Penerapan Teknologi *Blockchain* untuk Keamanan Citra Digital

Silvia Putri Anggraeni*[1], Bagus Satrio Waluyo Poetro[2]
Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Islam Sultan Agung
*[1]e-mail: **silviaputri28@**std.unissula.ac.id
[2]e-mail: **bagusswp@**std.unissula.ac.id

ABSTRAK
Sistem keamanan digital berbasis blockchain dan AI dikembangkan untuk verifikasi sertifikat akademik secara otomatis, menggantikan proses manual yang rentan pemalsuan dan memakan waktu lama. Sistem ini memanfaatkan AI-OCR berbasis deep learning untuk mengekstrak teks dari sertifikat, lalu menggunakan algoritma SHA-256 untuk menghasilkan *hash* gambar berdasarkan struktur piksel serta *hash* teks berdasarkan isi dokumen, yang kemudian disimpan di *database* dan blockchain guna memastikan keasliannya. Dengan dataset lebih dari 200 sertifikat asli dalam format PNG dan JPG, sertifikat diproses melalui grayscale dan resize sebelum *hashing* dan penyimpanan. Pengujian menunjukkan bahwa *hash* gambar memiliki kesesuaian 100% dengan yang tersimpan di blockchain, sementara verifikasi teks OCR mencapai akurasi 100%, membuktikan bahwa sistem ini mampu memverifikasi sertifikat secara cepat, aman, dan akurat. Integrasi AI-OCR juga meningkatkan efisiensi dibandingkan metode manual, sehingga penelitian ini diharapkan menjadi solusi anti-pemalsuan yang dapat diterapkan di institusi akademik dan organisasi lain yang membutuhkan sistem verifikasi dokumen digital yang andal dan transparan.

***Kata kunci* :** *AI-OCR; Blockchain; Keamanan Digital; SHA-256*

ABSTRACT
A blockchain and AI-based digital security system was developed for automatic academic certificate verification, replacing the manual process that is prone to forgery and time-consuming. This system utilizes deep learning-based AI-OCR to extract text from certificates, then applies the SHA-256 algorithm to generate an image hash based on pixel structure and a text hash based on document content, which are then stored in a database and blockchain to ensure authenticity. With a dataset of over 200 original certificates in PNG and JPG formats, certificates are processed through grayscale conversion and resizing before hashing and storage. Testing results show that the image hash achieves 100% consistency with the blockchain-stored data, while OCR text verification reaches an accuracy of 98.6%, proving that this system can verify certificates quickly, securely, and accurately. The integration of AI-OCR also enhances efficiency compared to manual methods, making this research a promising anti-counterfeiting solution that can be applied in academic institutions and other organizations requiring a reliable and transparent digital document verification system.

***Keywords* :** *AI-OCR; Blockchain; Digital Security; SHA-256*

PENDAHULUAN

Kemajuan teknologi kecerdasan buatan (*artificial intelligence* atau AI) berkembang pesat dan memberikan dampak signifikan di berbagai bidang, termasuk keamanan citra digital. Dengan semakin banyaknya aplikasi dan platform berbasis AI yang digunakan dalam berbagai sektor, seperti pengenalan wajah, analisis citra medis, dan forensik digital, perlindungan terhadap manipulasi atau pemalsuan data citra menjadi tantangan yang semakin kompleks. Serangan terhadap sistem AI melalui gambar yang dimodifikasi dapat menyebabkan kegagalan sistem atau menghasilkan analisis yang tidak akurat. Oleh karena itu, diperlukan metode keamanan yang lebih kuat untuk menjaga integritas dan autentisitas data citra digital dalam sistem AI.

Blockchain hadir sebagai salah satu solusi untuk meningkatkan keamanan citra digital dalam sistem AI. Teknologi ini dikenal dengan sifatnya yang desentralisasi, transparan, dan memiliki tingkat integritas tinggi karena setiap blok data yang telah dicatat tidak dapat diubah. Dengan memanfaatkan algoritma *Optical Character Recognition* (*OCR*) berbasis *deep learning* dan algoritma *hash* SHA-256, blockchain dapat

digunakan untuk memastikan keaslian citra digital. AI-*OCR* berperan dalam meningkatkan akurasi pembacaan teks pada sertifikat atau citra digital. Model *deep learning* yang digunakan dalam AI-*OCR* adalah *EasyOCR*, yang memiliki fleksibilitas tinggi dalam mengenali karakter dalam citra digital. Sementara itu, SHA-256 berfungsi sebagai sidik digital unik yang memungkinkan pendeteksian terhadap setiap perubahan atau manipulasi citra digital.

