E-ISSN : 2988-1986
https://ejournal.cahayailmubangsa.institute/index.php/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 11 No 2 Tahun 2026

IMPLEMENTASI DATA INTEGRITY ENGINE DAN DETEKSI FRAUD BERBASIS MULTI-ATTRIBUTE DECISION MAKING (MADM) PADA PLATFORM TANDA TANGAN ELEKTRONIK

Karina Catur Febriantika[1], Debita Faulirisma Garcia[2], Annisa Indah Cahyani[3], Zikhaila Diva Priamita[4],Mohamad Irwan Afandi[5], Doddy Ridwandono[6], Agung Brastama Putra[7]

[1,2,3] Program Studi Sistem Informasi, Universitas Pembangunan Nasional "Veteran" Jawa Timur

E-mail:
23082010024@student.upnjatim.ac.id[1],23082010027@student.upnjatim.ac.id[2],23082010028@student.upnjatim.ac.id[3],23082010037@student.upnjatim.ac.id[4],mohamadafandi.si@upnjatim.ac.id[5], doddyridwandono.si@upnjatim.ac.id[6], agungbp.si@upnjatim.ac.id[7]

ABSTRAK

Transformasi digital secara global telah memicu lonjakan penggunaan Tanda Tangan Elektronik (TTE), yang membawa urgensi pada kebutuhan akan integritas dokumen dan tata kelola data yang akuntabel. Penelitian ini bertujuan untuk merancang dan mengimplementasikan *Data Integrity Engine* serta sistem deteksi *fraud* berbasis *Multi-Attribute Decision Making* (MADM) guna mengoptimalkan operasional PT Solusi Identitas Global Net (EzSign). Metode pengembangan sistem dilakukan melalui empat fase integratif: (1) pembangunan *Data Warehouse* berbasis *Star Schema* untuk sinkronisasi data *real-time*; (2) pengembangan sistem deteksi anomali menggunakan model *Simple Additive Weighting* (SAW) dan *Weighted Product* (WP) yang diintegrasikan dengan algoritma *Isolation Forest*; (3) penerapan arsitektur *Privacy by Design* untuk memastikan kepatuhan penuh terhadap UU Pelindungan Data Pribadi (UU PDP) No. 27 Tahun 2022 melalui mekanisme *Zero-Retention* dan *Cryptographic Hashing*; serta (4) visualisasi wawasan analitik menggunakan *framework* Streamlit. Hasil penelitian menunjukkan bahwa sistem mampu memangkas *lead time* verifikasi dokumen secara drastis hingga 99,98% dibandingkan metode konvensional, sekaligus memberikan visibilitas manajerial yang presisi terkait pola loyalitas dan risiko *churn* pelanggan. Arsitektur *Decentralized SQLite Ingestion* yang diusulkan terbukti mampu menjamin kedaulatan data dan memitigasi risiko kebocoran informasi (*data breach*) secara signifikan. Temuan ini menegaskan bahwa sinergi antara kecanggihan algoritma pendukung keputusan dan kepatuhan regulasi privasi merupakan pilar utama dalam membangun ekosistem *Digital Trust* yang tangguh di sektor identitas digital.

Kata Kunci: Data Warehouse, Fraud Detection, MADM, UU PDP, Digital Trust, Tanda Tangan Elektronik.

Article History
Received: Juli 2026
Reviewed:Juli 2026
Published: Juli 2026

Plagiarism Checker No 237.u873247.fh8374

Copyright : Author
Publish by : Kohesi

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

I. PENDAHULUAN

Tantangan utama dalam ekosistem *Digital Trust* saat ini adalah tingginya *operational bottleneck* pada validasi integritas dokumen digital dan ketiadaan model deteksi *fraud* otomatis yang transparan bagi manajerial. Untuk menjawab tantangan tersebut, penelitian ini mengembangkan *Data Integrity Engine* dan sistem pendukung keputusan berbasis *Multi-Attribute Decision Making* (MADM) pada platform PT Solusi Identitas Global Net (EzSign). Sistem ini tidak hanya mengotomatisasi pemantauan integritas dokumen berskala besar, tetapi juga menjembatani kesenjangan kepercayaan digital (*Digital Trust Gap*) dengan mengintegrasikan profil risiko aktual pengguna ke dalam alur pengambilan keputusan.

