TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1345-1355
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10906

Sistem Informasi Arsip Berkas Perkara dengan Replikasi Basis Data dan Deteksi Anomali VAE

Sepfliana Qethi Jaminda Eka Putri*, Hadi Kurnia Saputra, Ahmaddul Hadi, Delvi Asmara

Fakultas Teknik, Program Studi Informatika, Universitas Negeri Padang, Padang, Indonesia
Email: [1,*]sepflianaqethi6@gmail.com, [2]hadiksaputra@ft.unp.ac.id, [3]dulhadi@ft.unp.ac.id, [4]delviasmara@ft.unp.ac.id
Email Penulis Korespondensi: sepflianaqethi6@gmail.com

Abstrak–Pengelolaan arsip berkas perkara pada instansi kejaksaan memerlukan proses penelusuran yang akurat, pengendalian akses, serta perlindungan informasi arsip yang andal selama tahapan pra penuntutan, penuntutan, dan eksekusi. Prosedur pengarsipan yang berjalan telah mengacu pada Jadwal Retensi Arsip (JRA) dan mekanisme pengendalian akses, tetapi pengelolaan dan perlindungan informasi arsip masih memerlukan dukungan digital untuk meningkatkan keterlacakan, integritas data, serta ketahanan terhadap aktivitas tidak sah dan risiko kehilangan data. Penelitian ini mengembangkan sistem informasi arsip berkas perkara yang mengintegrasikan metadata arsip dengan mekanisme keamanan dan ketahanan data. Sistem yang dikembangkan menggabungkan autentikasi dua faktor (2FA) berbasis TOTP, *Role-Based Access Control* (RBAC), *cryptographic hashing* SHA-256, *immutable audit log* dengan *hash chaining*, replikasi basis data menggunakan arsitektur *Primary-Replica* dengan *Write-Ahead Logging* (WAL) streaming, serta deteksi anomali menggunakan *Variational Autoencoder* (VAE). Sistem dikembangkan menggunakan model *Evolutionary Prototype* dan diimplementasikan dengan Electron, ReactJS, Node.js, PostgreSQL, serta PyTorch. Pengujian dilakukan pada lingkungan intranet dengan sekitar 100 pengguna aktif melalui *User Acceptance Testing*, pengujian API, pengujian integritas, pengujian replikasi basis data, serta evaluasi performa VAE menggunakan metrik *Precision*, *Recall*, *F1-Score*, dan *AUC-ROC*. Hasil pengujian menunjukkan bahwa seluruh 13 skenario fungsional dan 16 *endpoint* API berjalan sesuai harapan, mekanisme integritas berhasil mendeteksi seluruh manipulasi pada data uji, dan replikasi basis data tersinkronisasi secara otomatis. Model VAE mencapai *Recall* sebesar 1,0000, *F1-Score* sebesar 0,8197, dan *AUC-ROC* sebesar 1,0000, sedangkan *Precision* sebesar 0,6944 menunjukkan bahwa optimasi ambang batas dan penyempurnaan model masih diperlukan untuk mengurangi deteksi *false positive*. Sistem yang dikembangkan diposisikan sebagai sarana pendukung digital terhadap prosedur pengarsipan yang telah berjalan dan bukan sebagai pengganti prosedur pengarsipan di lingkungan kejaksaan.

Kata Kunci: Arsip Berkas Perkara; Autentikasi Dua Faktor; *Immutable Audit Log*; Replikasi Basis Data; *Variational Autoencoder*

Abstract–The management of case-file archives in prosecutorial institutions requires accurate tracking, controlled access, and reliable protection of archival records throughout the pre-prosecution, prosecution, and execution stages. Existing archival procedures rely on retention schedules and access-control mechanisms, but the management and protection of archival information require digital support to improve traceability, data integrity, and resilience against unauthorized activities or data loss. This study develops a case-file archive information system that integrates digital archival metadata with security and data-resilience mechanisms. The proposed system combines two-factor authentication (2FA) using TOTP, Role-Based Access Control (RBAC), SHA-256 cryptographic hashing, immutable audit logs with hash chaining, database replication using a Primary-Replica architecture with Write-Ahead Logging (WAL) streaming, and anomaly detection using a Variational Autoencoder (VAE). The system was developed using an Evolutionary Prototype approach and implemented with Electron, ReactJS, Node.js, PostgreSQL, and PyTorch. Evaluation was conducted in an intranet environment with approximately 100 active users through User Acceptance Testing, API testing, integrity testing, database replication testing, and VAE performance evaluation using Precision, Recall, F1-Score, and AUC-ROC. The results showed that all 13 functional scenarios and 16 API endpoints operated as expected, integrity mechanisms successfully detected all data manipulations in the test data, and database replication was synchronized automatically. The VAE achieved a Recall of 1.0000, F1-Score of 0.8197, and AUC-ROC of 1.0000, while its Precision of 0.6944 indicates that further threshold optimization and model refinement are required to reduce false-positive detections. The system therefore serves as digital support for existing archival procedures rather than replacing established archival practices in prosecutorial institutions.