Penelitian ini memiliki beberapa tujuan utama, yaitu: (1) membangun dan mengembangkan sistem yang mampu melindungi citra digital dari manipulasi atau pemalsuan menggunakan teknologi blockchain; (2) menerapkan algoritma SHA-256 untuk meningkatkan keamanan citra digital; serta (3) mengurangi risiko pemalsuan citra digital dengan sistem berbasis blockchain. Dengan adanya sistem ini, diharapkan dapat meningkatkan keamanan dan keabsahan sertifikat digital melalui penerapan teknologi SHA-256, AI-*OCR*, dan blockchain, sehingga pemalsuan dapat dicegah dan keaslian sertifikat tetap terjaga.

Untuk membatasi ruang lingkup penelitian, fokus utama diberikan pada penggunaan *private blockchain*. Selain itu, penelitian ini hanya menggunakan citra digital dalam bentuk gambar dan tidak mencakup semua jenis data visual. Adapun aspek keamanan yang dikaji hanya berfokus pada manipulasi atau pemalsuan data citra digital.

METODE PENELITIAN

Metode penelitian dalam studi ini mengembangkan sistem berbasis web yang menggunakan *Python* dengan *framework Flask* untuk *backend* serta *HTML*, *CSS*, dan *JavaScript* untuk *frontend*. Sistem ini berjalan pada *server* lokal dengan *XAMPP* dan dirancang untuk memverifikasi keaslian sertifikat digital menggunakan teknologi AI-*OCR*, *hashing* SHA-256, dan *blockchain* Ethereum dengan *Ganache* sebagai platform penyimpanan data terdesentralisasi. Studi ini mengimplementasikan kombinasi metode AI-*OCR*, *hashing* SHA-256, dan *blockchain* Ethereum. Dataset yang digunakan berupa sertifikat dalam format gambar yang mengalami *preprocessing*, ekstraksi teks menggunakan AI-*OCR*, dan *hashing* SHA-256 sebelum hasilnya disimpan dalam *database MySQL* serta diverifikasi melalui *blockchain* (*Ganache*). Model ini diimplementasikan dalam aplikasi berbasis *Flask* untuk mendeteksi keaslian sertifikat secara otomatis.

Tahapan penelitian meliputi perancangan alur kerja sistem dengan *flowchart* untuk proses input dan verifikasi sertifikat. Proses verifikasi dimulai dengan penginputan sertifikat yang kemudian diolah melalui teknik *preprocessing* seperti *grayscale*, *resize*, dan pengurangan *noise* agar dapat dikenali oleh AI-*OCR* (*EasyOCR*). Setelah itu, teks hasil ekstraksi AI-*OCR* dan citra sertifikat di-*hashing* menggunakan SHA-256. Hasil *hashing* dibandingkan dengan data yang telah tersimpan di *blockchain* dan *database*. Jika nilai *hash* cocok, sertifikat dianggap asli; jika tidak, sertifikat dikategorikan sebagai palsu.

Proses lebih lanjut mencakup tahapan pengumpulan dataset yang terdiri dari sertifikat asli dan sertifikat palsu (hasil manipulasi). Dataset ini mengalami *preprocessing* sebelum diproses oleh AI-*OCR* berbasis *deep learning*, yang menyoroti teks dalam sertifikat dengan kotak hijau sebagai indikator keberhasilan identifikasi. Setelah ekstraksi teks selesai, proses *hashing* dilakukan menggunakan SHA-256 untuk menghasilkan nilai *hash* unik dari teks AI-*OCR* maupun gambar sertifikat. Hasil *hash* ini kemudian disimpan di dalam *database MySQL* serta *blockchain* Ethereum melalui *smart contract* yang dikembangkan di *Remix IDE*. Penyimpanan *hash* dalam *blockchain* dilakukan dengan transaksi menggunakan dompet digital *MetaMask*, sementara akun *Ganache* digunakan sebagai tempat penyimpanan *hash* dari sertifikat dalam jaringan *blockchain*.

