

IMPLEMENTASI ALGORITMA SHA-256 UNTUK VERIFIKASI DIGITAL SIGNATURE PADA SISTEM PEMESANAN E-TIKET WISATA MITRA SIBAYAK BERBASIS WEB

Agus Karlina Br Sitepu, Antoni, Aulia Ichsan
Universitas Islam Sumatera Utara, Medan, Indonesia
Email : aguskarlinasitepu345@gmail.com

Informasi	Abstract
Volume : 3 Nomor : 10 Bulan : Oktober Tahun : 2026 E-ISSN : 3062-9624	<i>The tourism sector at Mitra Sibayak Bathing and Accommodation has high visitor potential; however, its conventional ticket booking system is vulnerable to ticket forgery and duplication of digital tickets. Data security issues and inaccurate ticket verification often result in financial losses for the management and uncertainty for tourists. This study aims to develop a web-based e-ticket booking system integrated with high-level security technology to ensure ticket authentication. The system was developed using the Waterfall methodology, with PHP as the programming language and MySQL as the database management system.</i> <i>To ensure data integrity, the SHA-256 (Secure Hash Algorithm 256-bit) algorithm was implemented as a Digital Signature mechanism. This algorithm works by converting transaction data into a unique hash value that cannot be manipulated, which is then embedded into a QR code for verification in the field. The result of this study is an e-ticketing information system capable of detecting ticket forgery attempts in real time while facilitating the operational management of Mitra Sibayak. System testing was conducted using Black Box Testing to ensure the functionality of the system features, along with an algorithm integrity test to demonstrate the robustness of the digital signature against data manipulation.</i> Keywords: SHA-256, Digital Signature, E-Ticket, Data Security, Mitra Sibayak.

Abstrak

Sektor pariwisata pada Pemandian dan Penginapan Mitra Sibayak memiliki potensi kunjungan yang tinggi, namun sistem pemesanan tiket yang masih konvensional rentan terhadap praktik pemalsuan dan penggandaan tiket digital. Masalah keamanan data dan verifikasi tiket yang tidak akurat seringkali menyebabkan kerugian finansial bagi pengelola serta ketidakpastian bagi wisatawan. Penelitian ini bertujuan untuk membangun sistem pemesanan e-tiket berbasis web yang terintegrasi dengan teknologi keamanan tingkat tinggi untuk menjamin autentikasi tiket. Pengembangan sistem menggunakan metodologi Waterfall dengan bahasa pemrograman PHP dan basis data MySQL. Untuk menjamin integritas data, diterapkan algoritma SHA-256 (Secure Hash Algorithm 256-bit) sebagai mekanisme Digital Signature. Algoritma ini bekerja dengan cara mengonversi data transaksi menjadi nilai hash unik yang tidak dapat dimanipulasi, yang kemudian diimplementasikan ke dalam kode QR untuk proses verifikasi di lapangan. Hasil penelitian ini adalah sebuah sistem informasi e-ticketing yang mampu mendeteksi upaya pemalsuan tiket secara real-time sekaligus mempermudah manajemen operasional Mitra Sibayak. Pengujian sistem dilakukan menggunakan Black Box Testing

untuk memastikan fungsionalitas fitur dan uji integritas algoritma guna membuktikan ketangguhan tanda tangan digital terhadap manipulasi data.

Kata kunci: *SHA-256, Digital Signature, E-Ticket, Keamanan Data, Mitra Sibayak.*

A. PENDAHULUAN

Sektor pariwisata merupakan salah satu penopang ekonomi yang signifikan di wilayah Berastagi, Kabupaten Karo. Salah satu destinasi yang populer adalah Pemandian Air Panas Mitra Sibayak, yang menawarkan daya tarik pemandian air belerang alami serta fasilitas seperti penginapan bagi wisatawan. Namun, seiring dengan meningkatnya jumlah pengunjung, manajemen pemesanan tiket dan pengelolaan kapasitas menjadi tantangan tersendiri. Sistem pemesanan penggunaan tiket fisik rentan terhadap risiko kehilangan, kerusakan, hingga pemalsuan tiket yang dapat merugikan pihak pengelola.

Di era digitalisasi, penggunaan E-Tiket menjadi solusi praktis untuk mempermudah akses wisatawan tanpa harus mengantri panjang di loket fisik. Transformasi digital pada tata kelola destinasi wisata terbukti mampu mendongkrak efisiensi operasional sekaligus memberikan kenyamanan lebih bagi para pelancong (Sitorus & Hasibuan, 2023). Namun, penggunaan tiket digital berbasis kode batang (Barcode) atau QR Code standar memiliki celah keamanan, yaitu kemudahan untuk diduplikasi atau dimanipulasi oleh pihak yang tidak bertanggung jawab (Hidayat & Zulkifli, 2023).

Untuk mengatasi masalah tersebut, diperlukan mekanisme Digital Signature menggunakan Algoritma SHA-256. Algoritma ini mampu menciptakan hash unik yang menjamin keaslian tiket karena sifatnya yang sulit dimanipulasi (Pratama dkk, 2024). Kriptografi SHA-256 bekerja dengan menghasilkan nilai keluaran berukuran tetap yang mustahil untuk didekripsi kembali secara terbalik fungsi hash satu arah (one-way hash function), sehingga sangat tangguh dalam menjaga integritas data tiket dari upaya modifikasi ilegal (Putra & Rahmawati, 2022). Penelitian terdahulu membuktikan bahwa implementasi SHA-256 dapat menekan angka pemalsuan hingga 95% (Saputra, 2022) sekaligus mempercepat proses verifikasi data (Kurniawan, 2023).

Namun, penerapan sistem verifikasi berbasis SHA-256 yang terintegrasi untuk layanan pemandian sekaligus penginapan di Mitra Sibayak belum banyak dieksplorasi. Oleh karena itu, penelitian ini bertujuan mengembangkan Sistem Pemesanan E-Tiket Wisata Mitra Sibayak

Berbasis Web dengan implementasi SHA-256 guna menciptakan proses verifikasi yang lebih aman, transparan, dan efisien bagi pengelola maupun pengunjung.