Keywords: Case-File Archives; Two-Factor Authentication; Immutable Audit Log; Database Replication; Variational Autoencoder

1. PENDAHULUAN

Pengelolaan arsip berkas perkara pada instansi kejaksaan tidak hanya berkaitan dengan kegiatan administratif, tetapi juga dengan keberlangsungan informasi yang memiliki nilai hukum dan harus dapat dipertanggungjawabkan. Arsip perkara merekam proses penanganan perkara sejak tahap pra penuntutan, penuntutan, hingga eksekusi, sehingga pengelolaannya menuntut keteraturan, autentisitas, integritas, keamanan akses, serta keterlacakan sepanjang masa retensinya. Kebutuhan tersebut sejalan dengan kerangka kearsipan nasional yang menempatkan arsip elektronik sebagai bagian dari tata kelola pemerintahan berbasis elektronik. Peraturan Arsip Nasional Republik Indonesia Nomor 6 Tahun 2021 tentang Pengelolaan Arsip Elektronik menegaskan bahwa pengelolaan arsip elektronik diperlukan untuk mendukung penyelenggaraan pemerintahan yang efektif, transparan, akuntabel, serta menghasilkan informasi yang dapat dipercaya (A. N. R. Indonesia, 2021). Pada lingkungan Kejaksaan, pengelolaan arsip juga memiliki landasan khusus melalui Peraturan Kejaksaan Republik Indonesia Nomor 8 Tahun 2022 tentang Klasifikasi Arsip dan Peraturan Kejaksaan Republik Indonesia Nomor 9 Tahun 2022 tentang Jadwal Retensi Arsip di Lingkungan Kejaksaan Republik Indonesia. Peraturan tersebut menunjukkan bahwa pengelolaan arsip perkara tidak dapat dipisahkan dari pengendalian klasifikasi, akses, masa simpan, pemindahan, pemusnahan, maupun penyelamatan arsip yang memiliki nilai berkelanjutan (K. A. R. Indonesia, 2022a, 2022b).

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1345-1355
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10906

Konteks tersebut menjadi penting pada Kejaksaan Negeri Pariaman karena hasil analisis kondisi lapangan menunjukkan adanya kesenjangan antara prosedur pengelolaan arsip yang telah ditetapkan dan dukungan teknologi yang tersedia. Pengelolaan arsip berkas perkara masih menggunakan daftar arsip berbasis Microsoft Excel, sedangkan pencarian, pencatatan peminjaman, pengelolaan lokasi penyimpanan, dan sebagian proses administrasi arsip masih dilakukan secara manual. Kondisi ini tidak berarti bahwa prosedur kearsipan tidak tersedia, tetapi menunjukkan bahwa penerapan prosedur tersebut belum sepenuhnya didukung oleh sistem informasi yang mampu mengotomasi dan mencatat proses secara terintegrasi. Berdasarkan hasil wawancara yang terdokumentasi dalam penelitian, permasalahan yang ditemukan meliputi belum tersedianya sistem informasi khusus untuk arsip perkara, proses pencarian yang bergantung pada daftar Excel, belum adanya mekanisme pencadangan data yang terstruktur, belum diterapkannya kontrol akses secara sistematis, serta belum tersedianya mekanisme teknis untuk memverifikasi integritas arsip dan menjaga jejak aktivitas pengguna dari manipulasi. Kondisi penyimpanan fisik yang belum memadai juga pernah menyebabkan arsip menumpuk dalam kardus, sehingga risiko pengelolaan tidak hanya berkaitan dengan efisiensi pencarian, tetapi juga dengan keberlangsungan dan keterlacakan informasi arsip. (Lappin et al., 2021)

Permasalahan tersebut menjadi lebih signifikan ketika arsip dialihmediakan ke bentuk digital. Representasi digital memang dapat meningkatkan kemudahan akses dan penelusuran, tetapi digitalisasi tanpa mekanisme pengendalian yang memadai dapat memindahkan risiko dari kerusakan fisik menjadi risiko manipulasi, kehilangan data, akses tidak sah, dan kesulitan membuktikan perubahan terhadap arsip. Oleh karena itu, sistem digital untuk arsip perkara perlu dirancang bukan hanya sebagai media penyimpanan atau pencarian dokumen, tetapi sebagai lingkungan pengelolaan informasi yang mampu menjaga aspek kerahasiaan, integritas, dan ketersediaan data. Dalam penelitian ini, kebutuhan tersebut diterjemahkan ke dalam beberapa lapisan pengamanan, yaitu autentikasi dua faktor dan pengendalian akses berbasis peran untuk membatasi akses pengguna, hashing SHA-256 untuk memverifikasi integritas berkas, immutable audit log dengan hash chaining untuk menjaga keterlacakan aktivitas, serta replikasi basis data untuk mengurangi risiko kehilangan data akibat gangguan pada server utama. Penerapan replikasi menjadi relevan karena arsip yang bersifat permanen membutuhkan mekanisme penyimpanan cadangan yang terstruktur dan dapat dipulihkan tanpa bergantung sepenuhnya pada media penyimpanan eksternal. Implementasi penelitian menunjukkan bahwa PostgreSQL dengan WAL streaming dapat mempertahankan sinkronisasi antara basis data primary dan replica, termasuk melakukan sinkronisasi kembali setelah server replica mengalami kondisi tidak aktif. (Bawono, 2022; Oladejo & Hadžidedić, 2021)

