Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

Integrasi *QR Code* Terenkripsi Berbasis *AES-128* untuk Pencegahan Pemalsuan Sertifikat *English Test Program* (ETP): Studi Kasus UPA Bahasa Universitas Maritim Raja Ali Haji

Irwan Saputra[1*], Muhamad Radzi Rathomi[2], Berta Erwin Slam[3]
[1,2,3]Teknik Informatika, Universitas Maritim Raja Ali Haji, Indonesia
Email: [1*]irwansaputra192003@gmail.com, [2]radzi@umrah.ac.id, [3]bertaerwinslam@umrah.ac.id

Abstrak

Pemanfaatan Sertifikat *English Test Program* (ETP) dalam bentuk digital di Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji (UMRAH) masih menghadapi permasalahan keamanan karena penggunaan *QR Code* yang dibuat secara manual sehingga rentan terhadap duplikasi dan pemalsuan. Penelitian ini bertujuan mengembangkan mekanisme verifikasi keaslian Sertifikat ETP melalui integrasi algoritma *Advanced Encryption Standard* (AES-128) dengan *QR Code* terenkripsi. Kebaruan penelitian ini terletak pada penyematan *ciphertext* hasil enkripsi AES-128 ke dalam *QR Code* sebagai mekanisme autentikasi yang mendukung verifikasi keaslian sertifikat digital secara cepat, akurat, dan andal. Penelitian menggunakan pendekatan pengembangan sistem dengan membangun aplikasi berbasis web menggunakan React, Node.js, MongoDB, dan pustaka CryptoJS. Data sertifikat yang meliputi NIM, nama mahasiswa, dan skor ETP dienkripsi menggunakan AES-128, kemudian hasil enkripsi dalam format Base64 disematkan ke dalam *QR Code* pada sertifikat digital. Pengujian sistem dilakukan menggunakan metode *Black Box Testing*, pengujian *avalanche effect*, serta simulasi berbagai skenario pemalsuan sertifikat. Hasil penelitian menunjukkan bahwa seluruh fungsi sistem berjalan sesuai kebutuhan dengan tingkat keberhasilan *Black Box Testing* sebesar 100%, sedangkan pengujian *avalanche effect* menghasilkan nilai rata-rata 49,87% yang menunjukkan karakteristik keamanan AES-128 telah terpenuhi. Selain itu, sistem mampu mendeteksi seluruh skenario pemalsuan, meliputi modifikasi dokumen, penggantian maupun pembuatan *QR Code* tiruan, serta pemalsuan total sertifikat melalui proses verifikasi keaslian. Dengan demikian, mekanisme verifikasi berbasis integrasi AES-128 dan *QR Code* terenkripsi terbukti mampu meningkatkan keamanan dan integritas data serta mendukung autentikasi Sertifikat ETP secara efektif di lingkungan UPA Bahasa UMRAH.
Kata Kunci: *AES-128*; Kriptografi; QR Code; Sertifikat ETP; Pemalsuan Dokumen;

Abstract

The use of digital English Test Program (ETP) certificates at the Academic Support Unit (UPA) for Language of Universitas Maritim Raja Ali Haji (UMRAH) continues to face security challenges due to the manual generation of QR Codes, making the certificates vulnerable to duplication and forgery. This study aims to develop a certificate authenticity verification mechanism by integrating the Advanced Encryption Standard (AES-128) algorithm with encrypted QR Codes. The novelty of this study lies in embedding the AES-128 encrypted ciphertext into the QR Code as an authentication mechanism, enabling fast, accurate, and reliable verification of digital certificate authenticity. A web-based application was developed using React, Node.js, MongoDB, and the CryptoJS library. Certificate data, including student identification number, student name, and ETP score, were encrypted using AES-128, and the resulting Base64-encoded ciphertext was embedded into the QR Code of the digital certificate. The system was evaluated using Black Box Testing, avalanche effect analysis, and simulations of various certificate forgery scenarios. The results indicate that all system functionalities operated as intended, achieving a 100% success rate in Black Box Testing. Furthermore, the average avalanche effect reached 49.87%, demonstrating that the AES-128 implementation satisfied the expected cryptographic security characteristics. The proposed system successfully detected all simulated forgery attempts, including document modification, QR Code replacement, counterfeit QR Code generation, and complete certificate forgery through the authenticity verification process. Therefore, the proposed verification mechanism based on the integration of AES-128 and encrypted QR Codes effectively enhances data security and integrity while providing a reliable solution for authenticating ETP certificates within the UPA for Language at Universitas Maritim Raja Ali Haji.
Keywords: AES-128; Cryptography; QR Code; ETP Certificate; Document Forgery;

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

***Corresponding Author:**
Irwan Saputra, Teknik Informatika, Universitas Maritim Raja Ali Haji, Indonesia
Email: irwansaputra192003@gmail.com

1. PENDAHULUAN

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]. Namun demikian, berbagai kasus pemalsuan dokumen akademik di Indonesia menunjukkan bahwa keamanan dokumen digital masih menghadapi tantangan yang serius. Salah satu di antaranya adalah kasus dugaan penggunaan ijazah palsu yang ditangani oleh Polda Lampung pada tahun 2024, yang memperlihatkan bahwa lemahnya mekanisme verifikasi masih membuka peluang terjadinya penyalahgunaan dokumen akademik. Temuan tersebut menunjukkan bahwa sistem keamanan dokumen digital tidak hanya dituntut mampu melindungi data dari manipulasi, tetapi juga harus menyediakan mekanisme verifikasi yang dapat memastikan keaslian dokumen secara cepat, akurat, dan andal. Permasalahan ini tidak hanya terjadi pada ijazah dan transkrip akademik, tetapi juga mulai mengancam berbagai sertifikat pendukung akademik, khususnya sertifikat kemampuan bahasa Inggris yang saat ini banyak diterbitkan dalam bentuk digital dan digunakan sebagai persyaratan akademik maupun profesional.

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 [4]. Kondisi tersebut mengindikasikan bahwa mekanisme verifikasi yang masih bersifat konvensional belum mampu memberikan perlindungan yang memadai terhadap manipulasi data maupun pemalsuan dokumen. Permasalahan serupa juga menjadi perhatian di Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji (UMRAH), di mana proses penerbitan dan validasi Sertifikat *English Test Program* (ETP) masih menggunakan *QR Code* yang dibuat secara manual. Mekanisme tersebut berpotensi membuka peluang terjadinya duplikasi maupun modifikasi *QR Code*, sehingga diperlukan mekanisme keamanan yang mampu menjamin integritas data sekaligus mendukung proses verifikasi keaslian sertifikat secara cepat, akurat, dan andal. Salah satu bentuk kerentanan tersebut juga masih dijumpai pada mekanisme penerbitan dan validasi Sertifikat ETP di UPA Bahasa Universitas Maritim Raja Ali Haji yang memerlukan perhatian khusus.

Dalam konteks Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji, meskipun Sertifikat *English Test Program* (ETP) telah diterbitkan dalam bentuk digital, permasalahan utama masih terletak pada mekanisme validasinya. Sistem yang digunakan saat ini memanfaatkan *QR Code* konvensional yang dibuat secara manual untuk menyimpan informasi validasi sertifikat. Secara teknis, *QR Code* konvensional hanya berfungsi sebagai media penyimpanan dan penyajian data tanpa dilengkapi mekanisme keamanan, seperti enkripsi, autentikasi, maupun perlindungan terhadap integritas data. Akibatnya, informasi yang tersimpan di dalam *QR Code* dapat dibaca menggunakan berbagai aplikasi pemindai (*scanner*) maupun pembuat (*generator*) *QR Code* yang tersedia secara bebas, kemudian diduplikasi atau dimodifikasi untuk menghasilkan *QR Code* baru dengan informasi yang telah diubah. Kondisi tersebut membuka peluang terjadinya pemalsuan sertifikat melalui penggantian data validasi tanpa dapat dibedakan secara visual dari *QR Code* asli. Risiko ini secara langsung mengancam keabsahan proses verifikasi sertifikat, sehingga diperlukan mekanisme keamanan yang mampu menjamin kerahasiaan, integritas, dan keaslian data validasi. Salah satu pendekatan yang

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342 Page 542-557

dinilai efektif untuk mengatasi kelemahan tersebut adalah penerapan algoritma kriptografi dengan mengenkripsi data validasi sebelum disematkan ke dalam *QR Code*.

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. 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*. Mekanisme tersebut tidak hanya bertujuan menyembunyikan informasi penting, tetapi juga memungkinkan proses verifikasi keaslian sertifikat dilakukan secara aman melalui proses dekripsi.

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 [5]. 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 [6]. Efektivitas pendekatan tersebut juga telah diperkuat oleh berbagai penelitian terdahulu yang mengombinasikan algoritma kriptografi dengan teknologi *QR Code* untuk meningkatkan keamanan dokumen digital.

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 [7]. 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 [8]. Meskipun demikian, penelitian-penelitian tersebut masih menyisakan ruang pengembangan, khususnya dalam menyediakan mekanisme *anti-forgery* yang secara spesifik ditujukan untuk mengatasi pemalsuan *QR Code* pada Sertifikat ETP di lingkungan akademik.

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*, penelitian ini secara langsung menciptakan lapisan keamanan (*anti-forgery*) untuk menghilangkan risiko duplikasi *QR Code* manual yang sebelumnya mudah dibuat secara bebas. Model implementasi ini menyematkan *ciphertext* hasil enkripsi *AES-128* ke dalam *QR Code* sebagai parameter keaslian utama. Berdasarkan permasalahan, celah penelitian, dan kebutuhan akan sistem validasi yang lebih aman tersebut, penelitian ini bertujuan untuk merancang dan mengimplementasikan purwarupa aplikasi berbasis web yang menerapkan algoritma AES-128 pada data validasi Sertifikat ETP yang terintegrasi dengan QR Code, serta mengembangkan modul verifikasi yang mampu mendekripsi dan memvalidasi data sebagai upaya pencegahan pemalsuan Sertifikat ETP di Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji.

