

DESAIN DAN PENGEMBANGAN LUMINA: EKOSISTEM AUDIT DIGITAL ETIS BERBASIS AI DAN BLOCKCHAIN

Gianne Angely Puspa Pilatus^{1*}, Silvester Tirta Yoga², Edo Karisma³, Prastyadi Wibawa Rahayu⁴

^{1,2,3,4}Universitas Dhyana Pura

Email corresponding: gianneangelyv@undhirabali.ac.id¹

ABSTRAK Perkembangan keuangan digital meningkatkan volume transaksi dan pemanfaatan kecerdasan buatan dalam audit, tetapi diikuti tingginya insiden kebocoran data, risiko manipulasi laporan, dan keterbatasan transparansi algoritma yang melemahkan kepercayaan publik. Penelitian ini bertujuan merancang LUMINA (Learning Unified Machine Intelligence for Neutral Auditing) sebagai ekosistem audit digital etis yang mengintegrasikan kecerdasan buatan, blockchain, dan tata kelola data untuk memperkuat infrastruktur audit lembaga keuangan. Metode yang digunakan adalah penelitian pengembangan dengan pendekatan deskriptif kualitatif, meliputi pemetaan kebutuhan dan peran pemangku kepentingan utama (regulator, lembaga keuangan, asosiasi profesi, perguruan tinggi, dan komunitas pengguna) serta perancangan arsitektur sistem dan fitur inti. Penelitian ini menghasilkan rancangan prototipe konseptual LUMINA yang terdiri atas Integrity Vault berbasis blockchain untuk ketertelusuran transaksi, modul pemantauan risiko berbantu AI dengan pendekatan pembelajaran terfederasi guna menjaga privasi, dan Insight Board sebagai dasbor kolaboratif lintas sektor. Temuan utama menunjukkan bahwa integrasi ketiga komponen tersebut berpotensi meningkatkan integritas audit, memperkuat kepatuhan terhadap regulasi keamanan siber, dan membuka ruang kolaborasi berkelanjutan antara industri, regulator, dan akademisi dalam pengembangan audit digital. Dengan demikian, LUMINA berpotensi menjadi infrastruktur audit digital etis yang mendukung kepercayaan dan kolaborasi multisektor di ekosistem keuangan digital Indonesia.

Kata kunci: audit digital; kecerdasan buatan etis; blockchain; kepercayaan digital; kolaborasi multisektor

1. Pendahuluan

Perkembangan layanan keuangan digital meningkatkan kompleksitas pengelolaan transaksi sekaligus memperluas pemanfaatan teknologi analitik untuk pemantauan risiko dan audit. Dalam konteks nasional, ancaman siber menjadi isu yang konsisten muncul dan dipetakan oleh Badan Siber dan Sandi Negara (BSSN) melalui dokumen “Lanskap Keamanan Siber Indonesia” yang menyoroti insiden dan tren ancaman, termasuk penelusuran terhadap dugaan insiden dengan jenis dominan berupa kebocoran data (data breach). Pada 2024, BSSN juga melaporkan deteksi 241 dugaan insiden kebocoran data, yang menunjukkan bahwa isu privasi dan keamanan informasi masih relevan serta berdampak luas.

Selain isu kebocoran data, penggunaan AI untuk menilai transaksi atau perilaku pengguna dapat menimbulkan persoalan transparansi dan bias, karena algoritma sering bersifat “kotak hitam” sehingga sulit dijelaskan bahkan kepada pihak profesional. Kondisi ini dapat melemahkan akuntabilitas audit ketika auditor perlu menjelaskan alasan sistem memberi peringatan atau rekomendasi tertentu. Di sisi lain, privasi data pengguna menjadi taruhan ketika data dikumpulkan terpusat tanpa batas yang jelas, sehingga meningkatkan risiko kebocoran dan penyalahgunaan.

Dari sisi regulasi, Otoritas Jasa Keuangan menerbitkan Surat Edaran OJK Nomor 29/SEOJK.03/2022 tentang ketahanan dan keamanan siber bagi bank umum, yang

menekankan penerapan manajemen risiko keamanan siber dan mekanisme ketahanan (resilience) dalam proses identifikasi, perlindungan, deteksi, penanggulangan, serta pemulihan insiden. Pada ranah inovasi teknologi sektor keuangan, OJK juga menerbitkan POJK 3 Tahun 2024 tentang Penyelenggaraan Inovasi Teknologi Sektor Keuangan (ITSK) sebagai payung pengaturan dan pengawasan inovasi.