Penelitian mengenai sistem informasi kearsipan pada lingkungan kejaksaan sebelumnya telah menunjukkan manfaat digitalisasi dalam meningkatkan pengelolaan arsip. (Erfan, 2025), misalnya, mengembangkan sistem informasi arsip berkas perkara pidana umum pada Kejaksaan Negeri Palangka Raya dengan fokus pada digitalisasi dan efisiensi pengelolaan administrasi perkara. Penelitian lain pada Kejaksaan Tinggi Sulawesi Utara menerapkan K-Means untuk pengelompokan arsip surat masuk dan keluar, sedangkan penelitian (Elvina, 2023; Setiawan & Effiyaldi, 2022) pada Kejaksaan Negeri Padang berfokus pada perancangan sistem informasi arsip digital berbasis web. (Setiawan & Effiyaldi, 2022) juga mengembangkan sistem informasi manajemen berkas perkara pada Kejaksaan Negeri Merangin. Penelitian-penelitian tersebut menunjukkan bahwa digitalisasi pengelolaan arsip pada lingkungan kejaksaan telah menjadi kebutuhan yang diteliti, tetapi fokusnya masih dominan pada pengelolaan dokumen, efisiensi administrasi, dan penyediaan akses informasi. Berdasarkan penelusuran terhadap penelitian terkait yang digunakan dalam penelitian ini, belum ditemukan integrasi yang sama antara pengelolaan siklus hidup arsip berdasarkan JRA, kontrol akses berlapis, verifikasi integritas berkas, immutable audit log, replikasi basis data, dan deteksi anomali aktivitas pengguna dalam satu sistem arsip berkas perkara.

Kesenjangan tersebut juga berkaitan dengan kemampuan sistem dalam mengawasi aktivitas pengguna. Mekanisme berbasis aturan (*rule-based*) tetap relevan dan bahkan diperlukan untuk pelanggaran yang dapat didefinisikan secara deterministik, misalnya larangan akses terhadap fungsi tertentu berdasarkan peran pengguna. Namun, pendekatan berbasis aturan bergantung pada pengetahuan mengenai skenario pelanggaran yang telah diketahui sebelumnya. Pada sistem berbasis log, keterbatasan tersebut menjadi penting karena aktivitas mencurigakan tidak selalu berupa satu tindakan yang secara eksplisit melanggar aturan, tetapi dapat muncul sebagai kombinasi beberapa karakteristik aktivitas, seperti waktu akses, alamat IP, perangkat, frekuensi aktivitas, jenis tindakan, dan jumlah objek yang diproses. Penelitian mengenai deteksi anomali pada log juga menunjukkan bahwa pendekatan berbasis aturan memiliki ketergantungan pada aturan yang telah ditentukan sebelumnya dan dapat menghasilkan *false positive*, sehingga pendekatan pembelajaran tanpa pengawasan dapat digunakan sebagai lapisan tambahan untuk mengenali pola yang tidak dimodelkan secara eksplisit oleh aturan. (Fährmann, 2022)

Berdasarkan karakteristik tersebut, penelitian ini menggunakan *Variational Autoencoder* (VAE) sebagai metode deteksi anomali pada *audit log*, bukan sebagai pengganti mekanisme aturan dan kontrol akses. VAE merupakan model generatif yang dapat mempelajari representasi probabilistik dari distribusi data melalui ruang laten. Pendekatan ini relevan ketika contoh anomali historis sulit diperoleh atau tidak tersedia dalam jumlah memadai, karena model dapat dibangun berdasarkan karakteristik aktivitas normal dan kemudian digunakan untuk mengidentifikasi penyimpangan dari pola yang dipelajari. Kajian terhadap deteksi anomali berbasis deep learning menunjukkan bahwa pendekatan unsupervised dapat mempelajari pola log dan mendeteksi kejadian yang tidak diharuskan untuk dimodelkan satu per satu secara manual, meskipun efektivitasnya tetap dipengaruhi oleh kualitas data pelatihan, distribusi kelas, noise, dan strategi evaluasi (Landauer et al., 2023; Le & Zhang, 2022). Penelitian VAE terbaru juga menunjukkan penggunaan VAE sebagai pendekatan unsupervised untuk berbagai jenis data multivariat dan time series, yang memperkuat

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1345-1355
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10906

relevansinya sebagai salah satu pendekatan untuk memodelkan penyimpangan dari distribusi data normal (Giger & Csillaghy, 2024; Shahid et al., 2024).