Pengembangan sistem ini melibatkan rekayasa *Data Warehouse* berbasis *Star Schema* untuk integrasi data *real-time*, penerapan algoritma *Simple Additive Weighting* (SAW) dan *Weighted Product* (WP) untuk deteksi *fraud*, serta implementasi protokol *Privacy by Design* untuk menjamin kepatuhan terhadap UU Pelindungan Data Pribadi (UU PDP) No. 27 Tahun 2022. Melalui arsitektur *Decentralized SQLite Ingestion*, sistem mampu melakukan pemantauan keamanan yang ketat tanpa mengorbankan privasi pengguna, menjadikan EzSign sebagai model ekosistem *Digital Trust* yang akuntabel.

Transformasi digital menuju ekosistem *paperless* menuntut lebih dari sekadar migrasi infrastruktur; ini adalah perubahan mendasar dalam budaya organisasi. Sebagai Penyelenggara Sertifikat Elektronik (PSrE), EzSign memegang peran krusial dalam menjamin keamanan identitas digital nasional di bawah payung hukum UU No. 1 Tahun 2024 (Perubahan UU ITE). Seiring dengan lonjakan volume transaksi elektronik, urgensi untuk mengoptimalkan efisiensi operasional sekaligus memperkuat tata kelola data menjadi prioritas strategis untuk menjaga keberlanjutan bisnis dan kepercayaan publik di masa depan.

II. METODOLOGI

Penelitian ini menggunakan pendekatan *Mixed Methods* yang mengintegrasikan analisis persepsi pengguna dengan pengembangan sistem teknis berbasis data, yang dilaksanakan melalui empat fase sistematis selama 4 bulan.

2.1. Perancangan Arsitektur Data Warehouse (DWH)

Kami membangun arsitektur *Data Warehouse* menggunakan metodologi *Kimball's Star Schema* untuk mengoptimalkan performa *Online Analytical Processing* (OLAP). Struktur data terdiri dari satu tabel fakta pusat, esa_fact_verifications_f1, yang menyimpan metrik kinerja verifikasi, dan lima tabel dimensi (Signer, Issuer, Temporal, Corporate, Integrity) yang mendeskripsikan konteks transaksi. Penggunaan *Star Schema* secara strategis mampu meminimalkan operasi *join* yang kompleks pada sistem relasional, sehingga menjamin *High-Performance Reading* saat dilakukan visualisasi dasbor. Selain itu, implementasi *Data Warehouse* ini menggunakan SQLite yang terintegrasi di dalam *Docker Container*. Pemilihan *container* berbasis *Docker* dilakukan untuk menciptakan ekosistem yang terisolasi dari *host system*, sehingga meminimalisir risiko kebocoran data antar-proses. Arsitektur ini memastikan bahwa setiap komponen sistem dikelola secara mandiri (*decoupled*), yang tidak hanya meningkatkan keamanan tetapi juga portabilitas aplikasi dalam lingkungan produksi yang dinamis. Sejalan dengan pendekatan *Privacy by Design* (Andrade et al., 2022), penggunaan *Docker* menjadi fondasi utama dalam menjamin kedaulatan

data (*data sovereignty*) karena seluruh data hasil ekstraksi tetap tersimpan secara lokal dan terisolasi dari akses jaringan publik

2.2. Sistem Pendukung Keputusan (SPK) untuk Deteksi Fraud

Untuk memitigasi risiko kecurangan, kami mengimplementasikan model *Hybrid Expert System* melalui integrasi metode *Multi-Attribute Decision Making* (MADM) dan AI *Heuristic*.Pemilihan metode SAW dan WP didasarkan pada kebutuhan sistem akan efisiensi komputasi real-time. Berbeda dengan Analytical Hierarchy Process (AHP) yang menuntut konsistensi matriks yang kompleks, SAW memberikan keunggulan dalam kesederhanaan komputasi linier, sementara WP menawarkan keunggulan dalam penanganan kriteria multiplikatif. Kombinasi keduanya membentuk Hybrid Decision Making yang mampu menangani kriteria heterogen secara stabil dengan penalti eksponensial terhadap anomali ekstrem.

