E ISSN 2715 - 1212
Neraca : Jurnal Akuntansi Terapan Vol 6 , No. 1, Oktober 2024, pp. 22-26

Peran Artificial Intelligence dan Blockchain dalam Meningkatkan Cybersecurity pada Proses Akuntansi

Iin Andrayanti [1], Heksawan Rahmadi [2*], Sri Susanti Widyasari [3], Ambarwati [4]

[1234] Institut Ilmu Sosial dan Manajemen Stiami, Jakarta, Indonesia
[1] inez.stiami90@gmail.com ; [2] rahmadiheksawan@gmail.com; [3] srisusantiwidyasari64@gmail.com;
[4]ambarsidikstiami26@gmail.com
*** Corresponding author : Heksawan Rahmadi**

ARTICLE INFO

Keywords :
Artificial Intelligence;
Blockchain;
Cybersecurity;
Akuntansi;

ABSTRACT

Accounting has undergone significant transformation with the adoption of cutting-edge technologies, including Artificial Intelligence (AI), Cybersecurity, and Blockchain. In the contemporary technological landscape, the integration of artificial intelligence (AI), cybersecurity measures, and blockchain technology has emerged as an important development in accounting. The emergence of AI has revolutionised traditional accounting practices by enhancing data processing capabilities and enabling real-time analysis. Through machine learning algorithms, AI can identify patterns and anomalies in financial data, thereby improving accuracy and efficiency while minimising human error. These technological advancements not only streamline operations but also help in predictive analysis, thereby enabling accountants to make informed decisions based on comprehensive data interpretation. In integration with AI, Blockchain guarantees data accuracy and real-time access, allowing auditors to use verified information effectively. The combination of AI and IoT (Internet of Things) and Blockchain accelerates audit procedures, including substantive tests, and enables automated testing of all data, increasing audit efficiency and effectiveness (Kurniawan et al., 2020). In this context, this research will discuss the role and implications of these technologies in improving efficiency, transparency, and security in accounting practices. Organisational culture and industry-specific differences play an important role in shaping technology adoption strategies. The study provides recommendations for corporate firms in Jakarta, emphasising the importance of data security, change management, and skills development. In addition, this study also suggests future research to explore the long-term impact of technology adoption and new technologies in accounting practices. This research contributes to the growing discourse on technology-based transformation in accounting and offers actionable insights for multinational companies operating in a dynamic business environment.

1. PENDAHULUAN

Keberadaan Artificial Intelligence (AI) telah berkembang dengan sangat pesat di era revolusi industry 4.0 dengan memberikan beberapa manfaat dan kegunaan yang besar bagi transformasi bisnis untuk bergerak lebih cepat dan otomatis, dimana memiliki dampak signifikan pada beberapa bidang non-IT seperti bidang audit. Pelaksanaan audit telah mengalami perubahan dengan bergeser ke teknik audit 4.0 yang otomatis dengan pertumbuhan perusahaan sebagai klien yang telah beradaptasi dengan teknologi hingga proses penyajian laporan keuangan yang terintegrasi dengan sistem, termasuk dengan penggunaan AI dan IoT (Internet of Things) yang membantu penyaluran informasi secara merata ke seluruh department bisnis. Selain itu, penerapan AI dengan dukungan blockchain dapat meningkatkan

kinerja deteksi intrusi, dan deteksi kinerja mencapai akurasi hingga 97,02%, dengan tingkat deteksi sebesar 97%. Dengan kehadiran Blockchain di bidang akuntansi dan audit, meningkatkan transparansi atas proyeksi informasi keuangan dari kegiatan operasional dan membantu menjamin keakuratan data melalui data privacy and security yang terbebas dari manipulasi informasi. Alat analisis data tingkat lanjut digunakan untuk menganalisis data keuangan dan mengidentifikasi tren, pola, dan anomali. Hal ini dapat membantu akuntan membuat keputusan dengan informasi yang lebih baik dan memberikan prakiraan keuangan yang lebih akurat (Cleary et al., 2022).