Pemilihan VAE dalam penelitian ini juga mempertimbangkan karakteristik data audit log yang digunakan. Audit log sistem memuat kombinasi atribut kategorikal dan numerik yang merepresentasikan aktivitas pengguna, antara lain identitas pengguna, jenis tindakan, tipe objek, status, perangkat, alamat IP, durasi aktivitas, jumlah objek, jam, dan hari dalam minggu. Dengan karakteristik tersebut, tujuan deteksi bukan sekadar menentukan apakah satu aktivitas termasuk dalam daftar aturan yang dilarang, tetapi mengidentifikasi aktivitas yang menyimpang dari pola penggunaan yang dianggap normal. VAE diposisikan untuk mempelajari distribusi pola tersebut dan menghasilkan skor anomali yang kemudian ditinjau oleh administrator. Posisi ini penting dalam konteks lingkungan hukum karena algoritma tidak diberi kewenangan untuk mengambil tindakan otomatis terhadap pengguna maupun arsip. Hasil deteksi hanya menjadi informasi pendukung bagi administrator, sedangkan keputusan menerima, menolak, atau melakukan *override* tetap berada pada pihak yang berwenang dan dicatat dalam audit log. Desain tersebut sesuai dengan implementasi penelitian yang secara eksplisit menempatkan VAE sebagai alat bantu pengawasan pasif. (Li et al., 2021)

Meskipun demikian, penggunaan VAE tidak dianggap bebas dari keterbatasan. Deteksi anomali berbasis pembelajaran mesin dapat menghasilkan *false positive* ketika variasi aktivitas normal tidak cukup terwakili dalam data pelatihan atau ketika ambang deteksi belum sesuai dengan karakteristik operasional sebenarnya. Penelitian mengenai deteksi anomali berbasis log juga menunjukkan bahwa kualitas data pelatihan, distribusi data, noise, dan konfigurasi evaluasi dapat memberikan pengaruh besar terhadap performa model (Le & Zhang, 2022). Oleh sebab itu, penelitian ini tidak menempatkan VAE sebagai mekanisme tunggal untuk menentukan pelanggaran, melainkan sebagai lapisan pengawasan tambahan yang bekerja bersama mekanisme autentikasi, RBAC, integritas berkas, *audit log*, dan replikasi basis data. Pendekatan tersebut memungkinkan sistem tetap menggunakan aturan deterministik untuk pengendalian akses sekaligus memanfaatkan pembelajaran mesin untuk mengidentifikasi pola aktivitas yang belum tentu dapat dirumuskan sebelumnya sebagai aturan.

Berdasarkan permasalahan dan kesenjangan tersebut, penelitian ini bertujuan mengembangkan sistem informasi arsip berkas perkara yang mendukung pengelolaan arsip sesuai tahapan penanganan perkara, klasifikasi, status retensi, lokasi penyimpanan, dan peminjaman, sekaligus menyediakan mekanisme keamanan dan ketahanan data melalui autentikasi dua faktor, RBAC, *hashing* SHA-256, immutable audit log, serta replikasi basis data *Primary-Replica*. Selain itu, penelitian menerapkan VAE sebagai alat bantu pengawasan pasif untuk mendeteksi penyimpangan pola aktivitas pengguna berdasarkan audit log. Kontribusi penelitian terletak pada integrasi pengelolaan siklus hidup arsip perkara dengan mekanisme keamanan berlapis, ketahanan data melalui replikasi basis data, dan deteksi anomali berbasis pembelajaran tanpa pengawasan dalam satu sistem yang dirancang untuk lingkungan intranet instansi penegak hukum. Dengan demikian, kontribusi penelitian tidak terletak pada penciptaan algoritma VAE baru, melainkan pada penerapan dan integrasi metode tersebut ke dalam arsitektur sistem kearsipan perkara yang mempertahankan kewenangan pengambilan keputusan pada manusia serta menghubungkan aspek pengelolaan arsip, keamanan informasi, ketersediaan data, dan pengawasan aktivitas dalam satu lingkungan operasional.