HASIL DAN PEMBAHASAN

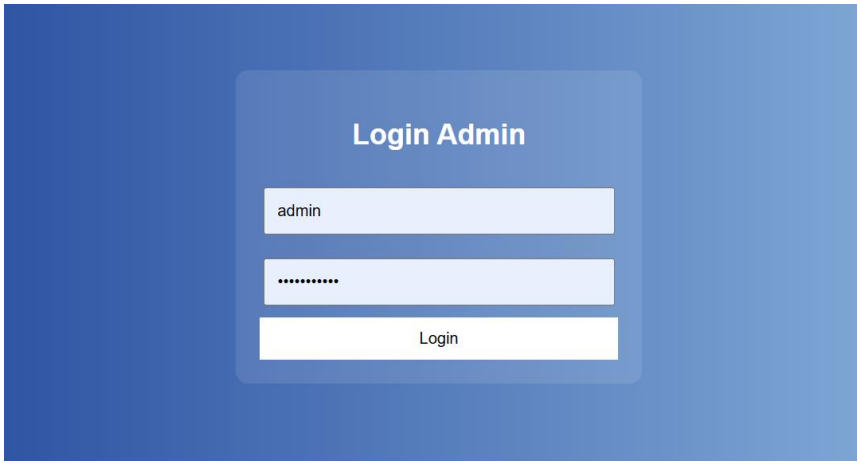
Sistem yang dikembangkan berupa *web* yang bertujuan untuk memverifikasi keaslian sertifikat digital menggunakan AI-*OCR*, SHA-256, dan *blockchain* Ethereum (*Ganache*). Sistem ini terdiri atas dua komponen utama, yaitu Halaman Admin dan Halaman Verifikasi. Halaman Admin berfungsi sebagai tempat untuk menginput dan menyimpan sertifikat ke dalam *database* serta *blockchain*. Sementara itu, Halaman Verifikasi digunakan untuk memeriksa keaslian sertifikat yang diunggah dengan membandingkan *hash* gambar dan *hash* teks hasil AI-*OCR* terhadap data yang tersimpan dalam *database* dan *blockchain*. Jika hasil perbandingan sesuai, sertifikat dinyatakan asli; sebaliknya, jika terdapat ketidaksesuaian, sertifikat dianggap telah dimanipulasi atau palsu.

Pengujian Unggah dan Penyimpanan Sertifikat



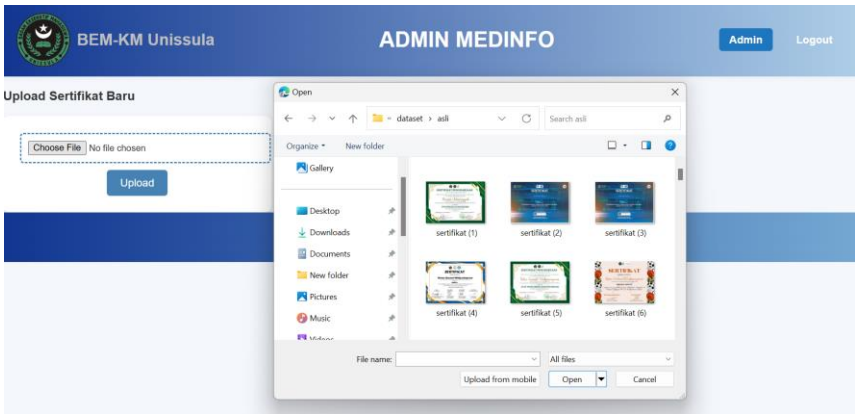
Gambar 1. Tampilan Landing Page

Gambar 1 menunjukkan tampilan *landing page*. Admin dapat mengklik tombol Admin di pojok kiri atas untuk memulai uji input data dan menyimpannya di database serta *blockchain*.



