

BAB I

PENDAHULUAN

1.1 Latar Belakang

Terlepas dari keberadaan komputer dan internet, kemajuan dalam teknologi informasi telah membuat proses pertukaran informasi semakin mudah. Akan tetapi, bersama dengan kemajuan teknologi, muncul masalah baru, yaitu ancaman terhadap keamanan data. Ketika orang bertukar data, data plainteks adalah sebuah bagian dari transaksi, dan jika ada pihak yang berhasil menyadapnya, pihak tersebut dapat dengan mudah mengubah data sebelum sampai ke penerima sebenarnya. [1]

SHA-256 diperkenalkan untuk mengatasi kelemahan algoritma hash generasi sebelumnya. Algoritma hash sebelumnya seperti SHA-1 yang mulai rentan terhadap *collision* atau serangan tabrakan hash. Pada hari Kamis, 23 Februari, Google mengumumkan bahwa tim penelitiannya dari *CWI Institute* di Amsterdam berhasil menunjukkan serangan pada algoritma hash SHA-1 dengan membuat dua file dengan hash nilai yang sama. Penemuan ini menunjukkan bahwa perlunya migrasi algoritma hash yang lebih kuat diperlukan untuk tanda tangan digital dan aplikasi lain yang membutuhkan ketahanan terhadap tabrakan. [2] Secara khusus, karakteristik seperti deterministik atau sifat dari sebuah fungsi hash di mana untuk setiap input yang sama, fungsi tersebut akan selalu menghasilkan output yang sama pula tanpa perubahan, membuat SHA-256 menjadi standar dalam berbagai aplikasi keamanan digital, mulai dari tanda tangan digital, hingga perlindungan kata sandi. Inilah yang membuat SHA-256 menjadi fondasi inti dalam memberikan keamanan data dan menjaminya integritas di era digital. [3]

Secure Hash Algorithm-256 (SHA-256) adalah salah satu algoritma dalam keluarga SHA-256 yang dirancang oleh *National Security Agency* (NSA) dan diadopsi sebagai standar oleh *National Institute of Standards and Technology* (NIST) pada tahun 2001. SHA-256 merupakan fungsi hash kriptografis yang menghasilkan nilai hash sepanjang 256-bit atau 32- *byte* dari data input berukuran

berapa pun. Fungsi hash ini bersifat satu arah (*one way function*), artinya nilai hash yang dihasilkan tidak dapat dengan mudah dikembalikan ke data aslinya [4], Studi [5] menunjukkan bahwa serangan collision potensial hanya dapat digunakan pada versi SHA-256 dengan jumlah ronde yang dikurangi, yang menunjukkan bahwa hingga saat ini belum ada serangan yang berhasil menghasilkan collision pada versi SHA-256 yang umum digunakan. Ini menunjukkan bahwa SHA-256 adalah algoritma hash yang aman dan tahan terhadap serangan praktis maupun teoritis.

Kedai Kopi Kambodja adalah salah satu usaha lokal yang terletak di Bengkalis, Riau. Sejak didirikan sekitar tahun 2024, kedai ini telah berkembang menjadi salah satu tempat warga untuk menikmati kopi dan makanan ringan serta tempat yang aktif untuk berinteraksi dengan orang lain. Bisnis ini masih mengelola secara konvensional, seperti pencatatan transaksi penjualan secara manual menggunakan buku tulis. Metode pencatatan manual ini memang sederhana dan tidak memerlukan biaya besar, namun seiring meningkatnya volume transaksi dan kebutuhan akan pelaporan keuangan yang lebih akurat, pendekatan ini mulai menunjukkan berbagai kelemahan. Beberapa permasalahan yang kerap muncul antara lain adalah data yang rawan hilang atau rusak, risiko *human error* dalam penulisan atau penghitungan, serta sulitnya melakukan rekapitulasi atau analisis pendapatan dalam jangka waktu tertentu. Dengan mengelola sistem menjadi efisien, kedai kopi kambodja dapat memperoleh keunggulan kompetitif dibandingkan dengan pesaingnya. Menurut [6] disarankan untuk membangun sistem atau aplikasi berbasis web yang mudah digunakan untuk memudahkan proses pengolahan dan penyebaran data.