Dalam integrasi dengan AI, Blockchain menjamin keakuratan data dan akses real-time, memungkinkan auditor menggunakan informasi terverifikasi secara efektif. Gabungan AIoT dan Blockchain mempercepat prosedur audit, termasuk substantive test, dan memungkinkan pengujian otomatis dari seluruh data, meningkatkan efisiensi dan efektivitas audit (Kurniawan et al., 2020). Pada Studi Kong et al. (2024) mengembangkan sistem pemantauan AIoT untuk manajemen sistem keamanan dengan operasi otonom, pencegahan kerusakan sensor, lingkungan komunikasi optimal, prediksi berbasis machine learning, dan keamanan data yang kuat. Integrasi AI dengan berbasis blockchain memungkinkan sistem mengelola data efisien, memprediksi potensi kerusakan, dan beradaptasi otomatis selama kejadian berisiko, memastikan manajemen System Development Life Cycle (SDLC) perusahaan lebih cepat, aman, dan efisien apabila mengimplementasikan sistem yang dikembangkan secara mandiri. Kedua teknologi tersebut berperan krusial dalam keamanan dengan algoritma kecerdasan buatan untuk mendeteksi dan mencegah ancaman lebih efektif.

Kehadiran AI-Bchain berperan krusial dalam keamanan dengan memanfaatkan algoritma kecerdasan buatan untuk mendeteksi dan mencegah ancaman lebih efektif. Algoritma kecerdasan buatan mampu menganalisis data besar dari perangkat IoT, mengidentifikasi pola, dan mendeteksi anomali atau potensi pelanggaran keamanan secara real-time. Keamanan dan akurasi data yang disediakan oleh AIoT membantu auditor mencegah pengaruh cyber-threats yang dapat mengganggu kinerja proses audit. Dengan memanfaatkan keamanan, desentralisasi, dan consensus meningkatkan keamanan data perusahaan melawan ancaman siber (Kurniawan et al., 2020).

Terlepas dari meningkatnya antusiasme terhadap transformasi berbasis teknologi di bidang akuntansi, terdapat kebutuhan untuk memahami secara komprehensif bagaimana Perusahaan-perusahaan multinasional beradaptasi dan memanfaatkan AI dan Blockchain untuk meningkatkan cybersecurity dalam praktik akuntansi mereka. Interaksi yang rumit antara teknologi ini dan nuansa prosedur akuntansi dalam lingkungan bisnis yang unik memerlukan penyelidikan mendalam.

2. METODE

Penelitian ini bertujuan untuk mengeksplorasi peran Artificial Intelligence (AI) dan Blockchain dalam meningkatkan cybersecurity dalam proses akuntansi. Metode penelitian menggunakan pendekatan kualitatif dengan metode systematic literature review, yang melibatkan analisis dan sintesa dari berbagai sumber penelitian yang relevan.

a. Pengumpulan Data

1) Studi Literatur Sistematis: Metode ini melibatkan pengumpulan data dari berbagai sumber penelitian yang relevan. Sumber-sumber ini dapat berupa jurnal ilmiah, artikel, laporan penelitian, dan buku-buku yang terkait dengan topik AI, Blockchain, dan cybersecurity dalam akuntansi.
2) Survei dan Wawancara: Untuk mendapatkan data yang lebih spesifik dan kontekstual, survei dan wawancara dapat dilakukan dengan auditor, akuntan, dan perusahaan yang telah menggunakan AI dan Blockchain dalam proses akuntansi mereka.

Neraca : Jurnal Akuntansi Terapan Vol 6 , No. 1, Oktober 2024, pp. 22-26

b. Analisis Data

1) Kualitas Data: Data yang dikumpulkan harus memenuhi kriteria kualitas yang tinggi, seperti validitas, reliabilitas, dan akurasi. Analisis ini dilakukan untuk memastikan bahwa data yang digunakan dapat diandalkan dan relevan dengan tujuan penelitian.

2) Klasifikasi dan Pengelompokan: Data yang dikumpulkan kemudian diklasifikasikan dan dikelompokkan berdasarkan kriteria yang telah ditentukan. Misalnya, data dapat diklasifikasikan berdasarkan jenis pajak, jenis teknologi yang digunakan, dan dampaknya terhadap cybersecurity.

c. Pembahasan dan Kesimpulan

Berdasarkan hasil analisis, pembahasan dilakukan untuk menjelaskan secara detail peran AI dan Blockchain dalam meningkatkan cybersecurity dalam proses akuntansi. Pembahasan ini melibatkan diskusi tentang kelebihan dan kekurangan teknologi ini, serta contoh-contoh implementasi yang sukses. Kesimpulan penelitian ini kemudian disampaikan untuk memberikan gambaran yang jelas tentang hasil penelitian dan implikasinya dalam praktik akuntansi.