Gambar 2. Tampilan Login Admin

Gambar 2 merupakan tampilan halaman login bagi admin.



Gambar 3. Tampilan Admin untuk Input Sertifikat Digital

Gambar 3 menunjukkan tampilan halaman input bagi admin untuk mengunggah dan menyimpan sertifikat digital ke dalam database dan *blockchain*.



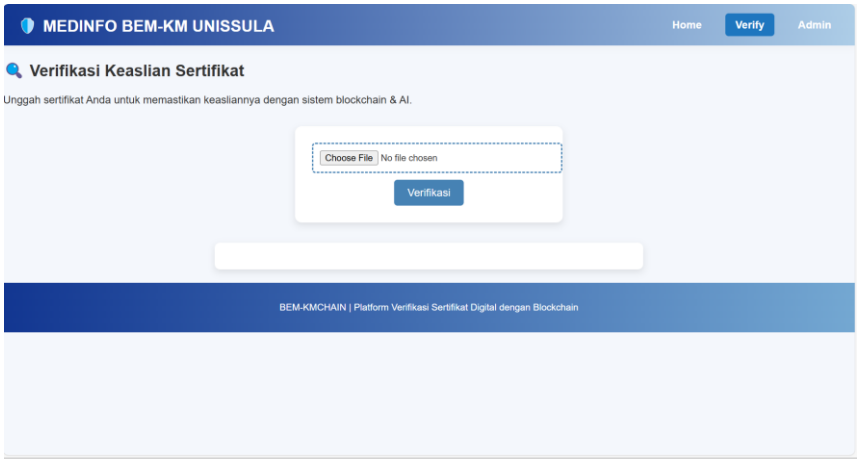
Gambar 4. Tampilan Logout pada Halaman Admin

Gambar 4 menunjukkan tampilan tombol Logout di pojok kiri atas halaman admin. Ketika tombol diklik, sistem akan mengarahkan kembali ke *landing page*.



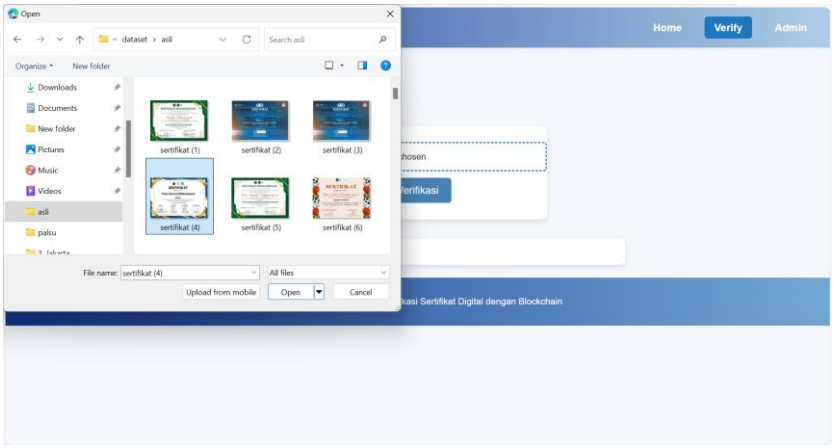
Gambar 5. Tampilan Landing Page

Gambar 5 kembali menampilkan *landing page*, di mana pengguna dapat mengklik tombol Verifikasi untuk beralih ke halaman verifikasi sertifikat digital.



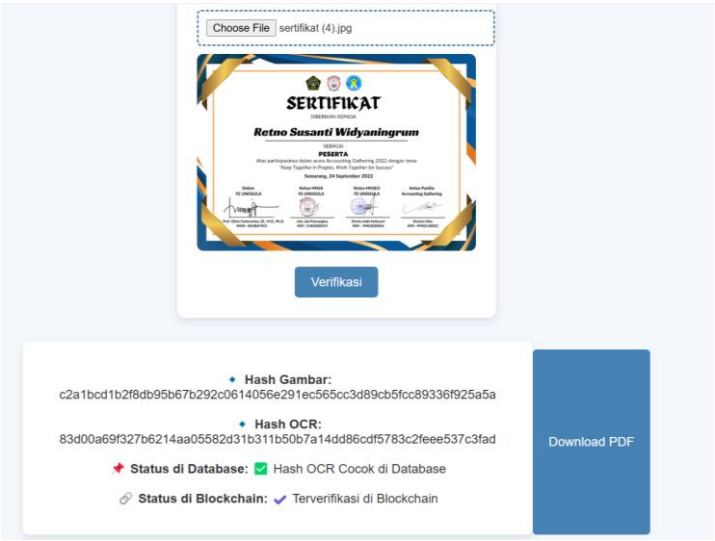
Gambar 6. Halaman Verifikasi Sertifikat Digital