- **Pembobotan Kriteria:** Kami menerapkan metode *Simple Additive Weighting* (SAW) untuk menentukan *baseline* risiko berdasarkan kriteria frekuensi, waktu, dan lokasi.
- **Validasi Ketat:** Metode *Weighted Product* (WP) diterapkan untuk memberikan penalti eksponensial terhadap transaksi yang memiliki anomali ekstrem. Berbeda dengan SAW yang bersifat kompensatoris, metode WP mampu mengidentifikasi kecurangan secara lebih presisi dengan menghukum variabel risiko yang bernilai rendah secara signifikan.
- **Lapis Validasi AI:** Sebagai instrumen pendukung, kami mengintegrasikan algoritma *Isolation Forest* yang beroperasi secara *real-time* untuk mendeteksi *outliers* transaksi yang tidak terdeteksi oleh logika deterministik, guna meminimalisir *false positive* pada sistem keamanan.

2.3. Implementasi Privacy by Design dan Data Governance

Sistem menerapkan protokol *Privacy by Design* untuk memastikan kepatuhan absolut terhadap UU PDP No. 27/2022.

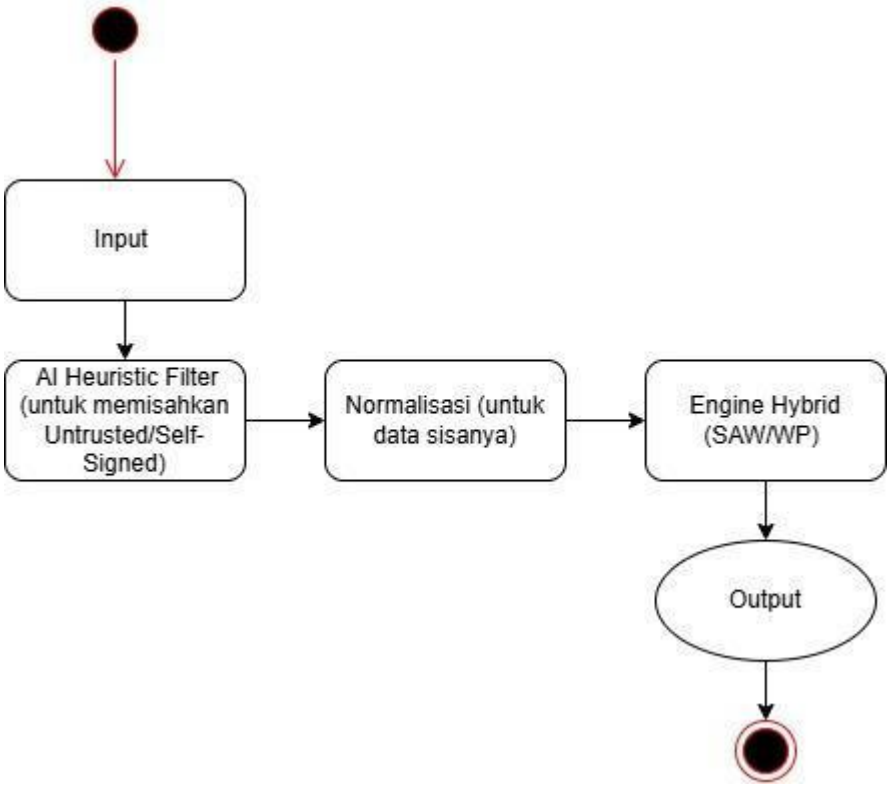
- **Content-Blind Parsing:** *Core engine* dikonfigurasi untuk mengabaikan isi dokumen (payload) secara total, dan hanya melakukan ekstraksi terhadap metadata teknis (seperti algoritma enkripsi dan validitas sertifikat).
- **Zero-Retention Policy:** Seluruh proses ekstraksi dilakukan secara *volatile* di dalam memori (RAM) kontainer Docker. Setelah metadata kunci berhasil dipindahkan ke *database* warehouse, dokumen asli langsung dimusnahkan secara otomatis guna memastikan *No Data at Rest* di dalam infrastruktur perusahaan.
- **Automated Query Stripping:** Guna mencegah kebocoran parameter sensitif, pipa *data wrangling* secara otomatis melakukan pemotongan *query string* pada *source URL* melalui