Berangkat dari kondisi tersebut, penelitian ini bertujuan merancang LUMINA (Learning Unified Machine Intelligence for Neutral Auditing) sebagai ekosistem audit digital etis yang mengintegrasikan blockchain, AI yang dapat dijelaskan, pendekatan pembelajaran terfederasi untuk menjaga privasi, serta dasbor kolaboratif lintas sektor. Penelitian menempatkan etika (privasi dan keadilan algoritma), keamanan (integritas transaksi), dan transparansi (explainability) sebagai prinsip desain agar sistem audit digital tidak hanya meningkatkan efisiensi, tetapi juga memperkuat kepercayaan publik.

2. Metode

Penelitian ini menggunakan penelitian pengembangan dengan pendekatan deskriptif kualitatif. Pengumpulan dan analisis data dilakukan melalui:

- (1) analisis ancaman keamanan siber dan dampaknya pada masyarakat Indonesia,
- (2) kajian literatur tentang blockchain, federated learning, dan ethical AI, serta
- (3) pemetaan kebutuhan teknis dan sosial dari pemangku kepentingan utama (regulator, lembaga keuangan, asosiasi profesi, perguruan tinggi, dan komunitas pengguna).

Analisis kualitatif kemudian digunakan untuk menyusun rancangan arsitektur sistem yang aman, transparan, dan menghormati privasi, termasuk strategi monitoring bias algoritma secara berkelanjutan.

Pertimbangan etika dalam rancangan ditekankan pada dua aspek: perlindungan privasi data pengguna dan keadilan dalam algoritma. Pelibatan komunitas pengguna dalam proses desain (co-design) diposisikan sebagai mekanisme untuk mencegah rancangan yang eksklusif serta untuk memperkuat legitimasi sosial terhadap sistem audit digital yang diusulkan.

3. Hasil dan Pembahasan

3.1 Rancangan prototipe konseptual LUMINA

Hasil penelitian berupa rancangan prototipe konseptual LUMINA yang terdiri atas Integrity Vault berbasis blockchain untuk ketertelusuran transaksi, modul pemantauan risiko berbantu AI dengan pendekatan pembelajaran terfederasi guna menjaga privasi, dan Insight Board sebagai dasbor kolaboratif lintas sektor. Secara desain, kombinasi ini diarahkan untuk meningkatkan integritas audit, memperkuat kepatuhan pada kebutuhan keamanan siber, serta membuka ruang kolaborasi berkelanjutan antara industri, regulator, dan akademisi.

Berdasarkan pemetaan komponen pada materi presentasi, LUMINA dijabarkan menjadi lima komponen teknologi terintegrasi: Integrity Vault (Blockchain), Trust Profile (Interpretable AI), Silent Watch (Federated Learning), Insight Board (Explainable Dashboard), dan Secure Exchange (Encrypted Cross-Border). Integrity Vault mencatat transaksi menggunakan hash cryptography sehingga manipulasi dapat dideteksi, Trust Profile memberi skor sekaligus alasan/faktor yang memengaruhi penilaian, Silent Watch melatih model tanpa memusatkan data sensitif, Insight Board menyajikan analisis dalam tampilan

visual yang mudah dipahami, dan Secure Exchange memperkuat transaksi lintas negara dengan enkripsi end-to-end.

Tabel 1. Komponen LUMINA dan fungsi utama

Komponen	Fungsi utama	Output audit yang dituju
Integrity Vault (Blockchain)	Pencatatan permanen berbasis hash untuk mendeteksi perubahan/manipulasi.	Audit trail kuat dan verifikasi integritas.
Trust Profile (Interpretable AI)	Skoring risiko disertai faktor penyusun agar dapat dijelaskan.	Akuntabilitas penilaian risiko.
Silent Watch (Federated Learning)	Pembelajaran pola tanpa memusatkan data; data tetap lokal.	Privasi terjaga dan pengurangan risiko konsentrasi data.
Insight Board (Explainable Dashboard)	Visualisasi temuan dan alasan rekomendasi.	Transparansi dan komunikasi lintas pihak.
Secure Exchange (Encrypted Cross-Border)	Enkripsi end-to-end transaksi internasional.	Kerahasiaan dan keamanan pertukaran data lintas batas.