Studi yang dibahas oleh [7] membahas bagaimana UMKM dapat menggunakan aplikasi pencatatan transaksi penjualan berbasis web. Studi ini berfokus pada UMKM Wonderful Rotan di Kabupaten Bandung Barat. Tujuan utama dari penelitian ini adalah membantu usaha kecil dan menengah (UMKM) dalam mencatat transaksi penjualan tunai dan kredit, mengelola inventaris, dan menyajikan laporan penjualan dan buku besar dengan benar dan efisien. Aplikasi dibangun menggunakan metode SDLC model waterfall dan menggunakan teknologi berbasis Laravel dan PostgreSQL secara langsung. Hasil akhir

menunjukkan bahwa aplikasi membantu usaha kecil dan menengah (UMKM) mencatat dan menyampaikan data keuangan harian dengan lebih efisien. Di sisi lain, penelitian oleh [8] menyelidiki penerapan algoritma SHA-256 dalam mengamankan password pengguna melalui simulasi pengujian terhadap berbagai jenis serangan, seperti brute force dan rainbow table. Studi tersebut juga menunjukkan bahwa metode tambahan seperti salting dan iterasi hashing dapat meningkatkan kekuatan password, dan SHA-256 dinilai efektif dalam menjaga integritas data asli. Meskipun berasal dari bidang yang berbeda, kedua penelitian ini menunjukkan bahwa efisiensi sistem kerja dan keamanan data sangat penting untuk meningkatkan kepercayaan dan kenyamanan pengguna sistem informasi.

Meskipun kedua penelitian tersebut memberikan kontribusi yang signifikan, terdapat kelemahan penting yang menjadi celah untuk penelitian ini. Studi [7] memberikan solusi yang tepat untuk UMKM dalam pencatatan transaksi penjualan dan laporan keuangan. Namun, penelitian ini hanya membahas aspek fungsional aplikasi secara lokal dan tidak membahas aspek keamanan data, seperti bagaimana data transaksi dapat dilindungi dari orang yang tidak berhak mengaksesnya atau dienkripsi. Selain itu, meskipun penelitian [8] berfokus pada kekuatan algoritma SHA-256 dalam hal keamanan password, mereka belum menggunakannya secara langsung dalam sistem informasi berbasis web yang mengelola data tentang pencatatan transaksi dan kehadiran karyawan.

Berdasarkan dari uraian diatas, maka akan dilakukan sebuah penelitian mengenai “Implementasi Algoritma SHA-256 pada aplikasi pencatatan transaksi dan kehadiran berbasis web di Kedai Kopi Kambojda” yang dapat memudahkan dalam pembuatan aplikasi pencatatan transaksi dan kehadiran secara digital. Sehingga aplikasi yang akan di bangun diharapkan dapat menjadi bagian dari solusi teknologi dalam menghadapi tantangan keamanan digital masa kini.

1.2 Rumusan Masalah

Perumusan masalah penelitian ini dapat disusun menjadi beberapa pertanyaan berikut berdasarkan latar belakang masalah:

1. Bagaimana merancang aplikasi pencatatan transaksi dan kehadiran berbasis web yang sesuai dengan kebutuhan operasional Kedai Kopi Kambodja agar lebih efisien dibandingkan metode manual?
2. Bagaimana algoritma SHA-256 dapat diterapkan pada sistem untuk melindungi data login pengguna apabila data dalam database bocor?
3. Bagaimana efektivitas sistem pencatatan transaksi dan kehadiran berbasis web dengan algoritma SHA-256 dalam meningkatkan keamanan data dan mengurangi risiko kehilangan data dibandingkan metode konvensional?