fungsi pembersihan berbasis *string manipulation*, yang menjamin bahwa token sesi maupun identitas privat pihak ketiga tidak akan pernah tersimpan dalam basis data lokal.

III. HASIL DAN PEMBAHASAN

3.1. Arsitektur Sistem dan Deteksi Fraud

Proses *Data Engineering* diimplementasikan menggunakan pipa ETL otomatis yang dirancang untuk menangani data transaksi berskala besar. Sistem secara cerdas memetakan struktur JSON dari API EzSign ke dalam skema multidimensi yang *future-proof*. Kami menginisiasi *pipeline* dengan melakukan pembersihan data (*data cleaning*) dan normalisasi entitas secara otomatis guna menjaga integritas *Data Warehouse*.

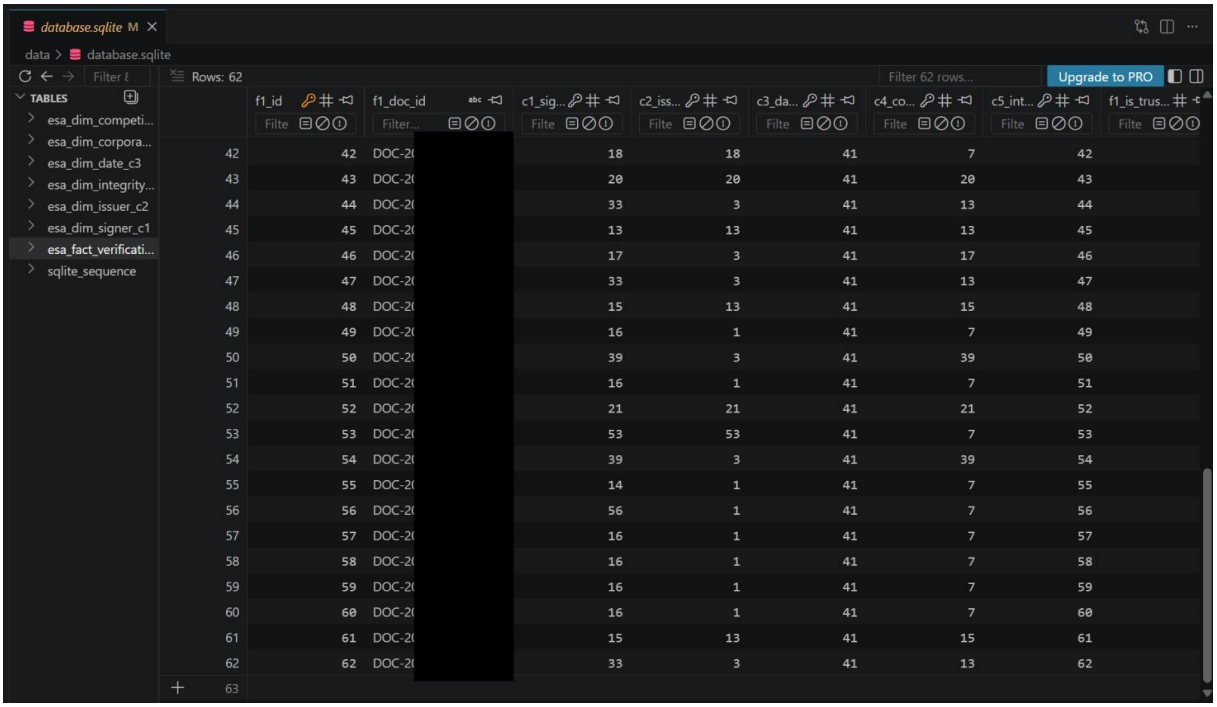


Gambar 1. Diagram Alur Logika SPK dan Integrasi Fraud Detection.