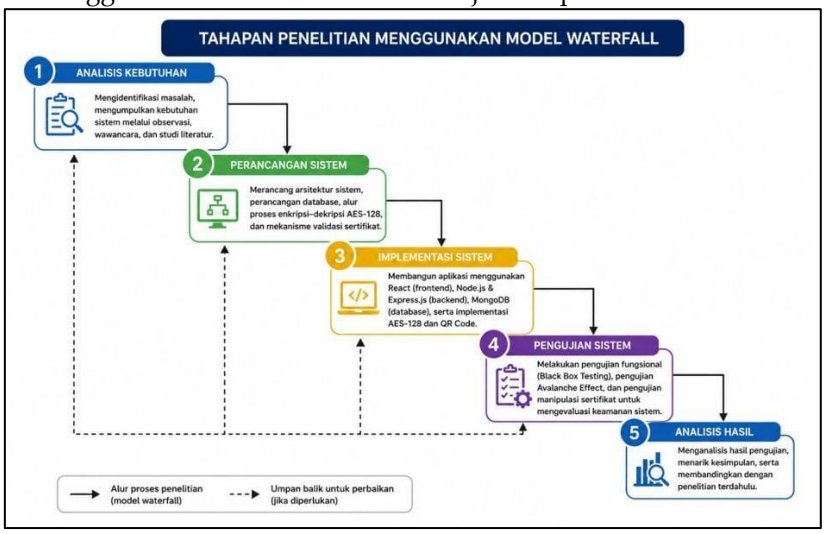
2. METODE PENELITIAN

Penelitian ini menggunakan metode *Research and Development* (R&D) yang bertujuan untuk menghasilkan sebuah produk berupa aplikasi berbasis web sebagai solusi pencegahan pemalsuan Sertifikat *English Test Program* (ETP) di Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji. Metode R&D dipilih karena tidak hanya berorientasi pada pengembangan produk, tetapi juga mencakup proses pengujian untuk memastikan bahwa produk yang dihasilkan mampu memenuhi kebutuhan pengguna serta berfungsi sesuai dengan tujuan yang telah ditetapkan [9]. Produk yang dikembangkan dalam penelitian ini berupa sistem verifikasi sertifikat digital yang mengintegrasikan

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

algoritma *Advanced Encryption Standard (AES-128)* dengan teknologi *Quick Response* (QR) *Code* sebagai mekanisme autentikasi dan pencegahan pemalsuan dokumen.

Dalam proses pengembangannya, penelitian ini menerapkan model *Waterfall* sebagai metode pengembangan perangkat lunak. Model *Waterfall* dipilih karena memiliki tahapan yang sistematis, terstruktur, dan berurutan, sehingga setiap tahap harus diselesaikan sebelum melanjutkan ke tahap berikutnya. Pendekatan ini dinilai sesuai dengan karakteristik penelitian karena kebutuhan sistem telah didefinisikan secara jelas sejak awal, mulai dari identifikasi permasalahan, perancangan mekanisme enkripsi menggunakan algoritma AES-128, hingga implementasi dan pengujian sistem. Selain itu, model *Waterfall* memudahkan proses dokumentasi pada setiap tahapan pengembangan sehingga hasil penelitian dapat dievaluasi secara sistematis [10]. Adapun tahapan penelitian yang dilakukan meliputi analisis kebutuhan, perancangan sistem, implementasi, pengujian sistem, dan analisis hasil. Alur tahapan penelitian menggunakan model Waterfall ditunjukkan pada Gambar 1.



Gambar 1. Tahapan Penelitian Menggunakan Model *Waterfall*

2.1. Analisis Kebutuhan

Tahap pertama dalam model *Waterfall* adalah analisis kebutuhan (*requirement analysis*). Pada tahap ini dilakukan identifikasi terhadap permasalahan yang terdapat pada proses penerbitan dan verifikasi Sertifikat *English Test Program* (ETP) di Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji. Analisis kebutuhan bertujuan untuk memperoleh informasi mengenai kelemahan sistem yang sedang berjalan serta menentukan kebutuhan fungsional dan nonfungsional yang harus dipenuhi oleh sistem yang akan dikembangkan [11].

Proses pengumpulan data dilakukan melalui observasi, wawancara, dan studi literatur. Observasi dilakukan secara langsung terhadap alur penerbitan, penyimpanan, serta mekanisme validasi Sertifikat ETP menggunakan lembar observasi (*observation checklist*) yang disusun berdasarkan aspek proses bisnis, keamanan data, dan mekanisme verifikasi sertifikat. Selain itu, wawancara semi-terstruktur dilakukan terhadap dua narasumber, yaitu Kepala UPA Bahasa dan satu orang administrator yang bertanggung jawab dalam proses penerbitan serta pengelolaan Sertifikat ETP. Wawancara bertujuan menggali informasi mengenai prosedur penerbitan sertifikat, mekanisme validasi yang diterapkan, kendala yang dihadapi, serta kebutuhan sistem keamanan yang diharapkan. Studi literatur dilakukan untuk mengkaji penerapan algoritma kriptografi AES-128 dan teknologi *QR Code* dalam pengamanan dokumen digital.

Berdasarkan hasil observasi dan wawancara, diketahui bahwa mekanisme validasi sertifikat masih menggunakan *QR Code* konvensional yang dibuat secara manual. Informasi yang tersimpan pada *QR Code* belum dilengkapi mekanisme enkripsi maupun autentikasi sehingga berpotensi untuk diduplikasi atau digenerasikan ulang menggunakan aplikasi *QR Code generator* yang tersedia secara bebas. Kondisi tersebut meningkatkan risiko manipulasi data dan pemalsuan sertifikat.

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

Hasil analisis kebutuhan menunjukkan bahwa sistem yang dikembangkan harus mampu memenuhi beberapa kebutuhan utama, yaitu: (1) menghasilkan Sertifikat ETP digital yang dilengkapi *QR Code* terenkripsi menggunakan algoritma AES-128; (2) mengenkripsi data penting yang meliputi Nomor Induk Mahasiswa (NIM), nama mahasiswa, nilai *Listening*, *Structure*, *Reading*, dan *Total Score* sebelum disematkan ke dalam *QR Code*; (3) menyediakan mekanisme verifikasi sertifikat melalui unggah dokumen PDF maupun pemindaian *QR Code* secara langsung; (4) melakukan proses dekripsi dan pencocokan data dengan basis data untuk memastikan keaslian sertifikat; serta (5) mampu mendeteksi berbagai bentuk manipulasi dokumen maupun *QR Code* sebagai upaya pencegahan pemalsuan sertifikat.

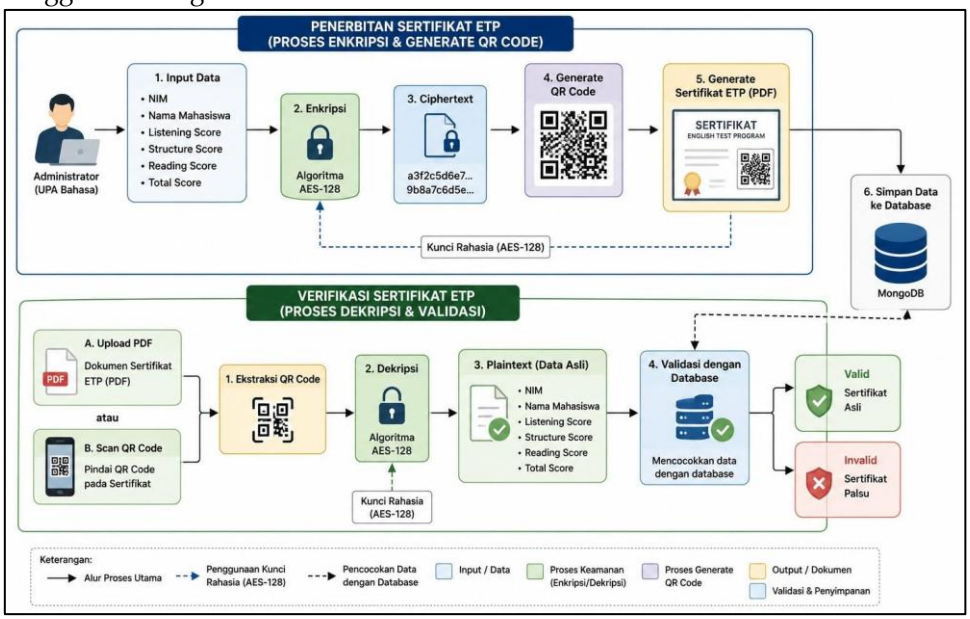
Berdasarkan hasil analisis tersebut, dapat disimpulkan bahwa penerapan algoritma *Advanced Encryption Standard (AES-128)* yang diintegrasikan dengan teknologi *QR Code* merupakan pendekatan yang sesuai untuk meningkatkan keamanan, menjaga integritas data, serta mendukung proses verifikasi Sertifikat ETP secara lebih cepat, akurat, dan terpercaya. Hasil analisis kebutuhan ini selanjutnya menjadi dasar dalam proses perancangan sistem pada tahap berikutnya.

2.2. Perancangan Sistem

Tahap kedua dalam model *Waterfall* adalah perancangan sistem (*system design*). Tahap ini bertujuan menerjemahkan kebutuhan sistem yang telah diidentifikasi pada tahap analisis menjadi rancangan teknis yang akan menjadi acuan dalam proses implementasi. Perancangan dilakukan agar seluruh kebutuhan fungsional dan nonfungsional dapat diakomodasi secara terstruktur sehingga sistem mampu mendukung proses penerbitan dan verifikasi Sertifikat *English Test Program* (ETP) secara aman, efisien, dan mudah dipelihara.