Berdasarkan uraian latar belakang di atas, rumusan masalah dalam penelitian ini meliputi bagaimana merancang dan membangun sistem pemesanan e-tiket berbasis web pada Wisata Mitra Sibayak yang terintegrasi untuk layanan pemandian air panas, bagaimana mengimplementasikan algoritma SHA-256 dalam pembuatan Digital Signature untuk menjamin keamanan dan keaslian e-tiket dari risiko duplikasi atau pemalsuan, serta bagaimana efektivitas sistem verifikasi Digital Signature dalam mempercepat dan memvalidasi proses check-in pengunjung di lokasi Wisata Mitra Sibayak. Agar penelitian lebih terfokus dan tidak meluas, batasan masalah dalam penelitian ini adalah lokasi penelitian berfokus pada Objek Wisata Pemandian Air Panas Mitra Sibayak, Berastagi, khususnya layanan pemesanan tiket masuk yang tersedia di lokasi tersebut; algoritma yang digunakan terbatas pada SHA-256 (Secure Hash Algorithm 256-bit) untuk menghasilkan Digital Signature unik sebagai kode verifikasi keamanan e-tiket; sistem dikembangkan berbasis web menggunakan bahasa pemrograman PHP dengan framework Laravel/CodeIgniter, CSS, serta MySQL sebagai sistem manajemen basis data (database); fitur verifikasi dilakukan melalui pemindaian (scanning) QR Code yang berisi hasil hash SHA-256 untuk memvalidasi keaslian tiket di pintu masuk wisata; serta sampel objek penelitian berjumlah 30 orang. Adapun tujuan yang ingin dicapai dalam penelitian ini adalah merancang dan membangun sistem pemesanan e-tiket berbasis web yang terintegrasi untuk layanan pemandian air panas dan penginapan di Mitra Sibayak guna mendigitalisasi proses transaksi, mengimplementasikan algoritma SHA-256 dalam pembentukan Digital Signature pada e-tiket untuk menjamin integritas data serta mencegah upaya pemalsuan atau penggandaan tiket, dan menghasilkan fitur verifikasi tiket yang cepat dan akurat bagi petugas di lokasi wisata melalui pemindaian QR Code guna meningkatkan efisiensi pelayanan serta keamanan data pengunjung.

B. METODE PENELITIAN

Penelitian ini menggunakan metode Research and Development (R&D) dengan model pengembangan perangkat lunak Waterfall untuk menghasilkan sistem pemesanan e-tiket wisata berbasis web yang dilengkapi mekanisme verifikasi Digital Signature menggunakan algoritma SHA-256. Model Waterfall dipilih karena memiliki tahapan yang sistematis dan berurutan, meliputi identifikasi masalah, pengumpulan data, analisis sistem, perancangan, implementasi, verifikasi tiket, pengujian, dan analisis hasil. Identifikasi masalah dilakukan terhadap keamanan data dan keaslian e-tiket yang berpotensi mengalami pemalsuan,

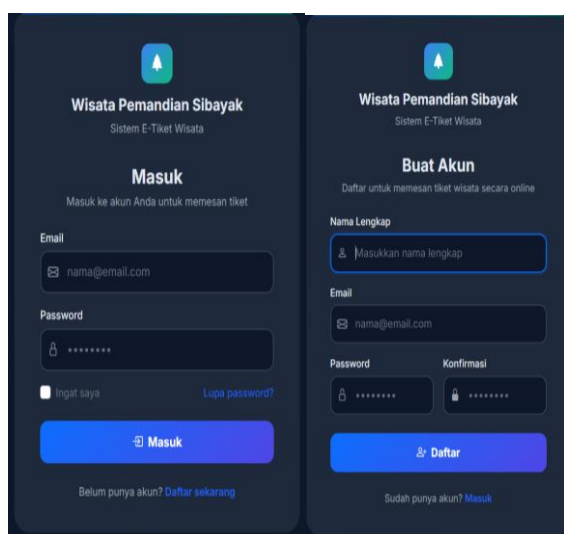
perubahan data, atau penggunaan tidak sah. Data penelitian dikumpulkan melalui observasi, wawancara, studi literatur, dan dokumentasi. Selanjutnya dilakukan analisis kebutuhan fungsional dan nonfungsional, perancangan flowchart, use case diagram, activity diagram, sequence diagram, ERD, basis data, serta antarmuka sistem.

Implementasi sistem dilakukan menggunakan PHP, HTML, CSS, dan MySQL, dengan algoritma SHA-256 untuk menghasilkan nilai hash sebagai dasar Digital Signature. Data tiket yang terdiri atas ID tiket, nama pengunjung, tanggal kunjungan, jenis tiket, dan total pembayaran digabungkan kemudian diproses menggunakan SHA-256 hingga menghasilkan hash sepanjang 256 bit atau 64 karakter heksadesimal. Selanjutnya, hash diproses menggunakan Private Key untuk membentuk Digital Signature dan data tersebut disimpan dalam basis data bersama QR Code. Pada proses verifikasi, petugas melakukan pemindaian QR Code, mengambil data tiket dari basis data, menghitung ulang nilai hash, kemudian memverifikasi Digital Signature menggunakan Public Key. Tiket dinyatakan valid apabila nilai hash sesuai dan tanda tangan digital berhasil diverifikasi. Pengujian sistem dilakukan menggunakan metode Black Box Testing terhadap fitur login, pemesanan tiket, pembentukan Digital Signature, pembuatan QR Code, dan proses verifikasi untuk memastikan sistem berjalan sesuai kebutuhan.

C. HASIL PENELITIAN DAN PEMBAHASAN

Implementasi Sistem

Tampilan Halaman *Login*



Gambar 1 Tampilan Login Customer, Admin dan Petugas Daftar Akun.

Gambar 1 menampilkan halaman Login Customer, Admin, dan Petugas pada Sistem E-Tiket Wisata Pemandian Sibayak yang berfungsi sebagai hak akses keamanan sistem. Pada halaman ini terdapat field input Email dan Password yang harus diisi sesuai dengan akun yang telah terdaftar. Selain itu, tersedia fitur Ingat Saya, Lupa Password, serta tombol Masuk untuk melakukan proses autentikasi pengguna. Setelah tombol Masuk ditekan, sistem akan memverifikasi data akun berdasarkan email, password, dan peran pengguna (*Customer*, Admin, atau Petugas) yang tersimpan di dalam database. Apabila data yang dimasukkan benar, pengguna akan diarahkan ke halaman dashboard sesuai dengan hak aksesnya, sedangkan jika data tidak valid maka sistem akan menampilkan pesan kesalahan. Pada bagian bawah halaman juga tersedia tautan Daftar Sekarang yang digunakan oleh customer untuk melakukan registrasi akun baru.