2. METODOLOGI PENELITIAN

2.1 Kerangka Dasar Penelitian

Penelitian ini merupakan penelitian rancang bangun (*design and development research*) di bidang rekayasa perangkat lunak yang bertujuan menghasilkan sistem informasi arsip berkas perkara beserta mekanisme keamanan, ketahanan data, dan deteksi anomali aktivitas pengguna. Penelitian dilakukan pada lingkungan Kejaksaan yang mengelola arsip berkas perkara melalui tahapan pra penuntutan, penuntutan, dan eksekusi. Sistem dirancang untuk mendukung tiga kelompok pengguna, yaitu Admin, Arsiparis, dan User, dengan hak akses yang disesuaikan dengan fungsi masing-masing pengguna. Kerangka penelitian dimulai dengan identifikasi proses pengarsipan yang berjalan, analisis kebutuhan, perancangan sistem, implementasi komponen, integrasi antarkomponen, dan pengujian untuk menilai kesesuaian sistem terhadap kebutuhan yang telah dirumuskan.

Pengembangan sistem dilakukan secara bertahap dengan mempertimbangkan ketergantungan antarkomponen, sehingga komponen yang menjadi dasar bagi komponen lain diselesaikan dan diuji terlebih dahulu sebelum dilakukan integrasi lebih lanjut. Komponen yang dikembangkan meliputi pengelolaan arsip dan retensi, autentikasi dan otorisasi, verifikasi integritas berkas, pencatatan aktivitas pengguna, replikasi basis data, serta deteksi anomali berbasis *Variational Autoencoder* (VAE). Urutan pengembangan tersebut digunakan untuk memastikan bahwa kebutuhan pengguna dapat divalidasi melalui implementasi dan pengujian pada setiap tahap sebelum komponen berikutnya diintegrasikan. Dengan demikian, model pengembangan digunakan sebagai mekanisme pengendalian proses rekayasa perangkat lunak, bukan sekadar sebagai tahapan formal dalam penelitian.

2.2 Tahapan Penelitian

Pengembangan sistem menggunakan model *Evolutionary Prototype*. Pemilihan model ini didasarkan pada kebutuhan untuk melakukan validasi dan penyempurnaan sistem secara bertahap. Dalam *evolutionary prototyping*, prototipe dikembangkan melalui siklus *guess-check-modify*, yaitu menghasilkan representasi awal sistem, memperoleh umpan balik terhadap hasil yang ditampilkan, kemudian melakukan modifikasi berdasarkan hasil evaluasi hingga sistem

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1345-1355
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10906

memenuhi kebutuhan pengguna. Pendekatan tersebut sesuai untuk kondisi ketika kebutuhan sistem perlu dikonfirmasi melalui implementasi dan evaluasi secara bertahap.

Tahap *Communication* dilakukan dengan mengidentifikasi proses pengarsipan yang berjalan, permasalahan yang ditemukan, kebutuhan fungsional dan nonfungsional, serta karakteristik pengguna. Tahap *Quick Plan* digunakan untuk menentukan kebutuhan teknis, lingkungan implementasi, komponen keamanan, rancangan basis data, arsitektur *Primary-Replica*, serta kebutuhan pengembangan layanan VAE. Tahap *Modelling Quick Design* menghasilkan rancangan sistem yang meliputi *Use Case Diagram*, *Activity Diagram*, *Sequence Diagram*, *Class Diagram*, *Entity Relationship Diagram* (ERD), arsitektur sistem, dan rancangan antarmuka pengguna.

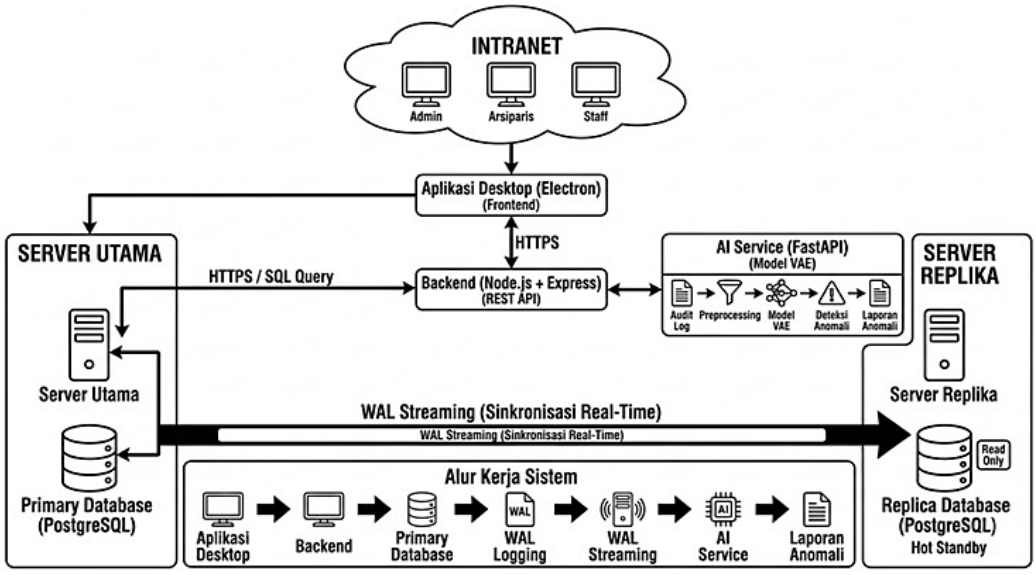
Tahap *Construction* dilakukan dengan mengimplementasikan rancangan menjadi sistem yang dapat dijalankan. Implementasi mencakup aplikasi desktop berbasis Electron dan ReactJS, backend menggunakan Node.js dan Express, basis data PostgreSQL, layanan AI menggunakan FastAPI dan PyTorch, serta mekanisme keamanan dan replikasi basis data. Setelah komponen dapat dijalankan, tahap *Deployment, Delivery, and Feedback* dilakukan melalui pengujian terhadap fungsi dan karakteristik sistem. Hasil pengujian digunakan untuk mengidentifikasi ketidaksesuaian dan menjadi masukan bagi penyempurnaan sistem pada siklus berikutnya.

