BAB I
PENDAHULUAN

1.1 Latar Belakang Penelitian

Pada era digital saat ini, teknologi berkembang sangat pesat, para peneliti berlomba-lomba dalam mengembangkan sistem yang dapat memudahkan pekerjaan manusia dan salah satunya dalam mengelola data. Di bidang pendidikan, peralihan data manual menjadi data digital sudah tidak dapat dipungkiri lagi, karena data digital lebih mudah diakses, secara lebih efektif dan efisien. Data yang berharga dan penting masih dilakukan secara konvensional dengan alasan lebih terjamin keasliannya dan lebih aman pada sisi keamanan, tetapi kenyataannya masih banyak sekali orang yang melakukan kecurangan terhadap data. Sebagai contoh beberapa kasus seperti pemalsuan ijazah, rapor, ataupun sertifikat yang beredar di Indonesia dan diperjual belikan yang belum dapat dipastikan keasliannya (Febriyanto dkk., 2020).

Sertifikat merupakan dokumen resmi yang digunakan sebagai bukti bahwa seseorang telah mengikuti suatu kegiatan atau meraih pencapaian tertentu. Dalam ranah pendidikan maupun kompetisi, sertifikat berfungsi sebagai bentuk penghargaan, pengakuan partisipasi, maupun rekam jejak capaian yang sah. Menurut Javier dan Dinata (2023), sertifikat menjadi bukti keikutsertaan seseorang dalam suatu kegiatan seperti seminar atau pelatihan, sehingga perlu dijaga keasliannya agar tidak disalahgunakan. Sertifikat tidak hanya bernilai simbolik, tetapi juga administratif, karena seringkali dibutuhkan sebagai dokumen pelengkap dalam dunia pendidikan atau profesional. Oleh karena itu, menjaga keautentikan sertifikat dalam sistem digital menjadi aspek penting yang perlu mendapat perhatian khusus.

Perbuatan pemalsuan dapat digolongkan pertama-tama dalam kelompok kejahatan “penipuan”, namun tidak semua perbuatan penipuan adalah pemalsuan. Perbuatan pemalsuan tergolong kelompok kejahatan penipuan, apabila seseorang memberikan gambaran tentang sesuatu keadaan atas sesuatu barang (surat) seakan-akan asli atau benar tersebut dimilikinya. Karena gambarannya ini orang lain terpedaya dan mempercayai bahwasanya keadaan yang digambarkan atas barang/ surat tersebut itu adalah benar. Pemalsuan terhadap tulisan/ surat terjadi apabila

isinya atas surat itu yang tidak benar digambarkan sebagai benar (M.C. Sholeh., 2021).

Berdasarkan informasi yang diper*oleh* dari situs resmi Pemerintah Provinsi Jawa Tengah, ditemukan adanya kasus dugaan pemalsuan piagam lomba yang digunakan sebagai syarat seleksi Penerimaan Peserta Didik Baru (PPDB) tahun 2024. Kasus ini mencuat setelah adanya temuan bahwa sejumlah siswa diduga menggunakan piagam palsu untuk memper*oleh* poin tambahan dalam proses seleksi. Penjabat Gubernur Jawa Tengah, Nana Sudjana, merespons tegas temuan tersebut dengan menginstruksikan pembatalan nilai tambahan bagi siswa yang terbukti menggunakan dokumen tidak sah serta mendorong pengusutan lebih lanjut terhadap pihak-pihak yang terlibat. Kasus ini mencerminkan bahwa pemalsuan sertifikat lomba tidak hanya menimbulkan ketidakadilan dalam proses seleksi pendidikan, tetapi juga merusak integritas sistem pendidikan secara keseluruhan. Kurangnya sistem verifikasi keaslian dokumen yang kuat menjadi celah utama terjadinya praktik curang tersebut.

Untuk menutup celah ini, diperlukan metode verifikasi digital yang dapat memastikan bahwa setiap sertifikat memiliki identitas unik yang tidak dapat dipalsukan. Salah satu solusi yang efektif adalah dengan melakukan proses *hashing* pada data sertifikat. Menurut Prabowo & Afrianto (2017) sertifikat perlu di *hashing* karena *hashing* berfungsi untuk memastikan integritas dan keaslian dokumen digital. Nilai *hash* yang dihasilkan bersifat unik untuk setiap isi sertifikat, sehingga jika ada perubahan sekecil apa pun pada data sertifikat, hasil *hash* akan berbeda secara signifikan. Hal ini membuat proses pemalsuan atau modifikasi data menjadi sangat sulit dilakukan tanpa terdeteksi. Dengan kata lain, *hashing* dapat menjadi "sidik jari digital" bagi sertifikat, yang mampu membedakan antara dokumen asli dan dokumen yang telah dimanipulasi, sehingga keamanannya lebih terjamin.

