSA sesuai untuk diterapkan pada sistem verifikasi sertifikat berbasis QR Code. Dengan memanfaatkan ECDSA, setiap sertifikat dapat memiliki digital signature yang unik dan hanya dapat dibuat oleh sistem resmi lembaga penerbit. Hal ini membantu memastikan bahwa dokumen yang beredar merupakan dokumen yang asli dan tidak mengalami perubahan.

Berdasarkan permasalahan tersebut, diperlukan suatu sistem yang mampu membantu proses verifikasi keaslian sertifikat secara cepat dan mudah. Melalui penerapan QR Code yang memuat digital signature berbasis ECDSA, proses verifikasi sertifikat dapat dilakukan dengan memindai kode yang terdapat pada sertifikat sehingga status keaslian dokumen dapat diketahui secara langsung. Oleh karena itu, penelitian ini mengangkat judul **"Rancang Bangun Aplikasi Web Verifikasi Keaslian 'Certificate of Completion' Berbasis QR Code Menggunakan Digital Signature ECDSA"** dengan tujuan untuk membantu meningkatkan validitas serta kemudahan dalam proses verifikasi sertifikat pada OLC Kampung Inggris Kuningan guna meminimalisir risiko manipulasi.

1.2 Identifikasi Masalah

Dari latar belakang masalah yang telah diuraikan, maka peneliti mengidentifikasi masalah sebagai berikut:

1. Proses verifikasi keaslian sertifikat di OLC masih dilakukan secara manual melalui pemeriksaan cap lembaga dan tanda tangan pada dokumen, Sehingga kurang efisien waktu dan bergantung pada pihak penerbit. Adanya laporan kasus pemalsuan data sertifikat menunjukkan bahwa metode verifikasi yang digunakan saat ini masih memiliki keterbatasan dalam memastikan keaslian sertifikat. Hasil kuesioner kepada 28 responden menunjukkan 83,1% responden berpendapat bahwa proses verifikasi sertifikat perlu dilakukan dengan cara yang lebih mudah dan cepat.
2. Sertifikat yang diterbitkan OLC belum memiliki mekanisme verifikasi digital yang dapat digunakan oleh pengguna umum untuk memverifikasi keaslian sertifikat secara mandiri.

1.3 Rumusan Masalah

Berdasarkan identifikasi masalah yang telah dipaparkan, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana merancang dan membangun sistem verifikasi sertifikat berbasis web pada Certificate Of Completion yang di terbitkan OLC?.
2. Bagaimana mengimplementasikan algoritma Elliptic Curve Digital Signature Algorithm (ECDSA) pada sistem verifikasi keaslian sertifikat yang digenerate kedalam bentuk QR Code?.

1.4 Batasan Masalah

Agar penelitian ini lebih terfokus dan dapat diselesaikan dengan sumber daya yang tersedia, maka batasan masalah ditetapkan sebagai berikut:

1. Objek yang digunakan dalam penelitian ini adalah Certificate of Completion yang diterbitkan oleh OLC Kampung Inggris Kuningan untuk program *speaking*.

2. Sistem verifikasi hanya digunakan untuk memverifikasi keaslian sertifikat yang diterbitkan oleh OLC Kampung Inggris Kuningan. Sistem tidak dirancang untuk memproses sertifikat dari lembaga lain.
3. Penelitian ini difokuskan pada proses verifikasi keaslian sertifikat menggunakan algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) dengan fungsi SHA-256 untuk menghasilkan nilai hash dokumen. Penelitian ini tidak membahas secara detail mengenai manajemen kursus maupun pengelolaan peserta.
4. Pengguna sistem terdiri dari dua jenis, yaitu Admin dan Pengguna Umum (Stakeholder atau Masyarakat), dengan hak akses sebagai berikut:
    a. Admin
        - Mengelola data sertifikat, meliputi proses tambah, ubah, hapus dan lihat data sertifikat.
        - Melihat history verifikasi sertifikat yang dilakukan oleh pengguna umum.
        - Dapat menghasilkan QR Code sertifikat secara otomatis pada setiap sertifikat yang diterbitkan.
    b. Pengguna umum (Stakeholder atau Masyarakat)
        - Dapat melakukan verifikasi keaslian sertifikat yang di terbitkan OLC.
        - Scan QR Code pada sertifikat untuk membuka halaman verifikasi dan melihat status keaslian beserta informasi sertifikat.
5. Penggunaan Algoritma ECDSA dan QR Code :
    a. Algoritma ECDSA digunakan untuk melakukan proses enkripsi pada sertifikat dan di generate ke dalam QR Code pada saat admin mengelola data sertifikat.
    b. Pengguna umum melakukan scan QR Code dan menghasilkan link, dimana ketika diklik sistem akan membuka website verifikasi kemudian sistem melakukan dekripsi nomor sertifikat yang terdapat pada link sebelum nya dan menampilkan data sertifikat.

6. Aplikasi berbasis web dikembangkan menggunakan framework Laravel dan database MySQL, sehingga sistem dapat diakses melalui web browser untuk melakukan proses verifikasi keaslian sertifikat melalui QR Code.
7. Penelitian ini menggunakan QR Code Static Model 2 yang dicetak pada sertifikat dengan ukuran 3 cm × 3 cm.

1.5 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan, maka tujuan dari penelitian ini adalah :

1. Merancang dan membangun sistem verifikasi keaslian sertifikat berbasis web pada Certificate of Completion yang diterbitkan oleh OLC Kampung Inggris Kuningan sehingga proses verifikasi dapat dilakukan secara lebih cepat dan mudah.
2. Mengimplementasikan algoritma Elliptic Curve Digital Signature Algorithm (ECDSA) yang digenerate ke dalam QR Code untuk mendukung proses verifikasi keaslian dan keutuhan data sertifikat.

1.6 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat bagi berbagai pihak, di antaranya:

1. Bagi Penulis

   Menambah pengetahuan dan pengalaman dalam penerapan algoritma Elliptic Curve Digital Signature Algorithm pada sistem verifikasi sertifikat berbasis QR Code.

2. Bagi OLC Kampung Inggris Kuningan

   Membantu menyediakan sistem verifikasi sertifikat yang lebih aman dan terstruktur, sehingga memudahkan pihak lembaga dalam memastikan keaslian sertifikat yang diterbitkan serta meningkatkan kepercayaan terhadap sertifikat Certificate of Completion yang dikeluarkan oleh OLC.

3. Bagi Peserta atau Pengguna Umum

   Memudahkan peserta atau pihak lain dalam melakukan verifikasi keaslian sertifikat secara mandiri melalui QR Code, sehingga dapat mengurangi risiko pemalsuan sertifikat dan memastikan informasi yang terdapat pada sertifikat merupakan data yang sah.

4. Bagi Akademisi atau Peneliti Selanjutnya

   Menjadi referensi bagi penelitian selanjutnya yang berkaitan dengan penerapan kriptografi, khususnya penggunaan algoritma Elliptic Curve Digital Signature Algorithm pada sistem verifikasi dokumen digital berbasis QR Code.