Penerapan model tersebut juga digunakan untuk mengendalikan ketergantungan antarkomponen. Fungsi dasar pengelolaan arsip dan autentikasi dikembangkan terlebih dahulu, kemudian mekanisme integritas dan audit log diterapkan untuk menghasilkan rekaman aktivitas yang dapat digunakan dalam pengawasan. Setelah alur penyimpanan data berjalan, mekanisme replikasi basis data dan layanan VAE diintegrasikan ke dalam sistem. Dengan demikian, setiap komponen dapat diuji sebelum digunakan sebagai bagian dari komponen berikutnya.

2.3 Arsitektur Sistem

Sistem dirancang sebagai aplikasi desktop menggunakan Electron dan ReactJS yang beroperasi pada lingkungan intranet. Aplikasi desktop berfungsi sebagai lapisan antarmuka pengguna, sedangkan proses autentikasi, otorisasi, logika bisnis, akses basis data, dan komunikasi dengan layanan kecerdasan buatan ditangani oleh *backend* Node.js dan Express. Pemisahan tersebut digunakan untuk mencegah aplikasi klien melakukan pengelolaan data secara langsung pada basis data dan menempatkan pengendalian akses pada lapisan *backend*. Arsitektur sistem terdiri atas beberapa komponen yang memiliki tanggung jawab berbeda. Aplikasi desktop Electron berfungsi sebagai *client layer* yang digunakan oleh Admin, Arsiparis, dan User. *Backend* Node.js dan Express berfungsi sebagai *application layer* yang menerima permintaan dari aplikasi desktop, melakukan autentikasi dan otorisasi berdasarkan JWT dan RBAC, menjalankan logika bisnis, serta berkomunikasi dengan Primary Database dan AI Service. Primary Database menggunakan PostgreSQL dan berfungsi sebagai penyimpanan utama seluruh data sistem. Replica Database digunakan sebagai salinan data pada server terpisah dan menerima perubahan dari Primary Database melalui mekanisme *Write-Ahead Logging* (WAL) streaming.

Aktivitas pengguna yang diproses melalui backend dicatat ke dalam *immutable audit log*. Rekaman tersebut menjadi sumber data bagi AI Service berbasis FastAPI untuk proses deteksi anomali menggunakan VAE. Data audit log melalui tahap *preprocessing* sebelum diberikan kepada model VAE. Model kemudian menghasilkan hasil deteksi berdasarkan penyimpangan pola aktivitas dan laporan anomali disampaikan kepada administrator sebagai informasi pendukung dalam proses pengawasan.



Gambar 1. Arsitektur Sistem Informasi Arsip Berkas Perkara

Gambar 1 menunjukkan alur komunikasi dan pembagian fungsi antarkomponen sistem dalam lingkungan intranet. Aplikasi desktop digunakan oleh pengguna sebagai titik akses sistem dan berkomunikasi dengan backend

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1345-1355
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10906

melalui HTTPS. Backend selanjutnya menjadi penghubung utama antara aplikasi dengan Primary Database dan AI Service. Primary Database menyimpan data utama sistem dan meneruskan perubahan data melalui WAL streaming ke Replica Database. Sementara itu, audit log digunakan sebagai sumber data untuk proses deteksi anomali pada AI Service. Dengan pembagian tersebut, keberadaan beberapa komponen dalam arsitektur tidak ditujukan untuk menambah kompleksitas jaringan, tetapi untuk memisahkan fungsi akses pengguna, logika aplikasi, penyimpanan data, ketahanan data, dan pengawasan aktivitas.