Salah satu teknologi yang dapat diimplementasikan untuk menjawab tantangan pemalsuan dokumen digital adalah algoritma SHA-256, bagian dari keluarga *Secure Hash Algorithm* (SHA). Algoritma SHA-256 mengubah pesan masukan menjadi *message digest* tetap berukuran 256-bit dan bersifat satu arah sehingga pesan asli tidak dapat dikembalikan dari hasil *hash* (Wijayanto & Waliyullah, 2024). Algoritma ini dirancang untuk menghasilkan nilai *hash*

sepanjang 256 bit yang unik dan sulit untuk direkayasa balik. SHA-256 memiliki kemampuan mendeteksi perubahan sekecil apa pun pada data asli, karena setiap perubahan akan menghasilkan *hash* yang berbeda secara signifikan (Refialy dkk., 2022).

Namun demikian, untuk meningkatkan kekuatan keamanan dari proses *hashing* ini, dibutuhkan elemen tambahan salah satunya *salt*. *Salt* merupakan data acak yang ditambahkan ke dalam input sebelum dilakukan proses *hashing*, sehingga dua data yang identik sekalipun akan menghasilkan *output hash* yang berbeda. Teknik ini mampu memperkuat kerahasiaan data dan membuat serangan menjadi tidak efektif. Menurut Pramod dkk. (2021), penggunaan *salt* dalam proses *hashing* dapat meningkatkan keamanan dengan menciptakan *output* yang tidak dapat diprediksi meskipun input awalnya serupa. Dengan demikian, integritas dan keaslian data digital dapat lebih terjamin.

Oleh karena itu, algoritma ini sangat sesuai untuk menjamin integritas dan keaslian dokumen digital, termasuk sertifikat lomba (Daulay dkk., 2022). Penerapan SHA-256 dalam sistem berbasis web tidak hanya memberikan perlindungan terhadap pemalsuan, tetapi juga sejalan dengan peraturan hukum yang berlaku di Indonesia. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE), khususnya Pasal 35, melarang segala bentuk manipulasi atau penciptaan informasi elektronik yang dimaksudkan agar dianggap seolah-olah data tersebut otentik. Dengan menggunakan SHA-256, sistem keamanan dapat memastikan bahwa setiap sertifikat digital yang dikeluarkan memiliki identitas kriptografis yang tidak dapat diubah atau ditiru secara sembarangan.

Untuk menunjang proses verifikasi yang praktis dan efisien, sistem ini juga memanfaatkan QR *Code* (*Quick Response Code*) sebagai media penyimpan kode *hash*. QR *Code* merupakan representasi visual dua dimensi yang dapat memuat informasi dalam jumlah besar dan dapat dipindai dengan cepat menggunakan kamera *smartphone* atau pemindai khusus. Dalam konteks ini, QR *Code* digunakan untuk memudahkan proses validasi sertifikat secara digital melalui pemindaian langsung. Teknologi ini telah terbukti efektif dalam berbagai sistem keamanan

karena sifatnya yang cepat, mudah diakses, dan mampu diintegrasikan dengan sistem digital secara fleksibel (Az-Zahra dkk., 2024).

Dengan menggabungkan algoritma SHA-256 dan QR *Code*, penelitian ini bertujuan untuk merancang serta mengimplementasikan sistem berbasis web yang mampu menghasilkan dan memverifikasi sertifikat lomba secara digital. Pendekatan ini diharapkan dapat mengurangi risiko pemalsuan, memperkuat kepercayaan terhadap keaslian dokumen, serta memberikan solusi digital yang aman dan efisien dalam proses validasi sertifikat.

1.2 Rumusan Masalah Penelitian

Berdasarkan latar belakang yang telah diuraikan, penelitian ini memiliki beberapa rumusan masalah:

1. Bagaimana merancang web yang memanfaatkan algoritma SHA-256 *salt* dan QR-*code* untuk memastikan keaslian dan verifikasi sertifikat?
2. Bagaimana kinerja SHA-256 dan *salt* dalam memastikan keaslian, keamanan serta memverifikasi sertifikat?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1. Merancang dan membangun sistem berbasis web yang mampu mengimplementasikan algoritma SHA-256, *salt* dan QR Code sebagai solusi untuk verifikasi keaslian sertifikat digital.
2. Menganalisis kinerja dari penerapan algoritma SHA-256 yang dikombinasikan dengan *salt* untuk mengukur efektivitasnya dalam mengamankan data dan menjaga keaslian sertifikat.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1.4.1. Manfaat Teoritis

1. Memberikan kontribusi ilmiah terhadap pengembangan teknologi keamanan dokumen berbasis algoritma *hash*, khususnya penggunaan SHA-256 yang dikombinasikan dengan *salt* untuk meningkatkan keunikan hasil *hashing*.

2. Menjadi referensi akademik bagi penelitian lanjutan yang ingin mengkaji implementasi metode *hash* dan verifikasi digital dalam menjaga keaslian dokumen berbasis web.