Perancangan sistem pada penelitian ini meliputi penyusunan arsitektur aplikasi, mekanisme pengamanan data menggunakan algoritma *Advanced Encryption Standard* (AES-128), perancangan basis data, serta mekanisme verifikasi keaslian sertifikat berbasis *QR Code* terenkripsi. Arsitektur aplikasi dikembangkan menggunakan React sebagai *frontend*, Node.js dan Express.js sebagai *backend*, serta MongoDB sebagai sistem manajemen basis data. Seluruh komponen tersebut saling terintegrasi untuk mendukung proses pengelolaan data mahasiswa, penerbitan sertifikat, pembangkitan *QR Code*, dan proses verifikasi keaslian Sertifikat ETP.

Untuk memberikan gambaran mengenai mekanisme kerja sistem yang diusulkan, Gambar 2 menyajikan arsitektur sistem beserta alur proses penerbitan Sertifikat ETP dan proses verifikasi keaslian sertifikat menggunakan algoritma AES-128.



Gambar 2. Perancangan Sistem Pencegahan Pemalsuan Sertifikat ETP Menggunakan Algoritma *AES-128*

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

Berdasarkan Gambar 2, mekanisme sistem yang diusulkan terdiri atas dua proses utama, yaitu proses penerbitan Sertifikat *English Test Program* (ETP) dan proses verifikasi keaslian sertifikat. Pada proses penerbitan, administrator UPA Bahasa terlebih dahulu memasukkan data mahasiswa yang meliputi Nomor Induk Mahasiswa (NIM), nama mahasiswa, nilai *Listening*, *Structure*, *Reading*, dan *Total Score*. Selanjutnya, sistem melakukan validasi terhadap kelengkapan data sebelum menjalankan proses enkripsi menggunakan algoritma *Advanced Encryption Standard* (AES-128). Hasil enkripsi berupa *ciphertext* kemudian dikodekan ke dalam *QR Code* yang disisipkan pada Sertifikat ETP digital. Setelah proses pembangkitan *QR Code* selesai, sistem menghasilkan sertifikat dalam format PDF dan menyimpan data sertifikat ke dalam basis data MongoDB sebagai acuan pada proses verifikasi.

Pada tahap verifikasi, pengguna dapat melakukan pemindaian *QR Code* secara langsung atau mengunggah Sertifikat ETP dalam format PDF melalui sistem. Sistem selanjutnya mengekstraksi *ciphertext* yang terdapat pada *QR Code*, kemudian melakukan proses dekripsi menggunakan algoritma AES-128. Hasil dekripsi dibandingkan dengan data sertifikat yang tersimpan pada basis data MongoDB untuk memastikan kesesuaian informasi. Apabila seluruh data yang diperoleh identik dengan data pada basis data, sistem akan memberikan status Valid sebagai indikasi bahwa sertifikat merupakan dokumen asli. Sebaliknya, apabila ditemukan ketidaksesuaian data atau proses dekripsi tidak dapat dilakukan, sistem akan memberikan status Invalid, yang menunjukkan adanya indikasi manipulasi data maupun pemalsuan sertifikat.

Pada penelitian ini, proses enkripsi menggunakan algoritma AES-128 dengan mode *Cipher Block Chaining* (CBC) dan skema *padding* PKCS#7 yang diimplementasikan melalui pustaka CryptoJS. Pemilihan mode CBC bertujuan untuk meningkatkan keamanan proses enkripsi karena setiap blok *plaintext* diproses berdasarkan blok *ciphertext* sebelumnya, sehingga menghasilkan *ciphertext* yang berbeda meskipun terdapat pola data yang sama. Dengan demikian, risiko serangan yang memanfaatkan kemiripan pola data (*pattern analysis attack*) dapat diminimalkan.

Selain itu, secret key yang digunakan dalam proses enkripsi dan dekripsi tidak disimpan di dalam *QR Code* maupun basis data. *Secret key* ditempatkan secara aman pada sisi *backend* menggunakan mekanisme *environment variable*, sehingga hanya dapat diakses oleh modul enkripsi dan dekripsi selama sistem dijalankan. Mekanisme tersebut mencegah pengguna maupun pihak yang tidak berwenang memperoleh akses terhadap kunci kriptografi, meskipun berhasil memperoleh salinan Sertifikat ETP atau *QR Code*.

Berdasarkan mekanisme tersebut, sistem yang diusulkan tidak hanya memanfaatkan *QR Code* sebagai media penyimpanan informasi, tetapi juga mengintegrasikan algoritma AES-128 sebagai mekanisme perlindungan data sebelum informasi disematkan ke dalam *QR Code*. Pendekatan ini mampu meningkatkan aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan keaslian (*authenticity*) data, sehingga proses verifikasi Sertifikat ETP menjadi lebih aman, cepat, akurat, dan andal dibandingkan penggunaan *QR Code* konvensional.

2.3. Implementasi Sistem

Tahap implementasi merupakan proses menerjemahkan hasil perancangan sistem ke dalam bentuk aplikasi yang dapat digunakan. Pada penelitian ini, sistem dikembangkan dalam bentuk aplikasi berbasis web menggunakan arsitektur *client-server*. Antarmuka (*frontend*) dibangun menggunakan *React* untuk memberikan pengalaman pengguna yang interaktif, sedangkan *backend* dikembangkan menggunakan *Node.js* dengan framework *Express.js* sebagai pengelola logika aplikasi dan komunikasi dengan basis data. Seluruh data sertifikat disimpan menggunakan *MongoDB*, yang berfungsi sebagai media penyimpanan informasi mahasiswa, data nilai *English Test Program* (ETP), serta data validasi sertifikat.

Implementasi algoritma *Advanced Encryption Standard (AES-128*) dilakukan menggunakan pustaka *CryptoJS* pada sisi *backend*. Data penting yang terdiri atas Nomor Induk Mahasiswa (NIM), nama mahasiswa, nilai *Listening*, *Structure*, *Reading*, dan *Total Score* terlebih dahulu dikonversi menjadi *plaintext*, kemudian dienkripsi menggunakan kunci rahasia (*secret key*) sehingga menghasilkan *ciphertext*. Selanjutnya, *ciphertext* tersebut dikodekan ke dalam bentuk *QR Code* dan disematkan secara

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

otomatis pada Sertifikat ETP berformat PDF. Dengan mekanisme tersebut, informasi yang tersimpan di dalam QR Code tidak dapat dibaca secara langsung tanpa melalui proses dekripsi menggunakan kunci yang sesuai.

Selain proses penerbitan sertifikat, sistem juga mengimplementasikan modul verifikasi yang dapat diakses oleh pengguna tanpa memerlukan proses autentikasi. Modul ini menyediakan dua mekanisme verifikasi, yaitu melalui unggah dokumen Sertifikat ETP dalam format PDF maupun melalui pemindaian QR Code secara langsung menggunakan kamera perangkat. Pada proses verifikasi, sistem akan mengekstrak *ciphertext* dari *QR Code*, melakukan proses dekripsi menggunakan algoritma AES-128, kemudian mencocokkan hasil dekripsi dengan data yang tersimpan pada basis data. Apabila seluruh data sesuai, sistem akan menampilkan status Valid, sedangkan apabila ditemukan ketidaksesuaian data atau QR Code tidak dapat didekripsi, sistem akan memberikan status Invalid sebagai indikasi bahwa sertifikat telah dimanipulasi atau tidak berasal dari sistem yang sah.

Implementasi tersebut menghasilkan sebuah sistem yang tidak hanya mampu menerbitkan Sertifikat ETP secara digital, tetapi juga menyediakan mekanisme verifikasi yang cepat, mudah diakses, dan memiliki tingkat keamanan yang lebih tinggi dibandingkan penggunaan *QR Code* konvensional. Dengan demikian, implementasi algoritma AES-128 yang diintegrasikan dengan teknologi QR Code diharapkan mampu meningkatkan keamanan, menjaga integritas data, serta meminimalkan risiko pemalsuan Sertifikat ETP di lingkungan Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji.

2.4. Pengujian Sistem

Tahap pengujian sistem dilakukan untuk mengevaluasi tingkat keberhasilan implementasi aplikasi yang telah dikembangkan, baik dari aspek fungsional maupun aspek keamanan. Pengujian bertujuan memastikan bahwa seluruh fitur sistem berjalan sesuai dengan kebutuhan yang telah ditetapkan serta mampu memberikan perlindungan terhadap upaya pemalsuan Sertifikat English Test Program (ETP). Pada penelitian ini, pengujian sistem terdiri atas tiga jenis pengujian, yaitu Black Box Testing, Avalanche Effect, dan pengujian manipulasi sertifikat.

Pengujian fungsional dilakukan menggunakan metode Black Box Testing, yaitu metode pengujian yang berfokus pada kesesuaian fungsi sistem terhadap spesifikasi kebutuhan tanpa memperhatikan struktur internal kode program [12]. Metode ini digunakan untuk memastikan bahwa setiap fitur pada aplikasi dapat berjalan sesuai dengan fungsi yang telah dirancang [16]. Pengujian dilakukan terhadap 12 skenario yang mewakili seluruh fungsi utama sistem, yaitu registrasi administrator, login administrator, logout administrator, input data sertifikat, pembangkitan Sertifikat ETP dalam format PDF, pembangkitan QR Code, unggah Sertifikat ETP dalam format PDF, validasi sertifikat PDF, pemindaian QR Code, proses dekripsi data QR Code, verifikasi keaslian sertifikat, serta pengujian responsive layout. Setiap skenario dievaluasi berdasarkan kesesuaian keluaran sistem dengan hasil yang diharapkan untuk memastikan bahwa seluruh fungsi aplikasi berjalan sesuai spesifikasi.