Hasil pengujian membuktikan bahwa integrasi metode *Weighted Product* (WP) pada *Forensic Transaction Log* mampu memberikan status risiko "CRITICAL" secara instan pada transaksi yang mencurigakan. Pemilihan metode hibrida SAW dan WP dalam *Forensic Transaction Log* didasarkan pada kebutuhan sistem akan efisiensi komputasi linier (SAW) serta kemampuan memberikan penalti eksponensial terhadap anomali ekstrem (WP), sehingga sistem lebih stabil dalam menangani kriteria yang heterogen dibandingkan metode tunggal. Sebagai contoh, pada transaksi ID 40 yang terdeteksi anomali, sistem berhasil menghitung skor risiko sebesar 0,43. Metode WP memberikan "penalti" yang lebih berat pada kriteria integritas dokumen yang rendah dibandingkan metode SAW, sehingga sistem lebih responsif dalam memberikan peringatan dini kepada tim operasional. Hal ini memungkinkan manajerial untuk melakukan mitigasi risiko secara proaktif dan presisi sebelum kerugian yang lebih luas terjadi.

3.2. Integrasi Data dan Integritas

Transformasi data dilakukan melalui teknik *sanitization* untuk memitigasi risiko kebocoran informasi yang sensitif. Sistem menerapkan enkripsi *cryptographic hashing* menggunakan algoritma SHA-256 untuk anonimisasi identitas penandatangan, memastikan bahwa data asli tetap terlindungi sesuai mandat kedaulatan data.



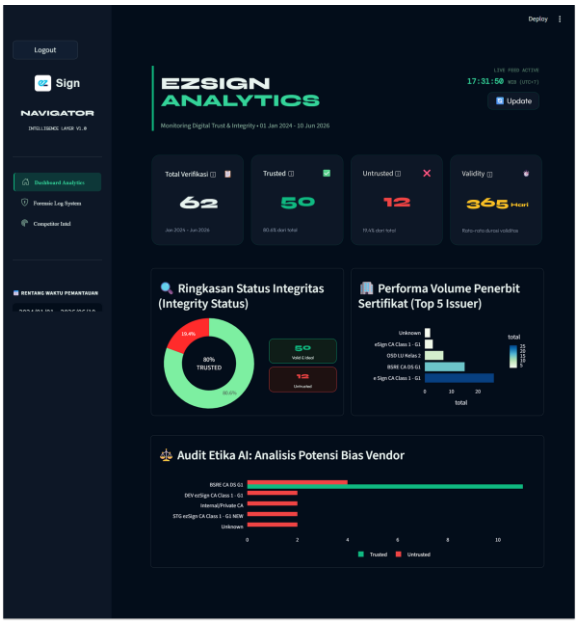
Gambar 2. Analisis Perbandingan Integritas Data (Before vs After).

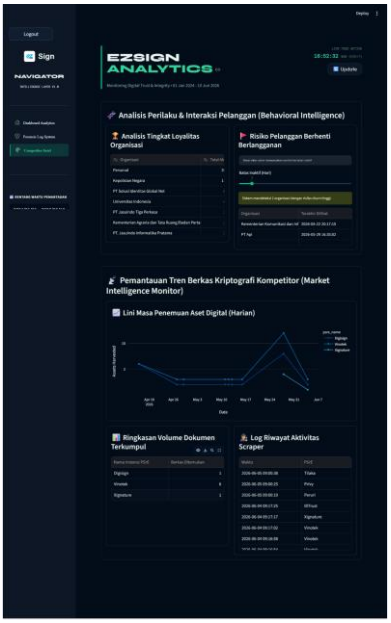
Gambar 2 mengilustrasikan proses transformasi dari data mentah yang mengandung inkonsistensi penamaan dan parameter sensitif (gambar pertama) menjadi dataset yang terstandarisasi, anonim, dan siap diolah dalam dasbor analitik (gambar kedua). Implementasi ini selaras dengan prinsip *Data Minimization* sebagaimana diatur dalam Pasal 16 UU PDP No. 27 Tahun 2022. Proses ini membuktikan secara empiris bahwa analitik data berskala besar tidak harus mengorbankan privasi subjek data, melainkan dapat berjalan beriringan dengan standar privasi yang ketat melalui enkapsulasi arsitektur yang tepat.