Tampilan Halaman *Dashboard*

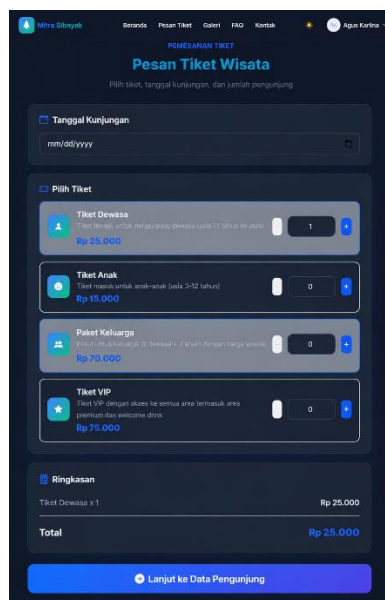


Gambar 2 Tampilan Dashboard *Customer*, Admin dan Petugas.

Gambar 2 di atas menampilkan halaman Dashboard *Customer*, Admin, dan Petugas pada Sistem E-Tiket Wisata Pemandian Sibayak yang akan ditampilkan setelah pengguna berhasil melakukan proses login. Halaman dashboard berfungsi sebagai halaman utama yang menyediakan informasi serta navigasi untuk mengakses seluruh fitur sistem sesuai dengan hak akses masing-masing pengguna. Pada halaman ini terdapat menu navigasi seperti Beranda, Pesan Tiket, Galeri, FAQ, dan Kontak, serta informasi bahwa sistem telah menggunakan algoritma SHA-256 untuk mendukung keamanan verifikasi *digital signature*. Selain itu, tersedia tombol Pesan Tiket Sekarang untuk memulai proses pemesanan tiket dan tombol Jelajahi untuk melihat informasi wisata. Dashboard juga menampilkan informasi singkat mengenai jumlah pengunjung, rating, tingkat keamanan sistem, dan layanan

pemesanan online yang dapat diakses selama 24 jam. Dengan adanya halaman dashboard ini, pengguna dapat mengakses seluruh fitur sistem dengan mudah, cepat, dan sesuai dengan peran yang dimiliki.

Tampilan Pemesanan Tiket



Gambar 3 Tampilan Pesanan Tiket

Gambar 3 menampilkan halaman Pesanan Tiket pada Sistem *E-Tiket* Wisata Pemandian Sibayak yang digunakan oleh customer untuk melakukan pemesanan tiket secara online. Pada halaman ini, pengguna terlebih dahulu memilih tanggal kunjungan, kemudian menentukan jenis tiket yang akan dibeli, seperti Tiket Dewasa, Tiket Anak, Paket Keluarga, atau Tiket VIP. Setiap jenis tiket menampilkan informasi harga, deskripsi singkat, serta tombol untuk menambah atau mengurangi jumlah tiket yang akan dipesan. Sistem secara otomatis menghitung total harga berdasarkan jumlah dan jenis tiket yang dipilih, kemudian menampilkan hasil perhitungan pada bagian ringkasan pesanan. Setelah seluruh data pemesanan sesuai, pengguna dapat menekan tombol Lanjut ke Data Pengunjung untuk melanjutkan ke tahap pengisian data pengunjung sebelum proses pembayaran dan penerbitan *e-tiket* dilakukan.

Tampilan Data Pengunjung

Gambar 4 Tampilan Data Pengunjung

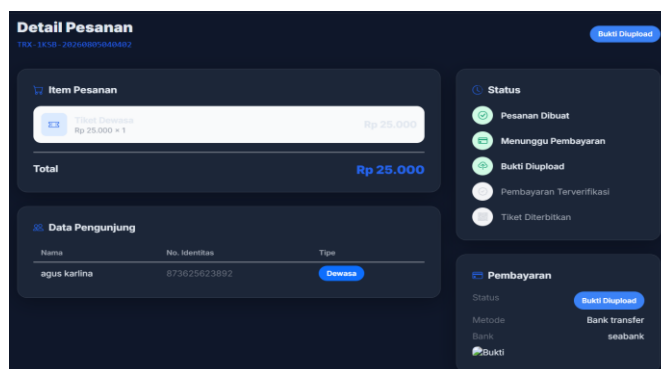
Gambar 4 menampilkan halaman Data Pengunjung pada Sistem *E-Tiket* Wisata Pemandian Sibayak yang digunakan untuk mengisi informasi setiap pengunjung sesuai dengan jumlah tiket yang telah dipilih pada tahap sebelumnya. Pada halaman ini ditampilkan informasi tanggal kunjungan, kemudian pengguna diwajibkan mengisi data berupa Nama Lengkap, Nomor KTP/Identitas, dan Nomor HP. Sistem juga menampilkan jenis tiket yang dipilih secara otomatis untuk memastikan kesesuaian data pengunjung dengan tiket yang dipesan. Setelah seluruh data diisi dengan lengkap dan benar, pengguna dapat menekan tombol Buat Pesanan untuk menyimpan data dan melanjutkan ke proses berikutnya, sedangkan tombol Kembali digunakan untuk kembali ke halaman pemesanan tiket apabila terdapat data yang ingin diubah.

Tampilan Data Pembayaran

Gambar 5 Tampilan Data Pembayaran

Gambar 5 menampilkan halaman Data Pembayaran pada Sistem *E-Tiket* Wisata Pemandian Sibayak yang digunakan oleh customer untuk menyelesaikan proses pembayaran setelah melakukan pemesanan tiket. Pada halaman ini ditampilkan detail pesanan, seperti nomor transaksi, jenis tiket yang dipesan, dan total pembayaran yang harus dibayarkan. Selain itu, sistem juga menyediakan informasi rekening tujuan yang meliputi nama bank, nama pemilik rekening, nomor rekening, serta jumlah transfer yang harus dibayarkan. Setelah melakukan transfer, pengguna diwajibkan mengisi data pembayaran berupa metode pembayaran, nama bank atau *e-wallet*, nama pengirim, nomor rekening pengirim, serta mengunggah foto bukti transfer. Selanjutnya, pengguna menekan tombol Upload Bukti Pembayaran untuk mengirimkan data pembayaran ke sistem agar dapat diverifikasi oleh petugas sebelum *e-tiket* diterbitkan.