Gambar 6 menunjukkan tampilan halaman untuk verifikasi keaslian sertifikat digital.



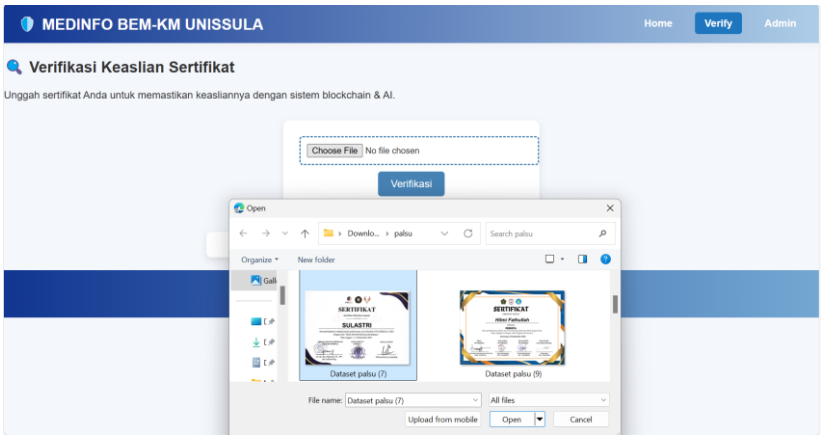
Gambar 7. Tampilan Pemilihan Dataset Asli untuk Verifikasi

Gambar 7 menunjukkan tampilan pemilihan dataset asli untuk menguji sertifikat digital yang akan diverifikasi. Setelah memilih dataset, pengguna dapat mengklik tombol Verifikasi.



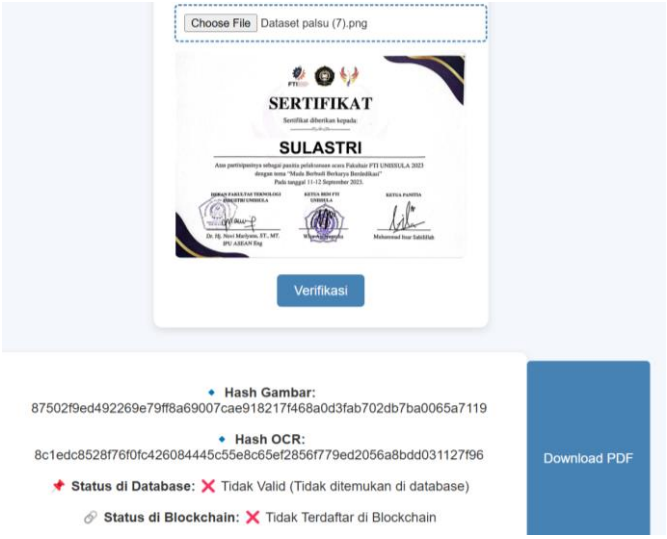
Gambar 8. Tampilan Hasil Uji Sertifikat Digital (Asli)

Gambar 8 menunjukkan hasil uji sertifikat digital yang diverifikasi sebagai asli, karena *hash* sertifikat terdaftar di *blockchain* dan database.



Gambar 9. Tampilan Pemilihan Dataset Palsu untuk Verifikasi

Gambar 9 menunjukkan tampilan pemilihan dataset palsu untuk menguji keaslian sertifikat digital.



Gambar 10. Tampilan Hasil Uji Sertifikat Digital (Palsu)

Gambar 10 menunjukkan hasil uji sertifikat digital yang diverifikasi sebagai palsu, karena *hash* tidak terdaftar di *blockchain* dan database.