1.4.2. Manfaat Praktis

1. Sistem ini dapat membantu lembaga pendidikan, pelatihan, maupun institusi lain dalam menjamin keaslian sertifikat melalui penerapan algoritma *hash* dan pemanfaatan QR *Code* sebagai alat verifikasi.
2. Memberikan solusi praktis bagi instansi dalam mengelola penerbitan dan verifikasi sertifikat digital secara otomatis, tanpa perlu proses manual atau pencocokan fisik dokumen.
3. Penggunaan QR *Code* yang mengarah langsung ke halaman verifikasi memungkinkan pengguna untuk memvalidasi keaslian sertifikat secara cepat dan mudah hanya dengan pemindaian.
4. Meningkatkan efisiensi operasional karena seluruh proses, mulai dari pembuatan hingga validasi sertifikat, dilakukan secara terpusat melalui platform berbasis web.
5. Memberikan gambaran implementatif bagi pengembang sistem yang ingin membangun aplikasi serupa dalam konteks keamanan dan keaslian dokumen digital berbasis web.

1.5 Ruang Lingkup Penelitian

Ruang lingkup dalam penelitian ini di antaranya:

1. Penelitian ini difokuskan pada pengembangan sistem web untuk pembuatan dan verifikasi sertifikat digital menggunakan algoritma SHA-256 yang dikombinasikan dengan nilai *salt* untuk menghasilkan kode *hash* yang unik dan tidak dapat ditebak.
2. Sistem hanya memproses data berupa input teks seperti nama peserta, nama kegiatan, tanggal kegiatan, dan status juara yang kemudian digabungkan untuk proses *hashing*.
3. QR *Code* dihasilkan secara otomatis dari hasil *hashing* dan disimpan dalam *Database* sebagai *file* gambar, yang kemudian digunakan kembali saat proses pembuatan sertifikat dan verifikasi.

4. Proses verifikasi dilakukan berdasarkan pemindaian QR *Code* yang akan mencocokkan data dari *Database* dan menampilkan status keaslian sertifikat.
5. Sistem diuji hanya untuk menerapkan SHA-256 dan salt sebagai verifikasi dan autentifikasi sertifikat di lingkungan lokal dan tidak mencakup uji implementasi pada lingkungan lainnya.
6. Evaluasi sistem hanya mencakup pengujian *black box* untuk fungsionalitas fitur dan pengujian keaslian menggunakan korelasi *Pearson* untuk memastikan tingkat keacakan dari hasil *hashing*.
7. Dalam penelitian ini sertifikat yang digunakan untuk pengujian adalah sertifikat perlombaan, namun tidak menutup kemungkinan digunakan untuk sertifikat lainnya.

1.6 Struktur Organisasi Skripsi

Secara sistematika penulisan dalam penyusunan laporan penelitian terdapat rangkaian pembahasan setiap babnya, antara lain:

1. BAB I: PENDAHULUAN

   Memberikan gambaran umum penelitian, dimulai dari konteks yang menjelaskan pentingnya mengelola kredensial dengan aman di era digital. Kemudian dipaparkan pokok permasalahan yang diangkat dalam penelitian, dilanjutkan dengan tujuan penelitian yang ingin dicapai. Bab ini juga menguraikan manfaat teoritis dan praktis yang diharapkan dari hasil penelitian.

2. BAB II : KAJIAN PUSTAKA

   Mengulas literatur-literatur yang berkaitan dengan penelitian. Konsep dasar seperti sertifikat, algoritma *hashing*, keamanan data digital, dan sistem berbasis web dijelaskan. Selain itu, tinjauan terhadap penelitian terdahulu disajikan untuk menunjukkan posisi penelitian ini dalam konteks ilmiah yang lebih luas.

3. BAB III : METODE PENELITIAN

   Menjelaskan tentang pendekatan dan metode yang digunakan dalam penelitian, meliputi pengumpulan data, perancangan sistem berbasis web, dan implementasi algoritma *hashing*. Desain eksperimen untuk

mengevaluasi keandalan sistem juga dijelaskan secara rinci, termasuk parameter yang digunakan untuk mengukur efektivitas sistem.

4. BAB IV : HASIL DAN PEMBAHASAN

   Menyajikan hasil penerapan sistem berbasis web yang dikembangkan, termasuk proses penerapan algoritma *hash* untuk menghasilkan dan memverifikasi *hash* sertifikat unik. Analisis hasil pengujian dengan pembahasan mendalam dilakukan untuk mengevaluasi efektivitas sistem dalam mendeteksi sertifikat palsu dan membandingkan hasil penelitian ini dengan literatur terkait.

5. BAB V : KESIMPULAN DAN SARAN

   Merangkum kesimpulan utama penelitian khususnya terkait penerapan algoritma *hashing* dan efektivitas sistem dalam menjamin keakuratan keaslian sertifikat lomba. Selain itu juga diberikan saran untuk pengembangan lebih lanjut seperti mengintegrasikan teknologi tambahan atau memperluas cakupan penelitian ke aspek keamanan lainnya.