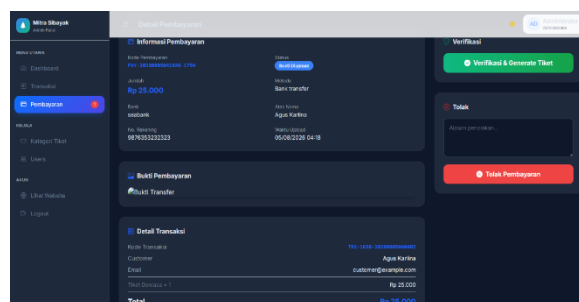
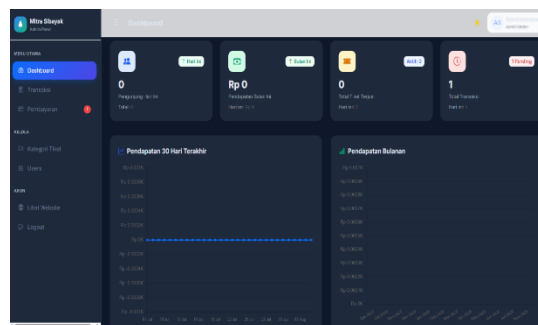
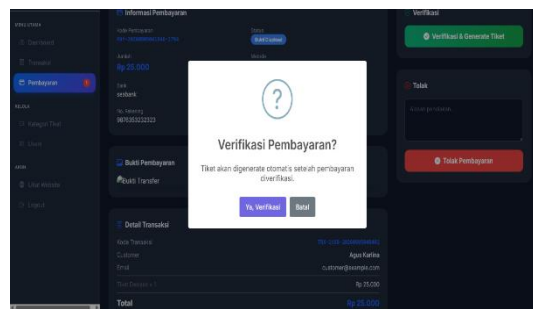
Tampilan Detail Pesanan



Gambar 6 Tampilan Detail Pesanan

Gambar 6 menampilkan halaman Detail Data Pembayaran pada Sistem *E-Tiket* Wisata Pemandian Sibayak yang digunakan untuk menampilkan informasi lengkap mengenai pesanan dan status pembayaran yang telah dilakukan oleh customer. Pada halaman ini ditampilkan informasi nomor transaksi, rincian item pesanan beserta total pembayaran, serta data pengunjung yang meliputi nama, nomor identitas, dan jenis tiket yang dipilih. Selain itu, sistem juga menampilkan status proses pemesanan mulai dari pesanan dibuat, menunggu pembayaran, bukti pembayaran diunggah, pembayaran terverifikasi, hingga tiket diterbitkan. Pada bagian informasi pembayaran ditampilkan metode pembayaran, nama bank atau *e-wallet* yang digunakan, status bukti pembayaran, serta bukti transfer yang telah diunggah oleh customer. Halaman ini memudahkan pengguna untuk memantau perkembangan proses verifikasi pembayaran hingga *e-tiket* diterbitkan oleh sistem.

Tampilan Profil Admin dan dan Verifikasi Pembayaran

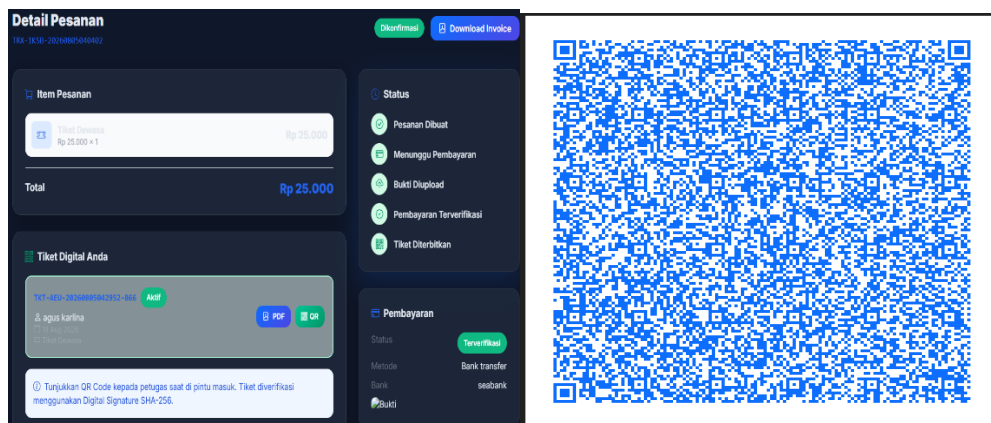


Gambar 7 Tampilan Profil Admin dan dan Verifikasi Pembayaran

Gambar 7 menampilkan halaman Profil Admin pada Sistem *E-Tiket* Wisata Pemandian Sibayak yang digunakan untuk mengelola dan memverifikasi pembayaran yang telah diunggah oleh *customer*. Pada halaman ini, admin dapat melihat informasi pembayaran yang meliputi kode pembayaran, jumlah pembayaran, nama bank, nomor rekening pengirim, metode pembayaran, serta bukti transfer yang telah diunggah. Selain itu, ditampilkan juga detail transaksi yang berisi kode transaksi, data customer, jenis tiket yang dipesan, dan total pembayaran. Setelah seluruh data dan bukti pembayaran dinyatakan sesuai, admin dapat menekan tombol Verifikasi & Generate Tiket sehingga sistem akan memverifikasi pembayaran sekaligus menerbitkan e-tiket yang telah dilengkapi dengan *digital signature* menggunakan algoritma SHA-256. Apabila pembayaran tidak valid, admin dapat mengisi alasan penolakan kemudian menekan tombol Tolak Pembayaran. Sebelum proses verifikasi dilakukan, sistem

akan menampilkan kotak dialog konfirmasi untuk memastikan keputusan admin sehingga proses verifikasi atau penolakan pembayaran dapat dilakukan dengan lebih aman dan akurat.