Hasil Evaluasi Model

1. Interpretasi Hasil

Berdasarkan hasil pengujian, sistem yang dikembangkan berhasil melakukan deteksi sertifikat dengan tingkat akurasi yang cukup baik. *Hash* gambar dan *hash* hasil *OCR* dapat dibandingkan dengan database dan *blockchain* untuk menentukan keaslian sertifikat. Jika *hash* gambar cocok, maka sertifikat dianggap asli, sementara ketidaksesuaian menunjukkan kemungkinan sertifikat palsu. Adanya perbedaan pada *hash OCR*, meskipun *hash* gambar cocok, menunjukkan bahwa teks hasil ekstraksi dapat mengalami variasi. Hal ini kemungkinan disebabkan oleh kualitas cetakan atau faktor lainnya.

2. Faktor yang Mempengaruhi Hasil

Terdapat beberapa faktor yang mempengaruhi hasil deteksi, di antaranya kualitas gambar sertifikat, *preprocessing* gambar, dan kinerja model *OCR*. Kualitas gambar sertifikat berperan penting dalam akurasi deteksi, di mana gambar dengan resolusi rendah atau buram dapat menyebabkan hasil *OCR* kurang akurat, sehingga mempengaruhi proses verifikasi. Selain itu, *preprocessing* gambar, seperti teknik *grayscale* dan *resizing*, harus dilakukan secara konsisten untuk memastikan bahwa *hash* yang dihasilkan tetap stabil dan tidak berubah. Faktor lainnya adalah kinerja model *OCR*, yang meskipun telah mampu mengekstrak teks dengan baik, masih berpotensi mengalami kesalahan deteksi akibat variasi jenis *font*, posisi teks, atau keberadaan tanda tangan yang dapat mengganggu proses ekstraksi.

3. Kelebihan dan Kekurangan Sistem

Sistem yang dikembangkan memiliki kelebihan dan kekurangan dalam proses verifikasi sertifikat digital. Beberapa kelebihannya antara lain proses verifikasi yang lebih cepat karena hanya memerlukan pencocokan *hash*, serta kombinasi *hash* gambar dan *hash OCR* yang memberikan tingkat keamanan lebih tinggi. Selain itu, penggunaan *blockchain* sebagai penyimpanan permanen memastikan bahwa data tidak mudah dimanipulasi. Namun, sistem ini juga memiliki beberapa kekurangan, seperti ketergantungan pada kualitas gambar, di mana jika gambar memiliki resolusi rendah atau buram, hasil *OCR* dapat berbeda dan menyebabkan ketidaksesuaian pada *hash* teks. Selain itu, sistem belum sepenuhnya mampu mendeteksi ciri khas fisik sertifikat, seperti *watermark* atau tanda tangan, secara langsung.

4. Implikasi dan Potensi Pengembangan

Sistem ini memiliki potensi besar untuk diterapkan dalam berbagai institusi yang memerlukan verifikasi dokumen digital. Pengembangannya dapat dilakukan dengan meningkatkan akurasi *OCR* menggunakan model *deep learning* yang lebih canggih, sehingga dapat mengenali teks dengan lebih presisi. Selain itu, sistem

dapat diperluas dengan menambahkan fitur deteksi elemen visual, seperti cap dan tanda tangan, untuk meningkatkan validitas verifikasi. Integrasi dengan *blockchain* publik juga dapat menjadi langkah strategis guna meningkatkan transparansi dan keamanan lebih lanjut dalam proses penyimpanan serta verifikasi data sertifikat digital.