Pengujian Avalanche Effect dilakukan untuk mengevaluasi kualitas implementasi algoritma AES-128 dalam menghasilkan perubahan ciphertext akibat perubahan kecil pada plaintext [13]. Pengujian dilakukan menggunakan 10 sampel data, yaitu dengan mengubah satu bit pada plaintext, kemudian membandingkan hasil ciphertext yang dihasilkan untuk menghitung jumlah bit yang mengalami perubahan. Persentase Avalanche Effect dihitung menggunakan Persamaan (1).

$$\textit{Avalanche Effect} = \frac{\text{Jumlah bit yang berubah}}{\text{Jumlah total bit ciphertext}} \times 100\% \qquad (1)$$

Semakin besar nilai *Avalanche Effect* yang diperoleh dan mendekati **50%**, semakin baik tingkat difusi (*diffusion*) algoritma kriptografi yang digunakan. Pengujian ini bertujuan memastikan bahwa perubahan yang sangat kecil pada *plaintext* menghasilkan perubahan yang signifikan pada *ciphertext*, sehingga pola data asli menjadi sulit diprediksi dan meningkatkan ketahanan sistem terhadap berbagai bentuk serangan kriptanalisis.

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

Pengujian keamanan dilakukan melalui simulasi manipulasi Sertifikat ETP untuk mengevaluasi kemampuan sistem dalam mendeteksi berbagai bentuk pemalsuan dokumen digital. Pengujian dilakukan menggunakan **empat skenario manipulasi** yang dipilih karena merepresentasikan bentuk ancaman yang paling mungkin terjadi pada implementasi Sertifikat ETP berbasis *QR Code*. Keempat skenario tersebut meliputi: **(1)** perubahan isi dokumen PDF tanpa mengubah *QR Code*, **(2)** penggantian *QR Code* menggunakan *QR Code* dari sertifikat lain, **(3)** pembuatan *QR Code* baru menggunakan data yang tidak sah, dan **(4)** pemalsuan keseluruhan dokumen menggunakan desain sertifikat tiruan. Pemilihan keempat skenario tersebut didasarkan pada kemampuannya dalam merepresentasikan seluruh bentuk serangan utama terhadap sistem, yaitu manipulasi isi dokumen, penyalahgunaan *QR Code*, pembuatan *QR Code* palsu, serta pemalsuan dokumen secara menyeluruh. Pada setiap skenario, sistem melakukan ekstraksi *QR Code*, proses dekripsi *ciphertext*, serta pencocokan hasil dekripsi dengan data yang tersimpan pada basis data untuk menentukan status keaslian sertifikat.

Melalui ketiga metode pengujian tersebut, penelitian ini mengevaluasi keberhasilan implementasi sistem dari aspek fungsional maupun keamanan. Pengujian *Black Box Testing* digunakan untuk memastikan bahwa seluruh fitur aplikasi berjalan sesuai dengan kebutuhan sistem, pengujian *Avalanche Effect* digunakan untuk mengevaluasi kualitas implementasi algoritma AES-128, sedangkan pengujian manipulasi sertifikat digunakan untuk mengukur kemampuan sistem dalam mendeteksi berbagai bentuk pemalsuan dokumen digital. Hasil dari masing-masing pengujian selanjutnya dianalisis pada bagian hasil dan pembahasan untuk menentukan tingkat efektivitas sistem dalam meningkatkan keamanan serta mendukung proses verifikasi keaslian Sertifikat *English Test Program* (ETP).

2.5. Analisis Data

Pada tahap akhir penelitian dilakukan analisis terhadap seluruh hasil pengujian untuk mengetahui tingkat keberhasilan sistem yang dikembangkan. Analisis dilakukan secara deskriptif berdasarkan hasil *Black Box Testing*, *Avalanche Effect*, dan pengujian manipulasi sertifikat.

Hasil *Black Box Testing* dianalisis berdasarkan kesesuaian antara keluaran sistem dengan spesifikasi fungsional yang telah ditentukan. Setiap skenario pengujian dinyatakan berhasil apabila fungsi yang diuji menghasilkan keluaran sesuai dengan hasil yang diharapkan. Persentase keberhasilan dihitung menggunakan Persamaan (2).

$$\text{Persentase Keberhasilan} = \frac{\text{Jumlah Skenario Berhasil}}{\text{Jumlah Seluruh Skenario}} \times 100\% \qquad (2)$$

Selanjutnya, hasil pengujian *Avalanche Effect* dianalisis berdasarkan persentase perubahan bit pada *ciphertext*. Implementasi algoritma AES-128 dinilai memiliki karakteristik keamanan yang baik apabila menghasilkan nilai *Avalanche Effect* yang mendekati 50%, sehingga menunjukkan bahwa perubahan kecil pada *plaintext* mampu menghasilkan perubahan yang signifikan pada *ciphertext*.

Analisis berikutnya dilakukan terhadap hasil pengujian manipulasi sertifikat. Sistem dinyatakan berhasil apabila mampu mengidentifikasi setiap skenario pemalsuan melalui proses dekripsi QR Code dan pencocokan data terhadap basis data. Sertifikat dikategorikan Valid apabila seluruh data hasil dekripsi sesuai dengan data yang tersimpan pada basis data, sedangkan sertifikat dikategorikan Invalid apabila ditemukan ketidaksesuaian data, QR Code tidak dapat didekripsi, atau QR Code tidak berasal dari sistem yang sah.

Hasil analisis dari ketiga metode pengujian tersebut kemudian digunakan sebagai dasar untuk mengevaluasi efektivitas implementasi algoritma AES-128 dalam meningkatkan keamanan, menjaga integritas data, serta mencegah pemalsuan Sertifikat *English Test Program* (ETP).

3. HASIL DAN PEMBAHASAN

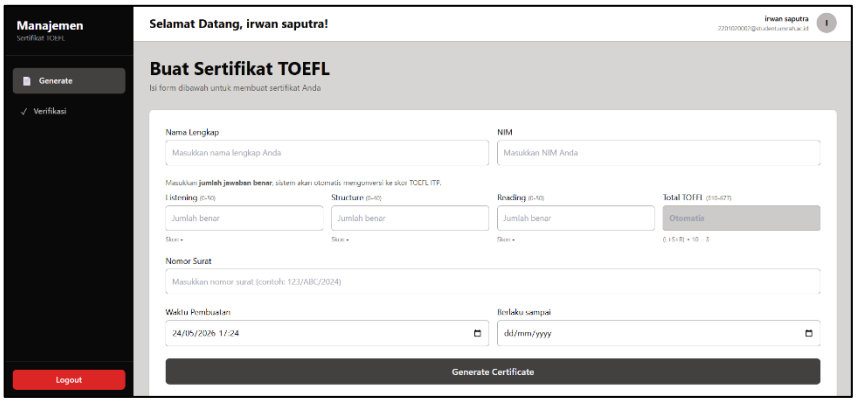
Hasil penelitian ini disajikan berdasarkan tahapan implementasi dan pengujian sistem yang telah dilakukan sesuai dengan metode penelitian yang dirancang. Pembahasan diawali dengan implementasi sistem pencegahan pemalsuan Sertifikat *English Test Program* (ETP) menggunakan algoritma *Advanced Encryption Standard* (AES-128) yang diintegrasikan dengan *QR Code*, kemudian dilanjutkan dengan pengujian fungsional menggunakan metode *Black Box Testing*, serta analisis keamanan melalui

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

pengujian *avalanche effect* dan simulasi berbagai skenario pemalsuan sertifikat. Setiap hasil yang diperoleh selanjutnya dianalisis untuk mengevaluasi tingkat keberhasilan implementasi sistem dalam meningkatkan keamanan, menjaga integritas data, serta mendukung proses verifikasi keaslian Sertifikat ETP di Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji.

3.1. Implementasi Sistem Pencegahan Pemalsuan Sertifikat ETP

Penelitian ini menghasilkan sebuah aplikasi berbasis web yang menerapkan algoritma *Advanced Encryption* Standard (AES-128) sebagai mekanisme pengamanan data pada Sertifikat *English Test Program* (ETP) di Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji. Sistem dikembangkan menggunakan *React* sebagai *frontend*, *Node.js* dan *Express.js* sebagai *backend*, serta *MongoDB* sebagai basis data. Implementasi AES-128 dilakukan menggunakan pustaka *CryptoJS* sehingga proses enkripsi dapat dilakukan secara efisien sebelum data disematkan ke dalam QR Code. Data yang dienkripsi meliputi Nomor Induk Mahasiswa (NIM), nama mahasiswa, skor *Listening*, *Structure*, *Reading*, dan total skor TOEFL. Seluruh data tersebut terlebih dahulu diubah menjadi *ciphertext* berformat Base64 sebelum dibangkitkan menjadi QR Code yang terintegrasi pada Sertifikat ETP digital. Untuk memberikan gambaran mengenai antarmuka aplikasi yang dikembangkan, tampilan halaman utama administrator disajikan pada Gambar 3.