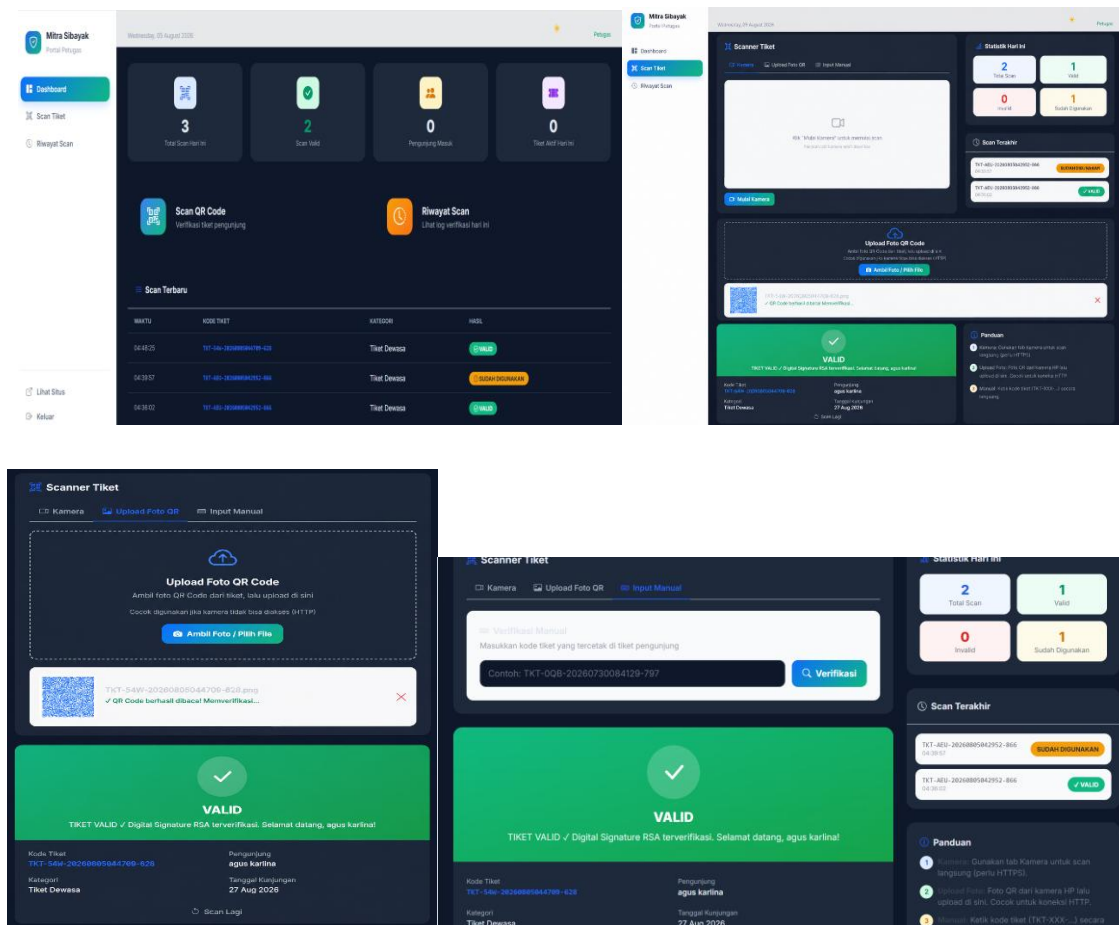
Tampilan Tiket Customer



Gambar 8 Tampilan Tiket *Customer*

Gambar 8 menampilkan halaman Tiket Customer pada Sistem *E-Tiket* Wisata Pemandian Sibayak yang digunakan untuk menampilkan *e-tiket* setelah pembayaran berhasil diverifikasi oleh admin. Pada halaman ini ditampilkan informasi detail pesanan, status transaksi yang menunjukkan bahwa pembayaran telah terverifikasi dan tiket telah diterbitkan, serta informasi pembayaran yang telah dikonfirmasi. Selain itu, sistem menampilkan tiket digital yang berisi kode tiket, nama pemilik tiket, tanggal kunjungan, jenis tiket, dan status tiket yang masih aktif. Pengguna juga dapat mengunduh invoice dalam format PDF atau menampilkan *QR Code* sebagai identitas tiket digital. *QR Code* yang dihasilkan telah dilengkapi dengan digital signature menggunakan algoritma SHA-256 sehingga keaslian dan integritas data tiket dapat diverifikasi oleh petugas pada saat proses pemindaian di pintu masuk. Dengan demikian, *e-tiket* yang diterbitkan memiliki tingkat keamanan yang lebih tinggi serta dapat mengurangi risiko pemalsuan tiket.

Tampilan Scanner Tiket



Gambar 9 Tampilan Tiket Customer pada saad di Scanner Tiket

Gambar 9 menampilkan halaman Portal Petugas (Mitra Sibayak) pada Sistem *E-Tiket* Wisata Pemandian Sibayak yang digunakan oleh petugas untuk memantau aktivitas pemindaian serta memverifikasi keaslian tiket pengunjung di pintu masuk secara *real-time*. Pada halaman ini ditampilkan ringkasan statistik harian meliputi total *scan*, tiket valid, pengunjung masuk, dan tiket aktifserta ta bel riwayat pemindaian terbaru yang memuat waktu, kode tiket, kategori, dan hasil status verifikasi (*VALID* atau *SUDAH DIGUNAKAN*). Untuk proses validasi tiket, sistem menyediakan tiga metode pemindaian pada menu *Scanner Tiket*, yaitu pemindaian langsung melalui kamera perangkat, metode unggah foto QR Code sebagai solusi alternatif jika kamera tidak dapat diakses (koneksi HTTP), serta metode *input manual* kode tiket sebagai opsi cadangan apabila *QR Code* fisik atau digital milik pengunjung mengalami kerusakan. Setiap pemindaian yang berhasil akan memverifikasi *Digital Signature* berbasis algoritma RSA pada QR Code dan menampilkan notifikasi status *VALID* lengkap dengan informasi detail seperti kode tiket, nama pengunjung, kategori tiket, dan tanggal

kunjungan, sehingga sistem ini memiliki tingkat keamanan yang tinggi dalam mencegah pemalsuan maupun penggunaan tiket ganda.

Hasil Pengujian Sistem (Evaluasi)

Verifikasi Fungsional (Black Box Testing)

Pengujian Iterasi Pertama (Temua Pengujian Kesalahan)

Hasil pengujian fungsional pada iterasi pertama menunjukkan bahwa seluruh fitur yang diuji masih mengalami kendala dan dinyatakan tidak lulus. Pada halaman login, ketika pengguna mengosongkan kolom email dan password, sistem seharusnya menolak proses login serta memberikan informasi bahwa kedua kolom tersebut wajib diisi. Namun, sistem tidak memberikan pesan kesalahan yang jelas sehingga pengguna tidak mengetahui penyebab kegagalan login. Pada halaman registrasi pengunjung, ketika pengguna menggunakan alamat email yang telah terdaftar, sistem seharusnya menolak proses registrasi dan memberikan informasi bahwa email tersebut sudah digunakan. Akan tetapi, sistem hanya menampilkan pesan gagal secara umum. Pada halaman pemesanan e-tiket, ketika pengguna tidak menentukan jumlah tiket, sistem seharusnya menolak proses penyimpanan dan meminta pengguna melengkapi data yang masih kosong. Hasil pengujian menunjukkan bahwa data pemesanan tetap diproses sehingga menyebabkan transaksi memiliki data yang tidak lengkap. Selanjutnya, pada proses generate SHA-256, sistem seharusnya menghasilkan nilai hash dari data e-tiket dan menyimpannya pada basis data sebagai digital signature. Namun, nilai hash belum tersimpan secara otomatis sehingga proses verifikasi tiket belum dapat dilakukan.