2.4 Pertimbangan Keamanan Penggunaan Electron

Penggunaan Electron pada sistem yang menangani arsip berkas perkara memerlukan pertimbangan keamanan khusus karena Electron menggabungkan teknologi web dengan kemampuan aplikasi desktop. Berbeda dengan aplikasi web pada browser biasa, kode pada aplikasi Electron dapat memiliki akses yang lebih besar terhadap sumber daya sistem. Oleh karena itu, kerentanan pada lapisan *renderer*, termasuk *Cross-Site Scripting* (XSS), dapat memiliki dampak yang lebih besar apabila kode yang tidak tepercaya memperoleh akses terhadap kemampuan Node.js atau API Electron. Dokumentasi keamanan Electron secara khusus menekankan bahwa kerentanan seperti *Cross-Site Scripting* (XSS) memiliki dampak keamanan yang lebih tinggi pada aplikasi Electron dibandingkan konteks web biasa (Electron, 2026). Dalam arsitektur penelitian ini, Electron ditempatkan sebagai lapisan antarmuka dan tidak digunakan sebagai lapisan penyimpanan data. Operasi terhadap data arsip dilakukan melalui backend sehingga akses terhadap Primary Database tidak diberikan secara langsung kepada aplikasi klien. Backend menjadi titik pengendalian untuk autentikasi, otorisasi, validasi permintaan, dan akses terhadap data. Pendekatan ini membatasi permukaan akses terhadap basis data dan memungkinkan aturan keamanan diterapkan secara terpusat pada sisi server. Pada sisi Electron, pengamanan aplikasi perlu memperhatikan pemisahan antara *renderer process* dan proses yang memiliki hak istimewa. Electron juga merekomendasikan penggunaan *context isolation* dan *process sandboxing*, tidak mengaktifkan *Node.js integration* untuk konten yang tidak tepercaya, membatasi navigasi dan pembuatan jendela, serta menerapkan *Content Security Policy* (CSP) untuk membatasi sumber skrip dan konten yang dapat dieksekusi (Electron, 2026).

Selain pengamanan pada sisi aplikasi desktop, komunikasi antara aplikasi dan backend menggunakan HTTPS untuk melindungi data selama transmisi. Penggunaan HTTPS memberikan perlindungan terhadap penyadapan dan perubahan data selama komunikasi berlangsung. Keamanan aplikasi juga tidak hanya bergantung pada jaringan intranet, tetapi dibangun secara berlapis melalui autentikasi dua faktor, RBAC, validasi pada backend, hashing SHA-256, *immutable audit log*, dan replikasi basis data.

Dengan demikian, lingkungan intranet diposisikan sebagai salah satu lapisan pembatas akses jaringan, bukan sebagai satu-satunya mekanisme keamanan. Pendekatan tersebut diperlukan karena keamanan aplikasi desktop tetap dipengaruhi oleh konfigurasi Electron, kode aplikasi, dependensi perangkat lunak, dan mekanisme komunikasi dengan layanan backend.

2.5 Teknik Pengujian Sistem

Pengujian sistem dilakukan melalui lima pendekatan untuk menilai kesesuaian fungsional dan nonfungsional. Pertama, *User Acceptance Testing* (UAT) untuk memverifikasi bahwa setiap fitur menghasilkan *output* yang sesuai dengan *output* yang diharapkan berdasarkan skenario yang dirancang. Kedua, pengujian API menggunakan Postman untuk memastikan setiap *endpoint backend* memproses permintaan HTTP dengan benar. Ketiga, pengujian integritas untuk membuktikan bahwa mekanisme *cryptographic hashing* dan *immutable audit log* mampu mendeteksi manipulasi data. Keempat, pengujian replikasi basis data untuk membuktikan sinkronisasi data antara basis data utama dan basis data cadangan, baik pada kondisi normal maupun setelah basis data cadangan sempat tidak aktif. Kelima, pengujian fungsional dan nonfungsional modul VAE, dengan pengujian nonfungsional menggunakan metrik Precision, Recall, F1-Score, dan AUC-ROC yang dihitung berdasarkan *confusion matrix* hasil klasifikasi model terhadap data uji. Nilai ambang batas (*threshold*) yang memisahkan aktivitas normal dan anomali ditentukan menggunakan rumus berikut.

$$Threshold = mean + 3\,x\,sigma \quad (1)$$

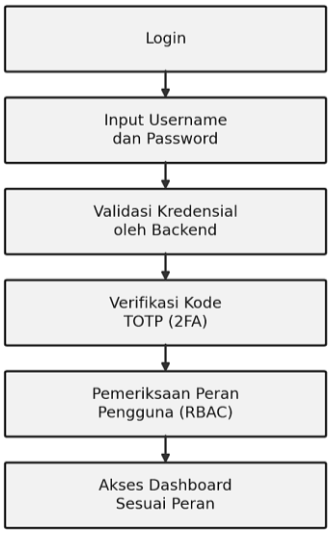
Dengan mean adalah nilai rata-rata *reconstruction error* pada data pelatihan dan sigma adalah standar deviasi *reconstruction error* pada data pelatihan. Aktivitas dengan *reconstruction error* yang melampaui nilai *threshold* diklasifikasikan sebagai anomali, sedangkan aktivitas dengan *reconstruction error* di bawah *threshold* diklasifikasikan sebagai aktivitas normal.