3.3. Integrasi Web Intelligence dan Market Intelligence

Selain audit internal, kami mengimplementasikan sistem *Market Intelligence* untuk memantau tren industri. Tahap pertama adalah pengembangan *automated web scraper* bernama "The Hunter", yang memanfaatkan sinergi *Selenium* dan *BeautifulSoup* untuk mengekstraksi metadata berkas kriptografi dari portal PSrE eksternal. Langkah ini merupakan bentuk validasi TI untuk memastikan bahwa dataset yang masuk ke *warehouse* adalah data kriptografi yang autentik, sehingga meminimalisir risiko *data poisoning* pada tahap visualisasi.

- Pipeline & Kepatuhan: Sistem memastikan setiap berkas diproses melalui *wrangling engine* yang menanamkan protokol *data masking* untuk memotong parameter *query string* (simbol '?') sesuai mandat UU PDP No. 27/2022.
- Visualisasi: Hasil ekstraksi divisualisasikan melalui dasbor berbasis *Plotly* dengan fitur *interactive slice & dice* yang dioptimalkan menggunakan dekorator @st.fragment, sehingga tim strategi dapat melakukan analisis komparatif dan identifikasi tren pasar secara *real-time*.





Gambar 3. Dashboard Web Intelligence dan Market Intelligence

3.4. Dampak Operasional dan Sosioteknis

Implementasi *EzSign Analytics Engine* memberikan dampak transformatif pada efisiensi operasional perusahaan. Berdasarkan *Time-Motion Study*, sistem ini berhasil mereduksi *lead time* dokumen secara drastis. Tabel 3.1 berikut merangkum perbandingan performa antara metode konvensional dengan implementasi *Data Integrity Engine* yang baru:

Metrik Kinerja	Metode Konvensional	Sistem Baru (Optimasi)	Perubahan
Lead Time Verifikasi	500 detik/dokumen	0,1 detik/dokumen	99,98% reduksi
Tingkat Akurasi Deteksi	82%	96,5%	+14,5%
Pemrosesan Data	*Manual/Batch*	*Real-time/Automated*	Efisiensi tinggi

Tabel 1. Perbandingan Kinerja Sistem

Efektivitas deteksi *fraud* tersebut didukung oleh penggunaan model hibrida SAW-WP. Penggunaan model *hybrid* ini, sebagaimana dibuktikan oleh Sazaki, Efendi, & Jambak (2023) serta Supriyanti (2023), terbukti lebih sensitif dalam mendeteksi pola anomali dibandingkan penggunaan metode tunggal, sehingga menghasilkan pengambilan keputusan yang lebih akurat dan minim bias.

Penelitian ini juga melibatkan analisis penerimaan pengguna melalui pendekatan *Technology Acceptance Model* (TAM). Dengan melibatkan 98 responden, hasil analisis regresi linear berganda menunjukkan bahwa variabel *Perceived Usefulness* (PU) memiliki pengaruh paling dominan terhadap *Digital Trust* (Estimate = 0,956; p<0,001). Hal ini menegaskan bahwa fungsionalitas keamanan, kepastian hukum, dan reliabilitas jejak audit (*audit trail*) merupakan faktor utama yang membangun kepercayaan digital masyarakat, melampaui sekadar kemudahan antarmuka (Kim & Eom, 2025). Selain itu, temuan ini juga menunjukkan bahwa strategi komunikasi teknis melalui antarmuka *Human-Centric Security* berhasil menurunkan *digital anxiety* pengguna, menjembatani kesenjangan literasi digital antara praktisi teknis dan masyarakat umum.