Gambar 3. Dashboard Administrator

Berdasarkan Gambar 3, sistem berhasil mengintegrasikan seluruh proses pengelolaan Sertifikat *English Test Program* (ETP) ke dalam satu platform berbasis web, mulai dari pengelolaan data mahasiswa, penerbitan sertifikat, hingga proses verifikasi keaslian dokumen. Integrasi tersebut menghilangkan ketergantungan pada proses manual yang sebelumnya dilakukan secara terpisah sehingga mampu meningkatkan efisiensi pengelolaan sertifikat sekaligus meminimalkan potensi kesalahan administrasi. Selain meningkatkan kemudahan penggunaan melalui antarmuka yang *user-friendly*, arsitektur berbasis web juga memungkinkan proses penerbitan dan validasi dilakukan secara terpusat sehingga mendukung konsistensi data dan mempercepat layanan akademik. Hasil tersebut sejalan dengan penelitian sebelumnya yang menyatakan bahwa digitalisasi layanan akademik mampu meningkatkan efektivitas pengelolaan dokumen sekaligus meminimalkan kesalahan administratif [14].

Proses penerbitan Sertifikat ETP diawali dengan pengisian identitas mahasiswa dan nilai hasil tes yang meliputi Nomor Induk Mahasiswa (NIM), Nama Mahasiswa, *Listening, Structure*, dan *Reading*. Setelah seluruh data dimasukkan, sistem secara otomatis menghitung skor total TOEFL, kemudian menggabungkan seluruh informasi tersebut menjadi satu kesatuan *plaintext*. Selanjutnya, *plaintext* diproses menggunakan algoritma AES-128 sehingga menghasilkan *ciphertext* berformat *Base64*. *Ciphertext* inilah yang kemudian digunakan sebagai *payload* pada QR Code dan disematkan secara otomatis ke dalam Sertifikat ETP digital.

Sebelum dilakukan proses enkripsi, sistem terlebih dahulu menentukan komponen data yang akan diamankan menggunakan algoritma AES-128. Komponen data tersebut disajikan pada Tabel 1.

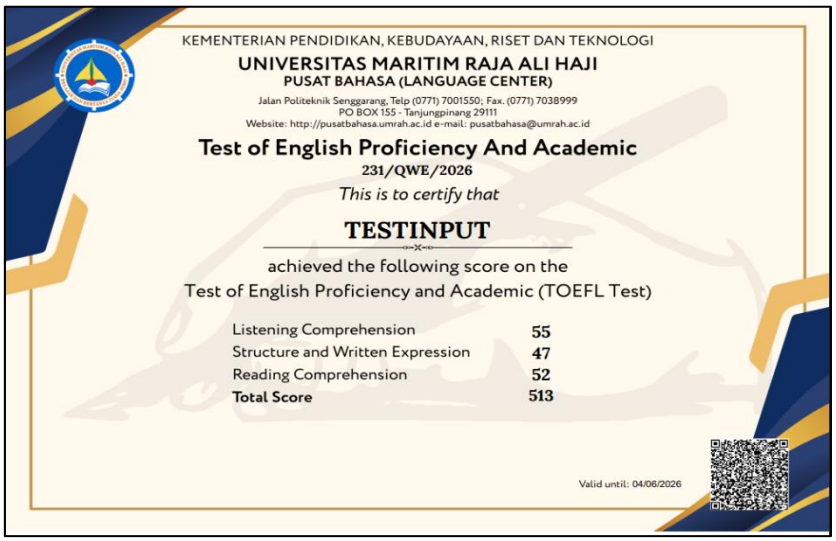
Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

Tabel 1. Komponen Data yang Dienkripsi Menggunakan Algoritma AES-128

No	Komponen Data	Keterangan
1	NIM	Nomor Induk Mahasiswa
2	Nama Mahasiswa	Identitas mahasiswa
3	Listening	Skor kemampuan Listening
4	Structure	Skor kemampuan Structure
5	Reading	Skor kemampuan Reading
6	Total TOEFL	Total skor hasil konversi ETP

Berdasarkan Tabel 1, seluruh informasi yang bersifat sensitif dienkripsi sebelum disematkan ke dalam *QR Code*. Pendekatan ini memastikan bahwa data penting pada Sertifikat ETP tidak dapat dibaca maupun dimodifikasi secara langsung oleh pihak yang tidak memiliki kunci enkripsi. Berbeda dengan penelitian yang memanfaatkan AES hanya sebagai mekanisme pengamanan data digital, penelitian ini mengintegrasikan hasil enkripsi secara langsung ke dalam *QR Code* sehingga proses pengamanan dan autentikasi sertifikat berlangsung secara bersamaan. Pendekatan tersebut tidak hanya menjaga aspek *confidentiality* dan *integrity*, tetapi juga memperkuat mekanisme verifikasi keaslian dokumen melalui pencocokan data hasil dekripsi dengan basis data [15]. Namun demikian, pada penelitian ini AES-128 tidak hanya digunakan sebagai metode pengamanan data, tetapi juga diintegrasikan dengan QR Code sebagai mekanisme autentikasi Sertifikat ETP.

Hasil implementasi proses enkripsi dan pembangkitan QR Code menghasilkan Sertifikat ETP digital yang telah dilengkapi dengan QR Code terenkripsi. Tampilan sertifikat yang dihasilkan oleh sistem ditunjukkan pada Gambar 4.



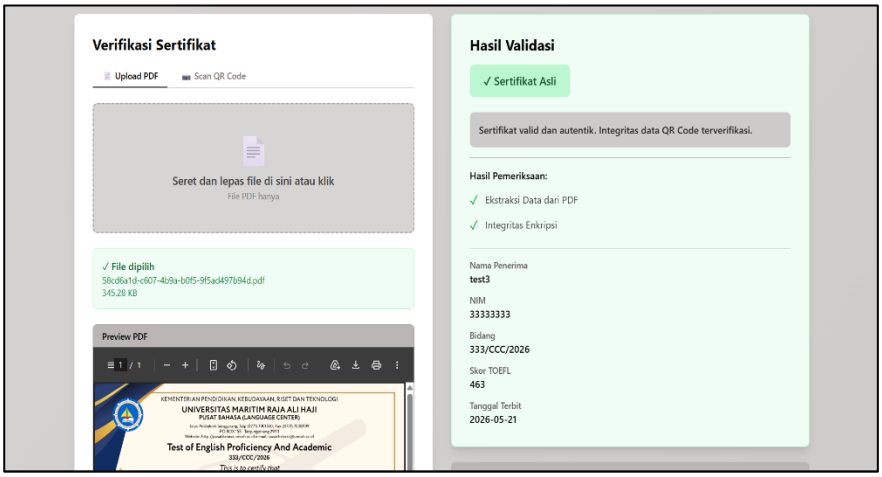
Gambar 4. Sertifikat ETP dengan QR Code Terenkripsi

Berdasarkan Gambar 4, *QR Code* yang dihasilkan tidak lagi berfungsi hanya sebagai media penyimpanan informasi, tetapi juga sebagai media autentikasi yang membawa *ciphertext* hasil enkripsi AES-128. Pendekatan ini memberikan lapisan keamanan tambahan karena informasi yang tersimpan tidak dapat diinterpretasikan tanpa proses dekripsi menggunakan *secret key* yang sesuai. Dibandingkan *QR Code* konvensional yang hanya menyimpan data dalam bentuk *plaintext*, mekanisme yang diusulkan mampu mengurangi risiko duplikasi maupun modifikasi informasi secara langsung. Temuan ini sejalan dengan penelitian yang menunjukkan bahwa integrasi QR Code dengan algoritma kriptografi mampu meningkatkan keamanan dokumen digital melalui perlindungan terhadap manipulasi dan pemalsuan informasi [16].

Selain modul penerbitan sertifikat, penelitian ini juga menghasilkan modul verifikasi yang dapat digunakan oleh masyarakat maupun instansi terkait untuk melakukan pengecekan keaslian Sertifikat ETP. Sistem menyediakan dua mekanisme verifikasi, yaitu melalui unggah dokumen PDF

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

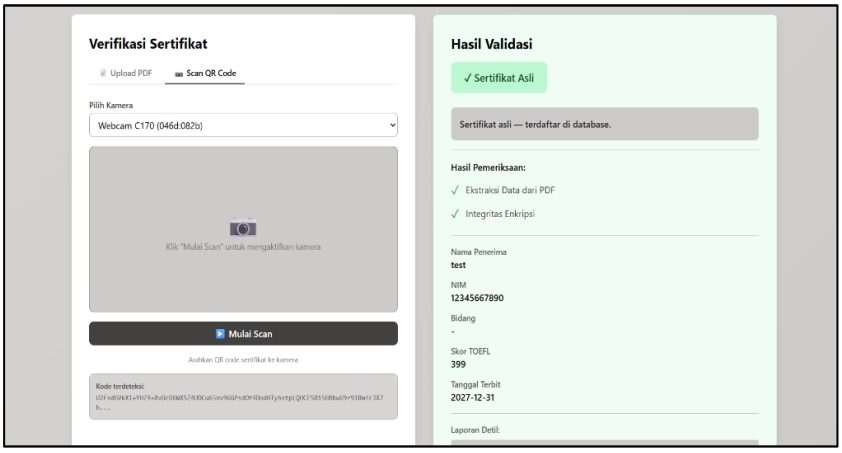
dan pemindaian QR Code secara langsung menggunakan kamera perangkat. Implementasi proses validasi melalui unggah dokumen PDF ditunjukkan pada Gambar 5.



Gambar 5. Halaman Validasi Sertifikat melalui Upload PDF

Mekanisme verifikasi melalui unggah dokumen PDF memberikan fleksibilitas bagi pengguna yang telah memiliki Sertifikat ETP dalam bentuk digital tanpa memerlukan perangkat tambahan untuk melakukan pemindaian *QR Code*. Proses ekstraksi *QR Code*, dekripsi, dan pencocokan data dilakukan secara otomatis sehingga mampu mempercepat proses verifikasi sekaligus mengurangi potensi kesalahan yang umumnya terjadi pada proses pemeriksaan manual. Pendekatan ini menunjukkan bahwa keamanan sistem tidak hanya bergantung pada algoritma kriptografi yang digunakan, tetapi juga pada integrasi proses verifikasi dengan basis data sehingga setiap perubahan pada dokumen dapat segera teridentifikasi.