Pada fitur generate QR Code, sistem berhasil menghasilkan QR Code setelah pengguna melakukan pemesanan dan pembayaran e-tiket, tetapi QR Code tersebut belum memuat nilai hash SHA-256 sehingga proses verifikasi belum berjalan dengan baik. Pada halaman scan QR Code, petugas seharusnya dapat memperoleh data tiket sekaligus status keaslian tiket, tetapi sistem hanya menampilkan data tiket tanpa melakukan verifikasi digital signature. Pada proses verifikasi digital signature, ketika petugas memindai tiket yang telah dimodifikasi, sistem seharusnya dapat mendeteksi perubahan data dan menolak tiket tersebut. Namun, sistem masih menerima tiket yang telah dimodifikasi karena proses pencocokan hash belum berjalan dengan benar. Selain itu, pada validasi status tiket, ketika tiket yang sama dipindai sebanyak dua kali, sistem seharusnya menolak pemindaian kedua dan memberikan informasi

bahwa tiket telah digunakan. Hasil pengujian menunjukkan bahwa tiket masih dapat dipindai kembali sehingga berpotensi menimbulkan penyalahgunaan tiket. Berdasarkan keseluruhan hasil pengujian tersebut, seluruh fitur pada iterasi pertama dinyatakan tidak lulus dan memerlukan proses bug fixing sebelum dilakukan pengujian pada iterasi berikutnya.

Perbaiki Sistem (Bug Fixing)

Berdasarkan hasil pengujian Black Box Testing pada iterasi pertama, masih ditemukan beberapa fitur yang belum berjalan sesuai kebutuhan fungsional sehingga dilakukan proses bug fixing. Perbaikan meliputi penambahan validasi input pada halaman login dan registrasi untuk memastikan data yang dimasukkan lengkap dan sesuai format, penyempurnaan validasi pada halaman pemesanan e-tiket, serta pengoptimalan pembentukan hash menggunakan algoritma SHA-256 setelah transaksi berhasil disimpan. Selain itu, proses pembuatan QR Code diperbaiki dengan mengintegrasikan informasi e-tiket dan digital signature agar dapat digunakan sebagai media verifikasi keaslian tiket. Perbaikan tersebut dilakukan untuk meningkatkan ketepatan proses pengolahan data dan memastikan setiap e-tiket memiliki nilai hash yang dapat digunakan dalam proses verifikasi.

Perbaikan selanjutnya dilakukan pada proses verifikasi digital signature dengan mencocokkan nilai hash hasil perhitungan ulang dengan nilai hash yang tersimpan di basis data. Tiket dinyatakan valid apabila kedua nilai hash sesuai, sedangkan perbedaan nilai menyebabkan tiket ditolak karena dianggap tidak valid atau telah mengalami perubahan data. Sistem juga ditambahkan validasi status penggunaan tiket, sehingga setelah berhasil diverifikasi status tiket berubah menjadi "Sudah Digunakan" dan pemindaian ulang terhadap tiket yang sama akan ditolak. Setelah seluruh proses bug fixing selesai, dilakukan pengujian iterasi kedua menggunakan metode Black Box Testing untuk memastikan seluruh fitur telah berjalan sesuai kebutuhan, meliputi proses pemesanan e-tiket, pembentukan hash SHA-256, pembuatan QR Code, verifikasi digital signature, dan validasi status penggunaan tiket.

Hasil pengujian fungsional final menunjukkan bahwa seluruh fitur sistem telah berhasil memenuhi skenario pengujian dan dinyatakan lulus. Pada halaman login, ketika pengguna mengosongkan kolom email dan password kemudian menekan tombol Login, sistem berhasil menampilkan pesan validasi pada setiap kolom yang kosong sehingga pengguna dapat mengetahui data yang harus dilengkapi sebelum melakukan login. Pada halaman registrasi pengunjung, ketika pengguna mendaftarkan akun menggunakan alamat

email yang sudah terdaftar, sistem berhasil menampilkan notifikasi bahwa email tersebut telah digunakan sehingga pengguna diminta menggunakan alamat email yang berbeda. Pada halaman pemesanan e-tiket, ketika pengguna tidak mengisi salah satu data pemesanan, sistem berhasil melakukan validasi terhadap seluruh data dan menampilkan pesan bahwa seluruh data wajib diisi sebelum transaksi diproses. Selanjutnya, pada proses generate SHA-256, sistem berhasil membentuk nilai hash SHA-256 secara otomatis dan menyimpannya sebagai digital signature pada basis data tanpa terjadi kesalahan. Pada proses generate QR Code, setelah data transaksi berhasil disimpan, sistem berhasil menghasilkan QR Code sesuai dengan data transaksi sehingga siap digunakan dalam proses verifikasi tiket.

Pada fitur scan QR Code, petugas dapat melakukan pemindaian QR Code melalui halaman verifikasi, kemudian sistem berhasil membaca QR Code, menampilkan informasi tiket, dan melakukan proses verifikasi digital signature secara otomatis. Pada proses verifikasi digital signature, ketika petugas memindai tiket yang data transaksinya telah dimodifikasi, sistem berhasil mendeteksi perubahan data dan menampilkan informasi bahwa tiket tidak valid sehingga proses verifikasi dibatalkan. Selain itu, pada validasi status tiket, ketika petugas melakukan pemindaian terhadap tiket yang telah digunakan sebelumnya, sistem berhasil mendeteksi status tiket sebagai Sudah Digunakan sehingga QR Code tidak dapat digunakan kembali. Berdasarkan hasil pengujian tersebut, seluruh fitur yang diuji telah berjalan sesuai dengan hasil yang diharapkan dan dinyatakan LULUS, sehingga sistem telah mampu menjalankan fungsi validasi data, pembentukan SHA-256 digital signature, pembuatan QR Code, serta proses verifikasi dan validasi status e-tiket dengan baik.

Analisis Hasil Pengujian

Berdasarkan hasil pengujian pada iterasi kedua, seluruh skenario pengujian memperoleh status LULUS. Hal ini menunjukkan bahwa seluruh permasalahan yang ditemukan pada pengujian iterasi pertama telah berhasil diperbaiki melalui proses bug fixing. Validasi pada proses login, registrasi, dan pemesanan e-tiket telah berjalan sesuai dengan kebutuhan sehingga sistem dapat mencegah data yang tidak lengkap maupun tidak valid tersimpan ke dalam basis data.

Selain itu, implementasi algoritma SHA-256 berhasil menghasilkan nilai hash yang unik pada setiap transaksi e-tiket dan digunakan sebagai digital signature untuk menjaga integritas data. Proses pembuatan QR Code juga telah terintegrasi dengan data transaksi

sehingga dapat digunakan sebagai media verifikasi tiket. Pada tahap verifikasi, sistem mampu membandingkan nilai hash hasil perhitungan ulang dengan nilai hash yang tersimpan di basis data sehingga perubahan data e-tiket dapat dideteksi secara otomatis. Sistem juga berhasil melakukan validasi terhadap status penggunaan tiket sehingga e-tiket yang telah digunakan tidak dapat dipindai kembali.