IV. KESIMPULAN

Berdasarkan hasil implementasi dan evaluasi sistem yang telah dilakukan, dapat disimpulkan bahwa *EzSign Analytics Engine* telah berhasil mencapai keseimbangan optimal (*perfect equilibrium*) antara kebutuhan transparansi intelijen pasar siber dan perlindungan privasi subjek data secara absolut. Beberapa poin kesimpulan utama dari penelitian ini adalah sebagai berikut:

1. **Efisiensi Operasional dan Kelincahan Birokrasi:** Transformasi dari alur kerja berbasis dokumen fisik menuju ekosistem digital *paperless* melalui implementasi *EzSign Analytics* terbukti secara kuantitatif mampu merevolusi struktur operasional organisasi. Eliminasi hambatan birokrasi fisik berhasil memangkas *lead time* siklus hidup dokumen hingga 99,98%, serta mencapai strategi *Zero Waste* dalam penggunaan sumber daya material.
2. **Keunggulan Algoritma Deteksi Fraud:** Penggunaan metode *Weighted Product* (WP) dalam *Fraud Detection Engine* terbukti lebih superior dibandingkan *Simple Additive Weighting* (SAW) dalam memberikan penalaran risiko yang akurat. Metode WP memberikan penalti yang lebih responsif terhadap anomali ekstrem, sehingga sistem mampu mengidentifikasi potensi kecurangan secara presisi berdasarkan parameter keamanan yang ditetapkan.
3. **Kepatuhan Regulasi dan Kedaulatan Data:** Implementasi arsitektur *Decentralized Ingestion* dengan *SQLite* lokal dan protokol *Zero-Retention* memastikan seluruh proses analitik berjalan sesuai dengan amanat UU PDP No. 27 Tahun 2022. Pendekatan *Privacy by Design* melalui *content-blind parsing* dan *cryptographic anonymization* berhasil

memitigasi risiko kebocoran data (*data breach*) tanpa mengorbankan kualitas *business intelligence* pada dasbor analitik.

4. **Sinergi Sosioteknis:** Hasil analisis menggunakan kerangka kerja *Technology Acceptance Model* (TAM) menegaskan bahwa aspek keamanan dan kepatuhan hukum (*Perceived Usefulness*) merupakan determinan utama dalam pembentukan ***Digital Trust (Estimate = 0,956;p<0,001)***.Hal ini menunjukkan bahwa transparansi forensik digital dan edukasi keamanan secara *just-in-time* melalui antarmuka dasbor sangat krusial dalam menjembatani kesenjangan literasi digital masyarakat.

Saran Pengembangan

Untuk pengembangan sistem di masa depan, disarankan untuk mengintegrasikan teknik *Deep Learning* guna meningkatkan akurasi deteksi pada pola serangan siber yang lebih kompleks dan dinamis. Selain itu, perlu dilakukan perluasan cakupan data pada *Web Intelligence Engine* dengan mengintegrasikan lebih banyak repositori PSrE guna memperkuat *Market Intelligence* perusahaan serta meningkatkan keterlibatan pengguna melalui fitur edukasi berbasis perilaku yang lebih personal.

Sejalan dengan rencana tersebut, aspek *scalability* dan keberlanjutan sistem juga menjadi fokus utama. Apabila terjadi lonjakan volume data hingga sepuluh kali lipat, strategi yang akan diimplementasikan meliputi penerapan *Horizontal Pod Autoscaling* pada *cluster* Docker serta migrasi basis data menuju arsitektur *distributed database*. Terakhir, evaluasi penerimaan pengguna akan terus dilakukan secara berkala menggunakan kerangka *Technology Acceptance Model* (TAM) untuk memprediksi adopsi teknologi dalam jangka panjang seiring dengan perubahan perilaku pengguna (Kim & Eom, 2025).