Selain melalui unggah dokumen PDF, sistem juga menyediakan mekanisme validasi menggunakan kamera perangkat untuk melakukan pemindaian QR Code secara langsung. Implementasi fitur tersebut ditunjukkan pada Gambar 6.



Gambar 6. Halaman Validasi Sertifikat melalui Pemindaian QR Code

Fitur verifikasi melalui pemindaian *QR Code* secara langsung memberikan keunggulan dari sisi efisiensi karena proses autentikasi dapat dilakukan secara *real-time* tanpa memerlukan autentikasi administrator. Kemudahan tersebut memungkinkan pihak eksternal, seperti institusi pendidikan, perusahaan, maupun lembaga penyedia beasiswa, melakukan verifikasi keaslian Sertifikat ETP secara mandiri. Dibandingkan mekanisme verifikasi manual yang mengandalkan pemeriksaan visual,

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

pendekatan ini menghasilkan proses yang lebih objektif, cepat, dan konsisten karena keputusan valid atau tidak valid ditentukan berdasarkan hasil dekripsi dan pencocokan data pada basis data.

Secara keseluruhan, hasil implementasi menunjukkan bahwa integrasi algoritma AES-128 dengan *QR Code* berhasil membangun mekanisme keamanan yang lebih baik dibandingkan penggunaan *QR Code* manual. Informasi yang tersimpan pada sertifikat tidak lagi berada dalam bentuk *plaintext*, melainkan telah dienkripsi menjadi *ciphertext* sehingga hanya dapat dipulihkan menggunakan *secret key* yang sesuai. Temuan ini sejalan dengan penelitian yang menunjukkan efektivitas AES dalam melindungi data digital [17], serta mendukung penelitian yang memanfaatkan *QR Code* sebagai media autentikasi dokumen [8]. Selain itu, hasil penelitian ini juga memperkuat temuan mengenai integrasi kriptografi dan *QR Code* dalam meningkatkan keamanan dokumen digital [16]. Namun demikian, penelitian ini memiliki kontribusi yang berbeda karena mengembangkan mekanisme verifikasi berbasis web yang mengintegrasikan proses enkripsi, dekripsi, pembangkitan *QR Code*, serta pencocokan data dengan basis data secara otomatis. Pendekatan tersebut menghasilkan mekanisme *anti-forgery* yang tidak hanya mampu melindungi data sertifikat, tetapi juga mendeteksi berbagai bentuk manipulasi dokumen secara otomatis sehingga memberikan tingkat keamanan yang lebih komprehensif dibandingkan penelitian terdahulu.

Secara keseluruhan, hasil implementasi menunjukkan bahwa integrasi algoritma AES-128 dengan QR Code berhasil membangun mekanisme keamanan yang lebih baik dibandingkan penggunaan QR Code manual. Informasi yang tersimpan pada sertifikat tidak lagi berada dalam bentuk *plaintext*, melainkan telah dienkripsi menjadi *ciphertext* sehingga hanya dapat dipulihkan menggunakan kunci yang sesuai. Temuan ini memperkuat hasil penelitian terdahulu yang menyatakan bahwa kombinasi algoritma kriptografi dan QR Code mampu meningkatkan keamanan dokumen digital [18]. Akan tetapi, penelitian ini memiliki kontribusi yang berbeda karena mengembangkan mekanisme anti-*forgery* yang secara khusus ditujukan untuk mencegah pemalsuan Sertifikat ETP melalui penyematan *ciphertext* AES-128 ke dalam QR Code. Pendekatan tersebut mampu mengatasi kelemahan sistem sebelumnya yang masih menggunakan QR Code manual sehingga lebih rentan terhadap duplikasi maupun manipulasi data.

3.2. Pengujian Fungsional Sistem Menggunakan *Black Box Testing*

Setelah proses implementasi sistem selesai dilakukan, tahap berikutnya adalah pengujian fungsional menggunakan metode *Black Box Testing*. Metode ini dipilih karena mampu mengevaluasi kesesuaian fungsi sistem berdasarkan kebutuhan pengguna (*user requirements*) tanpa bergantung pada struktur internal maupun kode program, sehingga sesuai untuk menilai keberhasilan implementasi sistem dari perspektif pengguna akhir [19]. Pengujian bertujuan untuk memastikan bahwa seluruh fungsi pada sistem telah berjalan sesuai dengan kebutuhan yang ditetapkan. Pengujian dilakukan terhadap 12 skenario pengujian yang mencakup seluruh fitur utama sistem, yaitu registrasi administrator, login, *logout*, pengelolaan data sertifikat, penerbitan Sertifikat *English Test Program* (ETP), pembangkitan *QR Code* terenkripsi, unggah dokumen PDF, validasi sertifikat, pemindaian *QR Code*, dekripsi data, verifikasi keaslian sertifikat, serta pengujian *responsive layout*. Proses pengujian dilakukan oleh peneliti bersama administrator UPA Bahasa Universitas Maritim Raja Ali Haji sebagai pengguna sistem untuk memastikan bahwa setiap fungsi telah berjalan sesuai dengan kebutuhan operasional. Hasil pengujian setiap skenario kemudian dibandingkan dengan keluaran yang diharapkan untuk menilai tingkat keberhasilan implementasi sistem.

Untuk mengevaluasi kinerja sistem, dilakukan pengujian terhadap dua belas skenario yang mewakili seluruh fungsi utama aplikasi. Ringkasan hasil pengujian disajikan pada Tabel 2.

Tabel 2. Hasil Pengujian *Black Box Testing*

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian	Status
1	Registrasi Administrator	Data berhasil disimpan	Berhasil	Valid
2	Login Administrator	Administrator berhasil masuk ke sistem	Berhasil	Valid
3	Logout Administrator	Sistem keluar dari akun administrator	Berhasil	Valid
4	Input Data Sertifikat	Data berhasil disimpan	Berhasil	Valid
5	*Generate* Sertifikat PDF	Sertifikat berhasil dibuat	Berhasil	Valid

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

6	*Generate* QR Code	QR Code berhasil dibuat	Berhasil	Valid
7	Upload Sertifikat PDF	Dokumen berhasil diproses	Berhasil	Valid
8	Validasi Sertifikat PDF	Status sertifikat ditampilkan	Berhasil	Valid
9	Scan QR Code	QR Code berhasil dipindai	Berhasil	Valid
10	Dekripsi Data QR Code	Data berhasil didekripsi	Berhasil	Valid
11	Verifikasi Keaslian Sertifikat	Status valid/invalid berhasil ditampilkan	Berhasil	Valid
12	Responsive Layout	Antarmuka berjalan pada berbagai perangkat	Berhasil	Valid

Berdasarkan Tabel 2, seluruh skenario pengujian menunjukkan hasil yang sesuai dengan keluaran yang diharapkan. Seluruh fungsi sistem, mulai dari proses registrasi administrator, autentikasi pengguna, penerbitan sertifikat, pembangkitan QR Code, validasi dokumen PDF, hingga pemindaian QR Code berhasil dijalankan tanpa ditemukan kesalahan fungsional. Selain pengujian pada kondisi normal, sistem juga diuji menggunakan beberapa skenario negative testing, seperti unggah dokumen PDF yang kosong atau tidak valid serta pemindaian QR Code yang rusak (corrupted QR Code) atau tidak dapat dibaca. Pada kedua kondisi tersebut, sistem berhasil menolak proses verifikasi dan menampilkan pesan kesalahan yang sesuai tanpa menyebabkan kegagalan sistem maupun kesalahan proses dekripsi. Hasil tersebut menunjukkan bahwa mekanisme validasi masukan (input validation) telah berjalan dengan baik dalam menangani kondisi yang tidak memenuhi persyaratan sistem. Dengan demikian, tingkat keberhasilan pengujian mencapai 100%, yang menunjukkan bahwa seluruh fungsi sistem, baik pada kondisi normal maupun kondisi tidak valid, telah memenuhi kebutuhan fungsional yang dirancang pada tahap analisis dan perancangan sistem.

Keberhasilan seluruh skenario pengujian menunjukkan bahwa integrasi antara algoritma AES-128, QR Code, dan mekanisme validasi berbasis web telah diimplementasikan secara baik. Pengujian ini membuktikan bahwa setiap fitur mampu menjalankan fungsi sesuai spesifikasi, baik pada proses penerbitan maupun proses verifikasi Sertifikat ETP. Hasil tersebut sejalan dengan penelitian sebelumnya yang menyatakan bahwa *Black Box Testing* merupakan metode yang efektif untuk mengevaluasi kesesuaian fungsi sistem terhadap kebutuhan pengguna tanpa harus menguji struktur internal perangkat lunak [20].

Selain memastikan keberhasilan setiap fungsi, hasil pengujian juga menunjukkan bahwa mekanisme verifikasi yang dikembangkan mampu memberikan respons yang konsisten terhadap setiap masukan pengguna. Keberhasilan tersebut didukung oleh integrasi yang baik antara *frontend*, *backend*, dan basis data, serta penerapan validasi data dan mekanisme enkripsi-dekripsi AES-128 yang berjalan sesuai dengan rancangan sistem. Kondisi ini menunjukkan bahwa sistem memiliki tingkat reliabilitas yang baik untuk diimplementasikan pada lingkungan operasional UPA Bahasa Universitas Maritim Raja Ali Haji. Dengan demikian, hasil pengujian *Black Box Testing* membuktikan bahwa aplikasi yang dikembangkan telah memenuhi aspek *functional suitability*, sehingga layak digunakan untuk mendukung proses penerbitan dan verifikasi Sertifikat *English Test Program* (ETP) secara aman dan efisien.