3. HASIL DAN PEMBAHASAN

Penggunaan AI dalam Deteksi Intrusi

Artificial Intelligence (AI) memiliki potensi besar untuk meningkatkan deteksi dan respon terhadap ancaman siber. Dengan kemampuan untuk menganalisis data dalam jumlah besar dan mendeteksi pola yang mencurigakan, AI dapat membantu organisasi merespon ancaman dengan lebih cepat dan efektif. Selain mendeteksi dan merespons ancaman, AI juga berperan penting dalam memperkuat strategi pertahanan melalui peningkatan sistem autentikasi dan protokol enkripsi. Misalnya, AI dapat memberikan sistem otentikasi biometrik yang lebih kompleks, mengintegrasikan pengenalan wajah, sidik jari, dan pola suara untuk memastikan hanya pengguna yang terverifikasi yang dapat mengakses sistem-sistem kritikal. Demikian pula, AI dapat bekerja dengan algoritma enkripsi untuk memastikan bahwa data penting disandikan dengan cara yang lebih dinamis dan sulit ditembus, menawarkan lapisan tambahan keamanan yang vital terhadap serangan cyber.

Penggunaan sistem deteksi intrusi adalah salah satu contoh aplikasi AI dalam otomatisasi respons keamanan yang ditingkatkan dengan algoritma pembelajaran mesin. Sistem ini dirancang untuk belajar dari berbagai kejadian keamanan yang terjadi sebelumnya dan terus menerus memperbaharui model deteksinya supaya dapat mengenali tipe serangan baru yang belum pernah terlihat sebelumnya. Ketika sistem mendeteksi aktivitas mencurigakan yang menunjukkan potensi serangan, AI dapat langsung memicu protokol respons otomatis, seperti memblokir alamat IP yang berasal dari serangan atau mengisolasi sistem yang terinfeksi untuk mencegah penyebaran lebih lanjut.

Kecepatan dalam merespons ancaman sangatlah kritikal, mengingat serangan siber dapat menyebar dengan sangat cepat dan merusak banyak aset dalam waktu singkat. AI membantu dalam mengurangi waktu yang dibutuhkan untuk mengidentifikasi dan merespons serangan, yang dikenal dengan istilah “time to respond”. Menggunakan AI, organisasi dapat mengurangi window of opportunity bagi penyerang untuk melancarkan serangan mereka. Ini berarti bahwa bahkan serangan yang paling canggih sekalipun dapat ditangani dengan lebih efektif, mengurangi risiko kerugian data, waktu operasional, dan dampak finansial yang mungkin ditimbulkan.

Penggunaan Blockchain dalam Keamanan Data

Blockchain menggunakan konsep desentralisasi, di mana data disimpan dalam blok-blok yang terhubung secara kriptografis di seluruh jaringan. Setiap blok memiliki hash unik yang terhubung dengan blok sebelumnya, membuatnya sulit untuk dimanipulasi. Sistem ini menjadikan blockchain sangat aman terhadap serangan cyber seperti perubahan data atau serangan Denial-of-Service (DoS). Data yang disimpan dalam blockchain tidak dapat diubah atau dihapus oleh pihak yang tidak bertanggung jawab.

Blockchain memastikan keakuratan dan transparansi data melalui teknologi distribusi ledger yang tidak dapat diubah dan Blockchain dapat mengurangi risiko manipulasi data dengan memastikan bahwa setiap transaksi yang dilakukan dapat direkam dan dilihat oleh semua pihak yang berkepentingan (Kurniawan et al., 2020).

Di Indonesia, beberapa proyek blockchain telah dilakukan, seperti verifikasi dan validasi sertifikat pendidikan, penyimpanan data medis, dan sistem pembayaran, Namun, implementasi teknologi blockchain di Indonesia masih menghadapi beberapa tantangan, seperti regulasi yang belum jelas, infrastruktur yang masih terbatas, dan kurangnya pemahaman tentang teknologi blockchain.

Integrasi AI dan Blockchain dalam Proses Akuntansi

Integrasi AI dan Blockchain dapat meningkatkan cybersecurity dalam proses akuntansi dengan memastikan keakuratan dan transparansi data. AI dapat membantu dalam deteksi intrusi dan analisis data serta otomatisasi tugas-tugas. AI juga dapat dengan cepat menemukan pola dan tren dalam data keuangan, memungkinkan analisis yang lebih akurat dan efisien dibandingkan dengan teknik manual. Selain itu, AI juga dapat membantu dalam penghematan waktu dan meningkatkan kemampuan analisis, sehingga memungkinkan pelaku bisnis dan investor untuk membuat keputusan yang lebih tepat.