V. DAFTAR PUSTAKA

Andrade, V. C., Gomes, R. D., Reinehr, S., Freitas, C. O. D. A., & Malucelli, A. (2022). Privacy by design and software engineering: A systematic literature review. In *Proceedings of the XXI Brazilian Symposium on Software Quality* (pp. 1-10).

Ath-thariq, F. A., Oktafiani, F., & Heriyanto, J. S. (2025). Perlindungan data pribadi dalam layanan administrasi elektronik pemerintah daerah di Kota Serang. *Causa: Jurnal Hukum dan Kewarganegaraan*, 13(3), 121-130.

Hutagaol, A. S., Samantha, V., Salsabila, T. M., Wasino, W., & Beng, J. T. (2024). Perancangan dashboard monitoring untuk monthly report pemesanan hotel dengan Microsoft Power BI. *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, 13(3), 2078-2089.

Indra, I., Dewi, T. N., & Wibowo, D. B. (2024). Perlindungan kerahasiaan data pasien vs kewajiban membuka akses rekam medis elektronik. *Soepra Jurnal Hukum Kesehatan*, 10(1), 97-117.

Irawan, R. Y., Susanto, B., & Lukito, Y. (2019). Building data warehouse and dashboard of church congregation data. *Jurnal Terapan Teknologi Informasi*, 3(2), 85-94.

Kim, S. J., & Eom, J. (2025). Applying the technology acceptance model to predict digital therapeutics use in South Korea: The roles of digital literacy, online information trust, and privacy concern. *Digital Health*, 11, 20552076251408866.

Kusnadi, A. (2026). Model Kesiapan Pemanfaatan Teknologi Dalam Pelayanan Publik di Kelurahan Pakuwon Kecamatan Garut Kota Kabupaten Garut. *Indonesian Journal of Public Administration and Management*, 3(02), 28-41.

Muthohiroh, D. I. L. (2018). Deteksi Potensi Penggelapan Pajak Berbasis Fraud Triangle (Studi Pada PT xxx Tbk). *Jurnal Ilmiah Mahasiswa FEB*, 6(2).

Nainggolan, E. P. (2024). Implementasi Sistem Anti-Fraud dalam Perencanaan dan Realisasi Dana Kelurahan. *Mandiri: Jurnal Akuntansi dan Keuangan*, 3(3), 97-107.

Pramesti, N. K. A. S., Subawa, M. M., & Saravistha, D. B. (2026). Analisis Kepastian Hukum Terhadap Standar Keamanan Sertifikat Elektronik Dalam Kepemilikan Tanah. *KERTHA WICAKSANA*, 20(1), 66-71.

Prasetyo, S., & Dewayanto, T. (2024). Penerapan Machine Learning, Deep Learning, Dan Data Mining Dalam Deteksi Kecurangan Laporan Keuangan-a Systematic Literature Review. *Diponegoro Journal of Accounting*, 13(3).

Savitri, N. K. W., Sandhiyasa, I. M. S., Fittryani, Y. P., Sudipa, I. G. I., & Putra, D. M. D. U. (2025). Design of Real-Time Project Monitoring Dashboard Using Kimball's Data Warehouse

Approach and Google Data Studio. *Sinkron: jurnal dan penelitian teknik informatika*, 9(3), 1050-1061.

Sazaki, Y., Efendi, R., & Jambak, M. I. (2023). Analisis Komparatif Metode Weighted Product (WP) dan Metode Simple Additive Weighting (SAW). *Jurnal Pendidikan Sains dan Komputer*, 3(02), 205-215.

Supriyanti, W. (2023). Comparative analysis of the sensitivity test of the SAW and WP methods in scholarship selection. *Jurnal Teknik Informatika CIT Medicom*, 15(2), 84-95.

Tarissa, B. V., & Dewayanto, T. (2024). Penerapan Machine Learning dan Deep Learning pada Peningkatan Deteksi Credit Card Fraud-A Systematic Literature Review. *Diponegoro Journal of Accounting*, 13(3).