3.3. Analisis Keamanan Sistem Menggunakan Algoritma AES-128

Selain dilakukan pengujian terhadap aspek fungsional, penelitian ini juga mengevaluasi tingkat keamanan sistem melalui pengujian *Avalanche Effect* dan simulasi berbagai skenario pemalsuan sertifikat. Pengujian ini bertujuan untuk mengetahui kemampuan algoritma *Advanced Encryption Standard* (AES-128) dalam menjaga kerahasiaan (*confidentiality*) dan integritas (*integrity*) data, sekaligus membuktikan efektivitas sistem dalam mendeteksi manipulasi terhadap Sertifikat *English Test Program* (ETP). Ruang lingkup pengujian keamanan meliputi tiga aspek utama, yaitu kerahasiaan data yang dievaluasi melalui pengujian *Avalanche Effect*, integritas data yang diuji melalui proses pencocokan hasil dekripsi dengan data pada basis data, serta keaslian (*authenticity*) sertifikat yang dievaluasi melalui simulasi berbagai skenario pemalsuan dokumen. Dengan ruang lingkup tersebut, pengujian tidak hanya menilai kekuatan algoritma kriptografi, tetapi juga kemampuan sistem dalam mempertahankan keaslian dan keutuhan sertifikat selama proses penerbitan maupun verifikasi.

Pengujian *Avalanche Effect* dilakukan dengan mengubah satu bit pada *plaintext*, kemudian mengukur perubahan bit yang dihasilkan pada *ciphertext*. Parameter ini digunakan untuk mengevaluasi kualitas

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

algoritma kriptografi, di mana algoritma yang baik diharapkan menghasilkan nilai *Avalanche Effect* mendekati 50%. Dalam penelitian ini, pengujian *Avalanche Effect* difokuskan pada evaluasi aspek kerahasiaan (*confidentiality*) data dengan mengukur kemampuan algoritma AES-128 dalam menghasilkan *ciphertext* yang berbeda secara signifikan akibat perubahan kecil pada *plaintext*. Berdasarkan 10 sampel pengujian, implementasi algoritma AES-128 pada sistem menghasilkan nilai rata-rata *Avalanche Effect* sebesar 49,87%. Nilai tersebut menunjukkan bahwa perubahan yang sangat kecil pada data masukan mampu menghasilkan perubahan yang signifikan pada *ciphertext*, sehingga memenuhi karakteristik dasar algoritma kriptografi simetris yang memiliki sifat difusi (*diffusion*) yang baik. Sementara itu, aspek integritas (*integrity*) dan keaslian (*authenticity*) sistem tidak dievaluasi melalui pengujian ini, melainkan melalui simulasi berbagai skenario manipulasi sertifikat yang dibahas pada pengujian keamanan berikutnya. Hasil ini sejalan dengan penelitian sebelumnya yang menyatakan bahwa algoritma AES memiliki sensitivitas tinggi terhadap perubahan data masukan sehingga mampu meningkatkan ketahanan terhadap berbagai bentuk serangan kriptanalisis [21].

Selain pengujian *Avalanche Effect*, sistem juga diuji melalui empat skenario manipulasi Sertifikat ETP untuk mengevaluasi kemampuan mekanisme verifikasi dalam mendeteksi dokumen yang telah dipalsukan. Skenario pertama dilakukan dengan mengubah nama mahasiswa pada dokumen PDF menggunakan aplikasi pengolah PDF, sementara QR Code asli tetap dipertahankan. Pada kondisi tersebut sistem berhasil mendeteksi ketidaksesuaian antara informasi hasil dekripsi QR Code dengan data yang tersimpan pada basis data, sehingga sertifikat dinyatakan Invalid. Selain itu, sistem juga mengidentifikasi adanya perubahan metadata dokumen, seperti ukuran berkas dan waktu modifikasi (*modified timestamp*), yang semakin memperkuat indikasi terjadinya manipulasi.

Skenario kedua dilakukan dengan mengganti *QR Code* asli menggunakan *QR Code* milik sertifikat lain. Hasil pengujian menunjukkan bahwa sistem tetap mampu membaca *QR Code* yang dipindai, namun informasi hasil dekripsi tidak sesuai dengan data sertifikat yang sedang diverifikasi. Akibatnya, sistem secara otomatis menolak proses verifikasi dan menampilkan status Invalid. Proses verifikasi pada skenario ini berlangsung dengan waktu rata-rata sebesar 1,18 detik sejak *QR Code* dipindai hingga status *Invalid* ditampilkan kepada pengguna. Temuan ini menunjukkan bahwa mekanisme verifikasi tidak hanya memeriksa keberadaan *QR Code*, tetapi juga memastikan kesesuaian antara data hasil dekripsi dengan data yang tersimpan pada basis data.

Skenario ketiga dilakukan dengan membuat QR Code baru menggunakan *plaintext* sembarang, kemudian menyematkannya pada dokumen sertifikat tiruan. Pada skenario ini sistem gagal melakukan proses dekripsi karena QR Code tidak dihasilkan menggunakan kunci rahasia AES-128 yang sama dengan sistem. Selain itu, data hasil pembacaan QR Code juga tidak memiliki kecocokan dengan data yang tersimpan pada basis data, sehingga sertifikat dinyatakan tidak valid. Hasil tersebut menunjukkan bahwa keberhasilan proses verifikasi sangat bergantung pada penggunaan kunci enkripsi yang benar, sehingga QR Code tidak dapat dipalsukan hanya dengan membuat kode baru secara sembarangan.

Skenario terakhir dilakukan dengan memalsukan keseluruhan dokumen sertifikat, baik tanpa menyertakan *QR Code* maupun dengan menggunakan gambar *QR Code* yang bukan merupakan hasil enkripsi sistem. Pada kondisi ini, sistem tidak dapat mengekstrak *ciphertext* yang valid dari *QR Code* sehingga proses verifikasi langsung dihentikan dan sertifikat dinyatakan tidak sah. Berdasarkan empat skenario manipulasi yang diuji, sistem berhasil mendeteksi seluruh bentuk pemalsuan dengan tingkat akurasi deteksi sebesar 100%, yang ditunjukkan oleh kemampuan sistem dalam memberikan status *Invalid* pada setiap dokumen yang telah dimanipulasi. Kemampuan sistem dalam menolak seluruh bentuk manipulasi tersebut menunjukkan bahwa mekanisme autentikasi yang dikembangkan mampu memberikan perlindungan yang lebih baik dibandingkan penggunaan QR Code konvensional yang hanya menyimpan informasi dalam bentuk *plaintext* [22].

Secara keseluruhan, hasil pengujian keamanan menunjukkan bahwa sistem berhasil mendeteksi seluruh skenario pemalsuan yang disimulasikan dengan tingkat akurasi deteksi sebesar 100%. Keberhasilan tersebut membuktikan bahwa implementasi algoritma AES-128 yang diintegrasikan dengan *QR Code* mampu menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), serta keaslian (*authenticity*) data Sertifikat *English Test Program* (ETP). Hasil penelitian ini sejalan dengan penelitian Damanik dan Arif yang menunjukkan bahwa algoritma AES memiliki karakteristik difusi yang baik

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

sehingga efektif digunakan untuk melindungi data digital dari berbagai bentuk serangan kriptanalisis [23]. Selain itu, penelitian ini juga mendukung temuan yang menyatakan bahwa pemanfaatan *QR Code* mampu meningkatkan efisiensi proses verifikasi dokumen digital, meskipun penelitian tersebut belum mengintegrasikan mekanisme enkripsi untuk melindungi informasi yang tersimpan di dalam *QR Code* [24]. Berbeda dengan penelitian-penelitian tersebut, penelitian ini mengintegrasikan algoritma AES-128 dengan *QR Code* pada aplikasi berbasis web yang tidak hanya mengenkripsi data sertifikat, tetapi juga menyediakan mekanisme verifikasi otomatis melalui proses dekripsi dan pencocokan data dengan basis data. Pendekatan tersebut memungkinkan sistem mendeteksi berbagai bentuk manipulasi sertifikat secara real-time, sehingga memberikan kontribusi baru berupa mekanisme *anti-forgery* yang lebih komprehensif untuk mendukung keamanan dokumen akademik digital.

4. KESIMPULAN

Penelitian ini berhasil mengimplementasikan algoritma *Advanced Encryption Standard (AES-128)* ke dalam aplikasi berbasis web sebagai mekanisme pencegahan pemalsuan Sertifikat *English Test Program* (ETP) di Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji. Implementasi dilakukan dengan mengenkripsi data penting sertifikat menjadi *ciphertext* berformat Base64 yang kemudian disematkan ke dalam *QR Code* pada dokumen sertifikat digital. Sistem yang dikembangkan juga mampu melakukan verifikasi keaslian sertifikat melalui mekanisme unggah dokumen PDF maupun pemindaian *QR Code* secara langsung, sehingga memudahkan proses validasi oleh berbagai pihak tanpa memerlukan autentikasi pengguna. Hasil pengujian menunjukkan bahwa seluruh fungsi sistem berjalan sesuai dengan kebutuhan fungsional yang telah dirancang dengan tingkat keberhasilan *Black Box Testing* sebesar 100%, sedangkan pengujian *avalanche effect* memperoleh nilai rata-rata 49,87% yang menunjukkan bahwa implementasi AES-128 telah memenuhi karakteristik keamanan kriptografi simetris. Selain itu, sistem mampu mendeteksi seluruh skenario pemalsuan sertifikat yang disimulasikan, sehingga membuktikan efektivitas integrasi AES-128 dan *QR Code* dalam menjaga integritas serta keaslian dokumen digital.