Blockchain dapat memastikan keakuratan dan transparansi data dalam proses akuntansi dengan memungkinkan data diverifikasi dan disetujui secara bersama. Integrasi ini dapat meningkatkan efisiensi dan efektivitas audit, serta mengurangi risiko kesalahan dalam proses akuntansi, sehingga dapat meningkatkan efisiensi, transparansi, dan keamanan dalam proses akuntansi. Blockchain juga dapat membantu dalam manajemen rantai nilai, audit, dan representasi mata uang kripto dalam laporan keuangan. Selain itu, blockchain memungkinkan pembuatan skema dengan validasi yang kuat, serta menciptakan peringatan terhadap kehilangan, kesalahan, atau manipulasi data.

Sehingga Integrasi AI dan Blockchain dalam akuntansi dapat meningkatkan efisiensi, transparansi, dan keamanan dalam proses akuntansi. AI dapat membantu dalam analisis data dan otomatisasi tugas-tugas, sementara Blockchain meningkatkan transparansi dan kepercayaan dalam praktik akuntansi dengan memungkinkan data diverifikasi dan disetujui secara bersama sehingga Cybersecurity dalam proses akuntansi akan memastikan keamanan data perusahaan melawan ancaman siber.

4. KESIMPULAN

Dalam keseluruhan, penggunaan AI dalam deteksi intrusi telah menunjukkan potensi besar dalam meningkatkan keamanan jaringan dan sistem informasi. Dengan kemampuan analisis yang canggih dan adaptif, AI dapat membantu mengidentifikasi dan mencegah serangan cyber yang semakin kompleks dan beragam. Sedangkan penggunaan blockchain dalam keamanan data telah menunjukkan potensi besar dalam menjaga integritas dan keamanan data. Dengan menggunakan enkripsi yang kuat dan

Neraca : Jurnal Akuntansi Terapan Vol 6 , No. 1, Oktober 2024, pp. 22-26

sistem terdesentralisasi, blockchain dapat memastikan bahwa data yang disimpan adalah aman dan tidak dapat diubah oleh pihak yang tidak bertanggung jawab.

Hal ini menunjukkan bahwa integrasi AI dan Blockchain dapat meningkatkan cybersecurity dalam proses akuntansi dengan memastikan keakuratan dan transparansi data. AI dapat membantu dalam deteksi intrusi dan analisis data, sedangkan Blockchain dapat memastikan keakuratan dan transparansi data. Integrasi ini dapat meningkatkan efisiensi dan efektivitas audit, serta mengurangi risiko kesalahan dalam proses akuntansi. Peran budaya organisasi muncul sebagai faktor penting dalam keberhasilan adopsi teknologi. Perusahaan dengan budaya inovasi dan manajemen perubahan yang proaktif akan lebih siap untuk menavigasi kompleksitas dalam mengintegrasikan teknologi baru ke dalam praktik akuntansi mereka.

DAFTAR PUSTAKA

BKN Yogyakarta. (2021). Silo Mentality: Batas Transparan Yang Menghambat Organisasi. *Kantor Regional I BKN Jogjakarta*. Retrieved February 18, 2024, from https://yogyakarta.bkn.go.id/artikel/0/2024/01/silo-mentality-batas-transparan-yang-menghambat-organisasi

Boul, P., & Bouaissi, K. (2023, February 23). Revised ISA 315 and IT risks: how to reduce the additional workload it creates on the alternative industry? EY Luxembourg. https://www.ey.com/en_lu/assurance/revised-isa-315-and-it-risks–how-to- reduce-the-additional-workl

Kong, S., Yoo, C., Park, J., Park, J., & Lee, S. (2024). AIOT monitoring technology for optimal fill dam installation and operation. Applied Sciences, 14(3), 1024. https://doi.org/10.3390/app14031024

Kurniawan, A. A., Santoso, H. A., Soeleman, M. A., & Anani, A. Z. (Eds.). (2020). *Intrusion Detection System as Audit in IoT Infrastructure using Ensemble Learning and SMOTE Method*. https://doi.org/10.1109/ICSITech46713.2019.8987524

PwC. (2022). *Satu dari empat perusahaan telah mengalami pelanggaran data secara global yang merugikan mereka US$1 – 20 juta atau lebih dalam tiga tahun terakhir* [Press release]. Retrieved February 18, 2024, from http://tinyurl.com/Pelanggaran-Data-Global-PwC

Raphael, J., & Steele, A. (2023). Audit transformation and opportunities in cognitive, blockchain, and talent. In *Deloitte*. Retrieved February 17, 2024, from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/audit/us-audit-transformation-and-opportunities-in-cognitive-blockchain-and-talent.pdf

Strengthening collaboration for cyber resilience: the key to a secure and resilient organization. (2023). ISACA. http://tinyurl.com/ISACA-Security-Data