3.2 Pemetaan masalah dan relevansi regulasi

Permasalahan keamanan siber dan kebocoran data menjadi dasar urgensi penguatan audit digital, karena BSSN menyoroti insiden kebocoran data sebagai salah satu jenis insiden dominan yang ditelusuri pada lanskap 2022 serta melaporkan deteksi 241 dugaan insiden kebocoran data pada 2024. Kondisi tersebut menuntut rancangan audit yang tidak hanya mendeteksi anomali, namun juga mengurangi risiko kebocoran melalui prinsip minimisasi pemusatan data dan penguatan pencatatan integritas.

Dalam sektor perbankan, SEOJK 29/SEOJK.03/2022 menekankan penerapan manajemen risiko keamanan siber serta proses ketahanan siber mencakup identifikasi, pelindungan, deteksi, penanggulangan, dan pemulihan insiden. Rancangan LUMINA mengarahkan komponen Integrity Vault sebagai penguatan integritas catatan dan akuntabilitas, Silent Watch sebagai pendekatan privasi dengan pembelajaran terfederasi, serta Insight Board sebagai sarana komunikasi temuan audit yang lebih transparan.

Tabel 2. Risiko kunci dan mitigasi desain pada LUMINA

Risiko	Indikator/implikasi	Mitigasi pada LUMINA
Kebocoran data	BSSN mendeteksi 241 dugaan insiden kebocoran data (2024).	Silent Watch (federated learning) + Secure Exchange (enkripsi end-to-end).

Manipulasi transaksi/laporan	Mengganggu integritas audit dan validasi bukti.	Integrity Vault (blockchain, hash cryptography, pencatatan permanen).
AI “kotak hitam”	Auditor sulit menjelaskan rekomendasi sistem.	Trust Profile (interpretable AI) + Insight Board (explainable dashboard).
Bias algoritma	Potensi ketidakadilan pada kelompok pengguna tertentu.	Monitoring bias berkelanjutan + co-design agar inklusif.

3.3 Tahapan implementasi

Implementasi LUMINA dirancang bertahap untuk memastikan kesiapan organisasi, literasi, dan kontrol etika berjalan seiring dengan pengembangan teknis. Tahap 1 (1–2 bulan) berfokus pada literasi dan awareness tentang bias AI, risiko privasi, dan teknologi etis; Tahap 2 (2–3 bulan) pada desain dan validasi melalui co-design; Tahap 3 (3–4 bulan) pada implementasi teknologi dengan pengujian ketat untuk deteksi bias; Tahap 4 pada monitoring dan feedback berkelanjutan; dan Tahap 5 pada scaling serta knowledge transfer

Tabel 3. Tahapan implementasi LUMINA

Tahap	Aktivitas inti	Durasi
1	Sosialisasi AI bias, privacy risks, dan teknologi etis.	1–2 bulan.
2	Co-design dan validasi kebutuhan.	2–3 bulan.
3	Deploy komponen dan testing ketat untuk deteksi bias	3–4 bulan.
4	Monitoring bias dan mekanisme feedback publik.	Berkelanjutan.
5	Scaling dan transfer pengetahuan melalui dokumentasi terbuka.	Berkelanjutan.

3.4 Keterbatasan dan rencana penelitian lanjutan

Keterbatasan penelitian ini adalah LUMINA masih pada tahap rancangan konseptual dan belum dilakukan implementasi penuh pada lembaga keuangan. Pengembangan berikutnya mencakup pembuatan prototipe perangkat lunak, uji coba dengan 2–3 lembaga keuangan, pengukuran efektivitas dalam mendeteksi kecurangan dan meningkatkan kepercayaan publik, serta penyusunan panduan adopsi untuk lembaga lain.