Dengan demikian, hasil pengujian pada iterasi kedua menunjukkan bahwa sistem pemesanan e-tiket Wisata Mitra Sibayak berbasis web telah berfungsi sesuai dengan kebutuhan fungsional yang telah ditetapkan. Implementasi algoritma SHA-256 mampu meningkatkan keamanan data e-tiket melalui mekanisme digital signature, sehingga proses verifikasi tiket menjadi lebih aman, akurat, dan dapat meminimalkan risiko pemalsuan maupun penggunaan tiket secara berulang.

D. KESIMPULAN

Berdasarkan hasil penelitian mengenai Implementasi Algoritma SHA-256 untuk Verifikasi Digital Signature pada Sistem Pemesanan E-Tiket Wisata Mitra Sibayak Berbasis Web, maka dapat diambil kesimpulan bahwa sistem pemesanan e-tiket berbasis web berhasil dirancang dan dibangun untuk mendukung proses pemesanan tiket wisata Mitra Sibayak. Sistem telah mengintegrasikan proses registrasi, login, pemesanan tiket, pembayaran, penerbitan e-tiket, hingga penyimpanan data transaksi ke dalam basis data. Dengan adanya sistem ini, proses pemesanan tiket dapat dilakukan secara lebih terstruktur dan praktis. Algoritma SHA-256 berhasil diimplementasikan dalam pembentukan Digital Signature pada e-tiket. Data transaksi yang telah selesai diproses digunakan untuk menghasilkan nilai hash SHA-256 yang kemudian disimpan pada basis data sebagai acuan dalam proses verifikasi. Hasil implementasi menunjukkan bahwa perubahan atau manipulasi data pada e-tiket dapat terdeteksi ketika nilai hash dihitung kembali dan dibandingkan dengan nilai hash yang tersimpan. Dengan demikian, penerapan SHA-256 dapat membantu menjaga integritas dan keaslian data e-tiket serta mengurangi risiko pemalsuan dan penggandaan tiket.

Fitur verifikasi tiket melalui pemindaian QR Code berhasil diterapkan dan berjalan sesuai kebutuhan. QR Code digunakan sebagai identitas unik e-tiket yang dapat dipindai oleh petugas di lokasi wisata. Sistem kemudian melakukan perhitungan ulang nilai hash SHA-256 dan membandingkannya dengan nilai hash yang tersimpan pada database untuk menentukan status tiket. Berdasarkan hasil pengujian Black Box Testing setelah dilakukan perbaikan (bug fixing), seluruh fitur utama seperti login, registrasi, pemesanan, pembentukan hash,

pembuatan QR Code, verifikasi Digital Signature, dan validasi status tiket telah berjalan dengan baik. Sistem juga mampu menolak tiket yang telah dimodifikasi maupun tiket yang sudah pernah digunakan.

E. REFERENSI

Andi Leo. Veeri Kuswanto, Lily Damayanti. (Agustus, 2022) , Mobile Commerce untuk Sales Order dan Tracking Order berbasis MVC. <https://share.google/zQIBdoDpxr8RskPBU>

Andi Asari, Bernadete Deta, Syahrial, Hidayatus Sibyan dan Tri Pratiwi Handayani (Agustus, 2024) buku: Sistem Basis Data. PT MAFY MEDIA LITERASI INDONESIA ANGGOTA IKAPI.

Ahmad Zaky Nadimsyah & Muhammad Ezar Al Rivan (2024, 1 Oktober) Implementasi Secure Hash Algorithm-256 dan Advanced Encryption Standard Untuk Verifikasi Tanda Tangan Digital. *Journal of Information System Research (JOSH)*, pp 229-239.

Az-Zahra, F., Marwati, R., & Sispiyati, R. (2024). Implementasi QR Code dengan Algoritma Secure Hash Algorithm (SHA)-256 dan Rivest Shamir Adleman (RSA) yang Ditingkatkan untuk Autentikasi Dokumen Digital. *Jurnal EurekaMatika*, 12(1), 11–22.

Ahmad Halimi & Abu Tholib, Moh. Ainol Yaqin (2024, 1 Juli 2024) Optimasi Keamanan Data Penerimaan Mahasiswa Menggunakan AES-256, SHA-256, dan Base64. *JUSTIFY: Jurnal Sistem Informasi Ibrahimy*.

Adhitya Saputra, (2022). Pemanfaatan Teknologi E-Ticketing sebagai Media Monitoring dan Manajemen Data Pengunjung Destinasi Wisata. <https://conference.upnvj.ac.id/index.php/senamika>

Ayunindya, F. C. (2024, May 15). Apa Itu Website? Ini Pengertian Website dan Jenis-Jenisnya. *Hostinger*. <https://www.hostinger.co.id/tutorial/website-adalah>

B. Harahap, R. A. Sitorus, & I. P. Sari (2022), Implementasi Kriptografi Klasik dan Modern dalam Pengamanan Informasi Digital.

C. Kurniawan, A. P. Sari, and A. Syahjaratu, "Sejarah Web Service dan Penggunaannya," 2017. [Online]. Available: <http://sejarahwebservice.blogspot.com/2017/03/sejarah-web-service.html>.