SIMPULAN

Hasil penelitian ini menunjukkan bahwa sistem yang dikembangkan mampu memverifikasi keaslian sertifikat digital secara otomatis dengan menggabungkan teknologi *OCR AI*, hashing *SHA-256*, dan *blockchain* Ethereum (Ganache). Dataset yang digunakan terdiri dari dua sistem utama, yaitu halaman admin untuk pengelolaan sertifikat dan halaman verifikasi untuk menguji keaslian sertifikat. Proses verifikasi diawali dengan ekstraksi teks menggunakan *OCR AI*, yang kemudian di-*hash* menggunakan *SHA-256* untuk menghasilkan nilai *hash* unik sebagai "sidik jari" sertifikat digital. Hasil *hash* dari teks dan gambar sertifikat kemudian disimpan dalam database *MySQL* dan *blockchain*. Saat proses verifikasi, sertifikat yang diuji akan menghasilkan *hash* baru yang kemudian dibandingkan dengan *hash* yang telah tersimpan. Jika nilai *hash* cocok, sertifikat dinyatakan asli; sebaliknya, jika tidak cocok, sertifikat dikategorikan sebagai palsu.

Untuk pengembangan lebih lanjut, penelitian ini menyarankan dua aspek utama. Pertama, diperlukan integrasi *blockchain* yang lebih kuat, karena saat ini sistem hanya menggunakan *private blockchain* atau jaringan lokal. Kedua, perlu dilakukan pengembangan lebih lanjut terhadap *OCR AI* dengan metode tambahan untuk meningkatkan akurasi dalam membaca dan mengekstraksi teks. Dengan pengoptimalan ini, sistem diharapkan lebih siap digunakan dalam verifikasi sertifikat digital di dunia nyata.

DAFTAR PUSTAKA

Alfina, & Syafrinal. (2022). Model Sistem Verifikasi Dokumen Ijazah Digital Berbasis Teknologi Blockchain. *SMARTICS Journal*, *8*(2), 59–65. https://doi.org/10.21067/10.21067/smartics.v8i2.7718

Argani, A., & Taraka, W. (n.d.). *Pemanfaatan Teknologi Blockchain Untuk Mengoptimalkan Keamanan Sertifikat Pada Perguruan Tinggi*.

Arwani, A., & Priyadi, U. (2024). Eksplorasi Peran Teknologi Blockchain dalam Meningkatkan Transparansi dan Akuntabilitas dalam Keuangan Islam: Tinjauan Sistematis. *JURNAL EKONOMI BISNIS DAN MANAJEMEN*, *2*(2), 23–37. https://doi.org/10.59024/jise.v2i2.653

Goodfellow, Bengio, & Courville. (2016). Book Review: Deep Learning. *Healthcare Informatics Research*, *22*(4), 351. https://doi.org/10.4258/hir.2016.22.4.351

Gunawan, A. , & Nurfita, R. D. (2018). *IMPLEMENTASI DEEP LEARNING BERBASIS TENSORFLOW UNTUK PENGENALAN SIDIK JARI PUBLIKASI ILMIAH*.

Iqbal, T., Ahmad, L., Studi Manajemen Informatika, P., Indonesia Banda Aceh Kota, S., Banda Aceh, K., & Aceh, P. (2024). Menerapkan Blockchain untuk Meningkatkan Transparansi dan Keamanan Rantai Pasokan: Studi Kasus di Industri Kelapa Sawit. *Jurnal Manajemen Dan Teknologi (JMT)*, *1*(1). https://doi.org/10.35870/jmt.vxix.775

Joshua P Nugraha. (n.d.). *PENERAPAN BLOCKCHAIN UNTUK PENCEGAHAN SERTIPIKAT TANAH GANDA DI KEMENTERIAN AGRARIA DAN TATA RUANGBADAN PERTANAHAN NASIONAL*.

Lecun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436–444. https://doi.org/10.1038/nature14539ï

Oknora Firza, S., & Ilmu Komputer, F. (2024). *Teknologi Blockchain dalam Keamanan Sertifikat Menggunakan Smart Contracts dan Distributed Ledger pada Platfrom Edutech* (Vol. 5, Issue 2).

Syahronny, M. R., & Dewayanto, T. (2024). PENERAPAN TEKNOLOGI ARTIFICIAL INTELLIGENCE DAN BLOCKCHAIN DALAM MENDETEKSI FRAUD PADA PROSES AUDIT: SYSTEMATIC LITERATURE REVIEW. *DIPONEGORO JOURNAL OF ACCOUNTING*, *13*(3), 1–14. http://ejournal-s1.undip.ac.id/index.php/accounting