4. Simpulan

Penelitian ini merancang LUMINA sebagai ekosistem audit digital etis yang mengintegrasikan blockchain, AI yang dapat dijelaskan, dan pembelajaran terfederasi untuk menjaga privasi serta mendukung kolaborasi lintas sektor. Rancangan tersebut memetakan lima komponen terintegrasi (Integrity Vault, Trust Profile, Silent Watch, Insight Board, Secure Exchange) dan tahapan implementasi bertahap yang mencakup literasi, co-design, pengujian bias, serta monitoring berkelanjutan. LUMINA masih berada pada tahap konseptual sehingga diperlukan prototyping dan uji institusional untuk menilai efektivitas dan aspek fairness algoritmik pada konteks nyata.

5. Daftar Rujukan

- Badan Siber dan Sandi Negara. (2023). Lanskap keamanan siber Indonesia tahun 2022. Badan Siber dan Sandi Negara Republik Indonesia.
- Badan Siber dan Sandi Negara. (2024). Lanskap keamanan siber Indonesia tahun 2023 dan 2024. Badan Siber dan Sandi Negara Republik Indonesia.
- Duha, T. (2025). Manajemen keuangan digital dalam era industri 5.0. *Jurnal Riset Manajemen dan Strategi Bisnis*, 3(1), 1–15.
- Dzulhasni, S. (2024). Implikasi etika pada penggunaan artificial intelligence dalam akuntansi manajemen. *Jurnal Akuntansi Manajemen Bisnis dan Teknologi*, 4(1), 136–143.
- Handarini, D. (2024). Akuntansi keuangan dalam era digital: Peran teknologi blockchain dan kecerdasan buatan dalam transparansi dan akuntabilitas. *Wahana Akuntansi*, 6(1), 1–15.
- Inas, R. P. A. L. (2025). Dampak dan etika penerapan artificial intelligence pada bidang akuntansi. *Jurnal Akuntansi*, 7(1), 1–15.
- Indrianingrum, I., dkk. (2025). Efektivitas penerapan blockchain dalam mengurangi risiko fraud pada audit keuangan. *Jurnal Costing*, 8(3), 200–215.
- Irmadhani, A. S. N. (2025). Peran teknologi blockchain dalam pelaporan keuangan dan audit. *Jurnal Akuntansi Universitas Diponegoro*, 14(1), 100–120.
- Jurnal PiLAR. (2023). Literasi artificial intelligence di sektor keuangan. *Jurnal PiLAR*, 14(2), 140–155.
- Otoritas Jasa Keuangan. (2022). Surat Edaran Otoritas Jasa Keuangan Nomor 29/SEOJK.03/2022 tentang ketahanan dan keamanan siber bagi bank umum. Otoritas Jasa Keuangan Republik Indonesia.
<https://www.ojk.go.id/id/regulasi/Documents/Pages/Ketahanan-dan-Keamanan-Siber-Bagi-Bank-Umum/SEOJK%2029%20SEOJK.03%202022.pdf>
- Otoritas Jasa Keuangan. (2023). Laporan tahunan Otoritas Jasa Keuangan 2023. Otoritas Jasa Keuangan Republik Indonesia.
- Otoritas Jasa Keuangan. (2024). Peraturan Otoritas Jasa Keuangan Nomor 3 Tahun 2024 tentang penyelenggaraan inovasi teknologi sektor keuangan. Otoritas Jasa Keuangan Republik Indonesia.
<https://ojk.go.id/id/regulasi/Pages/POJK-3-2024-Penyelenggaraan-Inovasi-Teknologi-Sektor-Keuangan.aspx>
- Pratiwi, L. L. (2022). Implementasi blockchain pada akuntansi dan audit di Indonesia. *Jurnal Fair Value*, 4(2), 2185–2196.
- Pryangan, W. (2025). Masa depan keuangan digital berbasis blockchain di Indonesia. *Jurnal Paradoks*, 8(1), 30–45.
- Putri, A. A., dkk. (2025). Ransomware di sektor keuangan: Studi kasus Bank Syariah Indonesia. *Jurnal Ilmu Informasi dan Komputer*, 5(1), 10–25.
- Rahman, A. (2023). Pengaruh artificial intelligence pada profesi akuntan. Dalam *Prosiding Konferensi Nasional Ilmu Administrasi* (hlm. 1–10).
- Setyawan, R. (2024). Dilema etis pengambilan keputusan berbasis artificial intelligence di sektor bisnis. *Dinamika Bisnis Digital*, 3(1), 67–84.