Pertanyaan-pertanyaan tersebut telah disusun untuk mencerminkan tujuan utama dari penelitian ini, yaitu membangun sistem digital yang efisien, aman, dan fungsional. Selain itu, pertanyaan-pertanyaan tersebut juga bertujuan untuk memberikan jawaban langsung terhadap masalah yang ada di Kedai Kopi Kambodja.

1.3 Batasan Masalah

Agar penelitian ini memiliki ruang lingkup yang jelas dan terfokus, maka batasan masalah dalam penelitian ini ditetapkan sebagai berikut:

1. Penelitian ini hanya membahas pengembangan dan penerapan aplikasi pencatatan transaksi dan kehadiran karyawan berbasis web yang diterapkan pada Kedai Kopi Kambojda sebagai objek penelitian.
2. Aspek keamanan sistem yang dikaji dibatasi pada keamanan autentikasi pengguna, khususnya pengamanan kata sandi menggunakan algoritma hash kriptografis SHA-256.
3. Penerapan algoritma SHA-256 dalam penelitian ini tidak mencakup enkripsi data transaksi, data kehadiran, maupun komunikasi jaringan, melainkan difokuskan pada proses penyimpanan dan verifikasi kata sandi pengguna.
4. Sistem yang dikembangkan hanya melibatkan tiga peran pengguna, yaitu Owner, Kasir, dan Karyawan, dengan pengaturan hak akses sesuai peran masing-masing.

5. Metode pengembangan perangkat lunak yang digunakan dibatasi pada model Waterfall, yang meliputi tahap analisis kebutuhan, perancangan sistem, implementasi, dan pengujian.
6. Pengujian sistem dibatasi pada pengujian fungsional dan pengujian keamanan autentikasi menggunakan pendekatan black-box testing, tanpa melakukan pengujian penetrasi (penetration testing) secara menyeluruh.
7. Sistem yang dikembangkan belum mencakup fitur lanjutan seperti pemesanan online, integrasi pembayaran digital, enkripsi database tingkat lanjut, maupun audit keamanan menyeluruh.

1.4 Tujuan

Dari permasalahan yang ada di dalam kedai kopi kambojda. Penelitian ini bertujuan untuk:

- a. Mengembangkan aplikasi berbasis web untuk mempermudah pencatatan transaksi dan kehadiran di Kedai Kopi Kambodja.
- b. Menerapkan algoritma SHA-256 untuk meningkatkan keamanan data pengguna, khususnya pada proses login dan penyimpanan informasi penting.
- c. Menilai sejauh mana sistem digital ini mampu mengurangi kesalahan pencatatan dan meningkatkan efisiensi serta keamanan dibandingkan metode manual.

Penelitian ini disusun berdasarkan latar belakang dan perumusan masalah yang telah diidentifikasi, Tujuan utama dari penelitian ini adalah untuk menemukan solusi untuk masalah operasional yang terjadi di Kedai Kopi Kambodja. Fokus penelitian ini adalah untuk membuat proses pencatatan transaksi dan kehadiran lebih efisien, akurat, dan aman. Ini dicapai melalui penggunaan pendekatan sistem berbasis web dan algoritma keamanan.

1.4 Manfaat

Penelitian ini dapat membantu UMKM dan penggunanya seperti berikut:

- a. Proses pencatatan transaksi dan kehadiran yang sebelumnya dilakukan secara manual sekarang dilakukan secara otomatis. Ini menghemat waktu dan tenaga dalam mengelola administrasi karyawan.
- b. Aplikasi dapat melindungi data sensitif seperti login pengguna
- c. Akurasi Penghitungan transaksi, Karena data – data yang masuk dihitung secara digital menggunakan parameter yang telah ditentukan, akurasi penghitungan transaksi membantu mengurangi kesalahan.
- d. Mengurangi Risiko Kesalahan serta Kecurangan
- e. Penerapan keamanan data dan kurangnya campur tangan manusia dapat mengurangi kemungkinan *human error* dan manipulasi data.
- f. Kemudahan Akses dan Penggunaan aplikasi berbasis web memiliki antarmuka yang mudah digunakan yang memungkinkan akses dan penggunaan dari mana saja dan kapan saja.