- Daryono, Sutikno, & Widhoyoko (2024), Pengembangan Aplikasi Warditem Untuk Mendukung Digitalisasi Pemasaran Produk IKM Di Desa Sijeruk.
- Fadila, Riri Ratna, Wedra Aprison, and Hari Antoni Musril (2021). "Perancangan Perizinan Santri Menggunakan Bahasa Pemograman PHP/MySQL Di SMP Nurul Ikhlas." CSRID (Computer Science Research and Its Development Journal) 11(2): 84.
- Ghofur, A., Rahman, A., & Lutfi, A. (2023). Sistem Informasi Perpustakaan Berbasis Web. Conference on Innovation and Application of Science and Technology (CIASTECH), 6(1), 665.
- Gagah Rizky Mulyawan & Asmunin (2025) Penerapan Tanda Tangan Digital Menggunakan Algoritma RSA dan SHA-256 dengan QR Code pada Sertifikat Elektronik, Manajemen Informatika, Fakultas Vokasi, Universitas Negeri Surabaya.
- Hidayat, dkk. (2022). "Membuat Blog Pribadi Menjadi Website Berita Online Menggunakan HTML dan CSS." Jurnal Ilmiah Sistem Informasi dan Ilmu Komputer (JUISIK), Vol. 2, No. 2, hlm. 30–40. Penerbit: Sinov Institute
- Hadi, A., & Nurfauzi, A. (2023). Implementasi Algoritma SHA-256 untuk Keamanan Pertukaran Data pada Sistem Informasi. <https://jurnal.syntax-id.co.id/index.php/syntax-akurat/index>
- Irawan, A. I., Santoso, I. H., Istikmal, & Rahayu, M. (2024). Implementation of QR Code Attendance Security System Using RSA and Hash Algorithms. Jurnal Nasional Teknik Elektro dan Teknologi Informasi (JNTETI), 13(1), 53–59.
- Jamil & Asri (2024), Analisis Keamanan Data dan Implementasi Kriptografi pada E-Commerce.
- Laily, I. N. (2022, February 7). Pengertian Website Menurut Para Ahli, Beserta Jenis dan Fungsinya. Katadata. <https://katadata.co.id/lifestyle/edukasi/6200a2a9697ec/pengertian-website-menurut-para-ahli-beserta-jenis-dan-fungsinya>
- M. Ariansyah, E. Yuliana (2021), Rancang Bangun Aplikasi Pelayanan Sistem Rujukan Pada Puskesmas Sukajadi Berbasis Web.

- M. Jamil & A. Asri (2024), Analisis Keamanan Data dan Implementasi Kriptografi pada E-Commerce.
- Manuhutu, M. A., & Otniel. (2021).Sistem Informasi Promosi TempatWisata Di Kota Sorong BerbasisWebsite (Kasus : Kawasan Wisata Mangrove Klawalu). Jurnal Sains Komputer & Informatika (J-SAKTI), 5(1), 304–317.
- National Institute of Standards and Technology. (2015). Secure Hash Standard (SHS) (Federal Information Processing Standards Publication 180-4). U.S. Department of Commerce, hal. 10–24.
- Novita Rahma & Sri Hartati, Defi Pujianto (2024). Aplikasi E-Book Berbasis Andaroid Untuk Mendukung Pembelajaran Interaktif di SMK Sentosa BH.
- Nadimsyah, A. Z., & Al Rivan, M. E. (2024). Implementasi Secure Hash Algorithm-256 dan Advanced Encryption Standard untuk Verifikasi Tanda Tangan Digital. Journal of Information System Research (JOSH), 6(1), 229–239.
- O. W. Purbo, A Systematic Analysis: Website Development using Codeigniter and Laravel Framework, Enrichment: Journal of Management, pp. 1008-1014, 2021.
- Putra, Y. W. S., Dawis, A. M., Novi, N., Natsir, F., Fitria, F., Widhiyanti, A. A. S., ... & Maniah, M. (2023). Pengantar Aplikasi Mobile. Penerbit Widina.
- Prasetyo, dkk. (2022). "Perancangan Website Company Profile Menggunakan HTML, CSS, dan Framework Bootstrap." Procedia of Engineering and Life Science (PELS), Vol. 2, No. 2, hlm. 1–10. Universitas Muhammadiyah Sidoarjo.
- Pratama, A. R., dkk. (2024). Penerapan Algoritma SHA-256 untuk Menjamin Integritas Data pada Sistem Informasi Berbasis Web. <https://journal.trunojoyo.ac.id/jtik>
- Putri NingTias, M. A., Abas, M., Pratiwi, R. O., & Ilham, F. (2025). Perancangan dan implementasi sistem jurnal kehadiran dan aktivitas guru berbasis web pada Madrasah Aliyah Negeri 16 Jakarta. JRIIN: Jurnal Riset Informatika dan Inovasi, 3(5), 1203–1210.
- Parjito, dkk (2022), Analisis Perangkat Lunak Berbasis Komputasi Terapan
- Rendy Kurniawan, (2023). Implementasi QR Code untuk Keamanan Autentikasi Tiket Elektronik pada Sistem Reservasi Online. <https://jsit.com/index.php/jsit>

- Ramadhan & N. K. Putri (2023), Penerapan Secure Hash Algorithm (SHA-256) untuk Verifikasi Keaslian Berkas Digital.
- R. Pratama & H. Wijaya (2025). Buku Ajar Kriptografi Modern dan Keamanan Informasi.
- Riva Abdillah Aziz, Arfan Sansprayada, Kartika Mariskhana (2024), Perancangan Sistem Adminisatrasi Penjualan pada PT SurMoRin dengan Menggunakan PHP dan MYSQL, Jurnal Minfo Polgan.
- Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Boston: Pearson Education, hal. 391–398.
- Selviana Anggreani,(2024, 1 Februari). Pengantar dan Pengenalan Konsep Dasar Algoritma Pemrograman. (Jurnal Pendidikan Berkarakter). P, 282-294.
- Syifaudin, E. (2022, October 26). Jenis Website di Internet Berdasarkan Fungsi, Platform dan Sifat. <https://www.exabytes.co.id/log/jenis-website-di-internet/>
- Syabania, R., & Rosmawani, N. (2021). Perancangan Aplikasi Customer Relationship Management (Crm) Pada Penjualan Barang Pre-Order Berbasis Website. *Rekayasa Informasi*, 10(1), 44–49.
- Sari, dkk. (2024). "Pengembangan Website Interaktif Menggunakan HTML, CSS, dan JavaScript sebagai Media Informasi." *Journal of Information Business System (JIBS)*, Vol. 2, No. 3, hlm. 468–479.
- Thalia, K. M., Oktaviyani, E. D., & Sylviana, F. (2021). Sistem Informasi Inventory Berbasis Website (Studi Kasus : Pada Toko Obyth). In *JOINTECOMS (Journal of Information Technology and Computer Science)*.
- Wahyu Hidayat dan Zulkifli, (2023). Analisis dan Perancangan Sistem Informasi E-Ticketing Berbasis Web pada Objek Wisata.<https://ejournal.stmik-wp.ac.id/index.php/jutisi>
- W. T. Pradana & H. Assegaff (2023), Implementasi Tanda Tangan Digital Menggunakan Algoritma Kriptografi Asimetris Untuk Keamanan Dokumen Elektronik. *Jurnal Ilmiah Media Sisfo*. pp. 78-89, 2023.

Yayan Albi Agustian & Agus Tedyyana, (2026, 1 Februari). implementasi algoritma sha-256 pada aplikasi pencatatan transaksi dan kehadiran berbasis web di kedai kopi kambojda. JATI (Jurnal Mahasiswa Teknik Informati