Hasil penelitian ini memberikan manfaat praktis bagi UPA Bahasa UMRAH sebagai solusi untuk meningkatkan keamanan penerbitan dan verifikasi Sertifikat ETP, sekaligus memperkuat kepercayaan pihak eksternal terhadap keaslian dokumen akademik. Meskipun demikian, penelitian ini masih memiliki keterbatasan karena pengujian keamanan dilakukan pada aspek fungsional dan simulasi pemalsuan, sehingga belum mencakup audit keamanan secara menyeluruh terhadap potensi serangan siber pada lingkungan produksi. Oleh karena itu, penelitian selanjutnya disarankan untuk melakukan *security assessment* oleh pihak ketiga yang independen, menerapkan mekanisme perlindungan tambahan seperti *Web Application Firewall* (WAF) dan *rate limiting*, serta mengembangkan fitur penerbitan sertifikat secara *batch*, integrasi dengan Sistem Informasi Akademik UMRAH, pengembangan aplikasi *mobile* untuk proses verifikasi, dashboard analitik, dan mekanisme *backup* basis data secara otomatis. Pengembangan tersebut diharapkan dapat meningkatkan skalabilitas, keamanan, dan efisiensi sistem sehingga dapat diimplementasikan secara lebih luas pada layanan sertifikasi digital di lingkungan perguruan tinggi.

UCAPAN TERIMA KASIH

Penulis menyampaikan ucapan terima kasih yang sebesar-besarnya seluruh dosen Program Studi Informatika Universitas Maritim Raja Ali Haji atas ilmu dan pengalaman yang telah diberikan selama masa perkuliahan. Penulis turut mengucapkan terima kasih kepada Kepala Unit Penunjang Akademik (UPA) Bahasa Universitas Maritim Raja Ali Haji beserta seluruh staf yang telah memberikan izin, dukungan, serta membantu proses pengumpulan data dan pelaksanaan penelitian. Penghargaan juga diberikan kepada keluarga, rekan-rekan, dan semua pihak yang telah memberikan dukungan moral maupun material sehingga penelitian ini dapat diselesaikan dengan baik. Penulis berharap hasil penelitian ini dapat memberikan kontribusi bagi pengembangan sistem keamanan dokumen digital, khususnya dalam upaya pencegahan pemalsuan sertifikat di lingkungan perguruan tinggi. Segala bentuk bantuan, dukungan, dan kerja sama yang telah diberikan menjadi bagian penting dalam keberhasilan pelaksanaan penelitian ini.

Journal of Artificial Intelligence and Technology Information
Website : https://ejournal.techcart-press.com/index.php/jaiti
E-ISSN 2985-6396
P-ISSN 2985-5306
Volume 4, Number 3, September 2026
https://doi.org/10.58602/jaiti.v4i3.342
Page 542-557

REFERENCES

[1] F. Irianti, S. Rahman, and S. Sahban, "Kekuatan Hukum Pembuktian Tanda Tangan Elektronik (Digital Signature) Dalam Surat-Surat Perjanjian Pemerintah," *J. Lex Philos.*, vol. 5, no. 2, pp. 2117–2136, 2024.
[2] T. A. Gani, *Kedaulatan data digital untuk integritas bangsa*. Syiah Kuala University Press, 2023.
[3] S. Abdullah, "Implementasi blockchain untuk keamanan data akademik dalam sistem informasi perguruan tinggi," *Go Infotech J. Ilm. STMIK AUB*, vol. 31, no. 1, pp. 149–160, 2025.
[4] K. O. Julialevi *et al.*, "Membangun Integritas Ilmiah Melalui Webinar Fraud dalam Akademik dan Penelitian," *ADMA J. Pengabdi. dan Pemberdaya. Masy.*, vol. 6, no. 2, pp. 315–324, 2026.
[5] B. Firmansyah, R. Subekti, N. Purwandari, and R. Karepesina, "Implementasi algoritma keamanan data berbasis enkripsi pada platform cloud computing untuk pembelajaran di SMK Cipta Insani Mandiri," *J. Data Anal. Information, Comput. Sci.*, vol. 2, no. 1, pp. 81–96, 2025.
[6] A. Cahyanti, F. Masykur, and A. F. Cobantoro, "Digitalisasi Perpustakaan Berbasis Qr Code Menggunakan Algoritma AES," *MEKAR J. Inf. Syst. Comput. Appl.*, vol. 1, no. 2, pp. 96–100, 2025.
[7] D. Firdaus and M. Z. Dafy, "Peningkatan Keamanan dan Privasi Aplikasi Website DNA Sequencing Menggunakan Enkripsi AES 256 dan Query Parameterization," *Simpatik J. Sist. Inf. dan Inform.*, vol. 4, no. 2, pp. 79–88, 2024.
[8] M. Halim and O. Pribadi, "Penerapan Qrcode Sebagai Tanda Tangan Digital Dalam Penerbitan Surat Keluar Pada Stmik Methodist Binjai," *J. TIMES*, vol. 13, no. 2, pp. 261–268, 2024.
[9] A. Rahayu, "Metode penelitian dan pengembangan (R&D): Pengertian, jenis dan tahapan," *DIAJAR J. Pendidik. Dan Pembelajaran*, vol. 4, no. 3, pp. 459–470, 2025.
[10] A. Ginting, E. P. Bangun, K. B. Purba, S. Wahyuni, E. N. Pasaribu, and O. Bangun, "Studi Analisis Model Waterfall pada Pengembangan Sistem Informasi," *J. Nirta Stud. Inov.*, vol. 5, no. 2, pp. 109–121, 2026.
[11] H. Aryasuta, F. Nisa, and A. Pratama, "Perancangan Sistem Informasi Pendaftaran dan Penjadwalan Tes TOEFL Berbasis Website di Pusat Bahasa Universitas Malikussaleh," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 6, pp. 9854–9861, 2025.
[12] B. E. Slam, F. Irawan, N. Efranda, and R. Herikson, "Pengujian Sistem Identitas Digital Siswa Berbasis Blockchain untuk Keamanan dan Transparansi Menggunakan Black-Box Testing," *J. Software, Hardw. Inf. Technol.*, vol. 5, no. 2, pp. 72–83, 2025.
[13] W. Prabowo and N. Anwar, "Pengujian Model Simulasi Efek Avalanche Kriptografi Simetris Algoritma AES 128-bit, Mode ECB dan CBC," *IKRA-ITH Inform. J. Komput. dan Inform.*, vol. 9, no. 1, pp. 178–186, 2025.
[14] A. A. Zulfa, T. Ibrahim, and O. Arifudin, "Peran sistem informasi akademik berbasis web dalam upaya meningkatkan efektivitas dan efisiensi pengelolaan akademik di perguruan tinggi," *J. Tahsinia*, vol. 6, no. 1, pp. 115–134, 2025.
[15] F. D. Insani and M. D. Anggraeni, "Analisis Kinerja Algoritma Advanced Encryption Standard (AES) Encryption dan Algoritma Blowfish pada Proses Enkripsi dan Dekripsi," *TRANSFORMASI*, vol. 21, no. 2, 2025.
[16] V. D. P. Anggraini, K. Ibnutama, and Z. Panjaitan, "Implementasi Algoritma AES Pada Qr-Code Untuk Validasi Keaslian Surat Kontrak Kerja Di Pt. Citra Alfa Sasmita," *J. SAINTIKOM (Jurnal Sains Manaj. Inform. dan Komputer)*, vol. 24, no. 2, pp. 252–261, 2025.
[17] M. Tania, T. S. Alasi, and R. Yap, "Algoritma Aes Untuk Keamanan Data Digital Berbasis Web Di Kantor Desa Aman Damai," *J. TIMES*, vol. 13, no. 2, pp. 142–149, 2024.
[18] F. Nuraeni, M. F. Amrulloh, A. Mulyani, and D. Kurniadi, "Implementasi superenkripsi DSA dan AES 128 bit dalam pengamanan file surat digital," *J. Algoritm.*, vol. 22, no. 1, pp. 601–613, 2025.
[19] D. N. Ayyasy and A. Voutama, "Pengujian fungsional sistem rental mobil berbasis web menggunakan metode black box testing," *J. Students 'Research Comput. Sci.*, vol. 7, no. 1, pp. 1–12, 2026.
[20] M. Jibril, "Pengujian sistem informasi e-modul pada SMPN 1 Tempuling menggunakan black box testing," *J. Perangkat Lunak*, vol. 6, no. 2, pp. 327–332, 2024.
[21] Y. Fatma, R. Gunawan, N. Fitri, R. Firdaus, R. Hayami, and S. Soni, "Klasifikasi Algoritma Kriptografi pada Pesan Terenkripsi menggunakan Support Vector Machine (SVM)," *J. FASILKOM*, vol. 15, no. 3, pp. 648–654, 2025.
[22] M. Johari, F. Rafdhi, and M. A. Sutisna, "Model Sistem Registrasi Sertifikat Akademik Berbasis Blockchain untuk Verifikasi Otentik Dokumen Akademik," in *Proceeding of Informatics Collaborations and Dessimenation Meeting*, 2026, pp. 96–106.
[23] N. S. Damanik and S. N. Arif, "Komparasi Algoritma Enkripsi Simetris dan Asimetris Berdasarkan Avalanche Effect dan Waktu Komputasi," *J. Sist. Inf. Triguna Dharma (JURSI TGD)*, vol. 5, no. 3, pp. 906–912, 2026.
[24] R. F. Wulandari, M. N. Muzaki, and R. Indriati, "Implementasi Base64 dan Pepper pada Sistem Verifikasi Dokumen Berbasis QR Code," *J. Penelit. Teknol. Inf. dan Sains*, vol. 4, no. 2, pp. 193–206, 2026.