3. HASIL DAN PEMBAHASAN

3.1 Implementasi Autentikasi Berlapis

Mekanisme autentikasi sistem menggabungkan *Two-Factor Authentication* (2FA) berbasis TOTP dengan *Role-Based Access Control* (RBAC) untuk tiga peran pengguna, yaitu Admin, Arsiparis, dan User. Alur autentikasi diilustrasikan pada Gambar 2.

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1345-1355
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10906



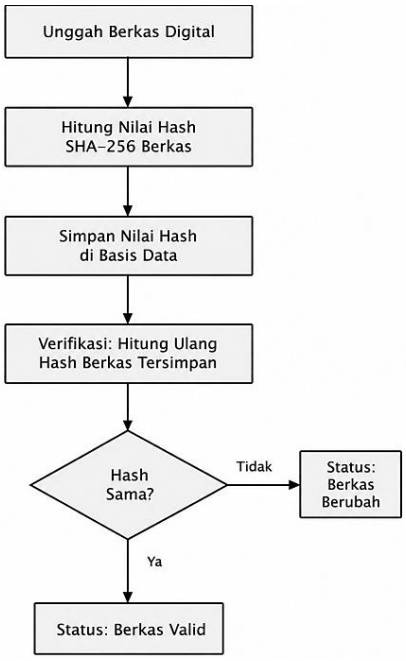
Gambar 2. Diagram Alur Autentikasi Berlapis (2FA dan RBAC)

Gambar 2 menunjukkan bahwa pengguna pertama kali memasukkan username dan password sebagai faktor pertama. Apabila kredensial tersebut valid, sistem meminta kode TOTP enam digit yang dihasilkan oleh aplikasi authenticator pada perangkat pengguna sebagai faktor kedua. Setelah kode TOTP terverifikasi, sistem memeriksa peran pengguna melalui mekanisme RBAC untuk menentukan menu dan fitur yang dapat diakses, sebelum akhirnya menampilkan dashboard sesuai dengan hak akses masing-masing peran. Admin memperoleh akses penuh ke seluruh menu dan konfigurasi sistem, Arsiparis dapat menambah, mengubah, menghapus, dan melihat data arsip, sedangkan User hanya dapat melihat data arsip tanpa kemampuan mengubah data.

Hasil pengujian User Acceptance Testing menunjukkan bahwa dari 13 skenario yang diuji, seluruhnya dinyatakan berhasil, termasuk skenario login dengan kredensial valid, verifikasi kode TOTP, penolakan login dengan password salah, serta penolakan akses lintas peran pada pengujian RBAC. Pengujian API menggunakan Postman turut menunjukkan bahwa *endpoint* /auth/login dan /auth/verify-otp menghasilkan response sesuai harapan pada seluruh 16 *endpoint* yang diuji. Dengan demikian, mekanisme autentikasi berlapis ini menyediakan lapisan verifikasi identitas tambahan yang melengkapi kontrol akses fisik terhadap ruang penyimpanan arsip yang telah berjalan pada instansi kejaksaan.

3.2 Implementasi Integritas Berkas dan Audit Log

Keaslian setiap berkas digital yang diunggah ke dalam sistem dijamin melalui *cryptographic hashing* menggunakan algoritma SHA-256, sedangkan seluruh aktivitas pengguna dicatat melalui *immutable audit log* dengan teknik *hash chaining*. Alur verifikasi integritas berkas ditunjukkan pada Gambar 3.



Gambar 3. Diagram Alur Verifikasi Integritas Berkas

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1345-1355
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10906

Gambar 3 menunjukkan bahwa setiap berkas yang diunggah terlebih dahulu dihitung nilai hash SHA-256-nya, kemudian nilai tersebut disimpan pada basis data bersama metadata berkas. Ketika keaslian berkas perlu diverifikasi, sistem menghitung ulang nilai hash berkas dan membandingkannya dengan nilai hash yang tersimpan. Apabila kedua nilai sama, berkas dinyatakan valid; apabila berbeda, sistem menyatakan bahwa berkas telah mengalami perubahan sejak pertama kali diunggah. Mekanisme yang sama diterapkan pada audit log, di mana setiap entri log menyertakan nilai hash dari entri sebelumnya sehingga membentuk rantai (chain) yang saling terkait secara kriptografis.

Tabel 1 menunjukkan hasil pengujian *cryptographic hashing* dan *immutable audit log* yang dilakukan dengan membandingkan berkas dan entri log asli terhadap berkas dan entri log yang dimodifikasi secara langsung pada server tanpa melalui sistem.

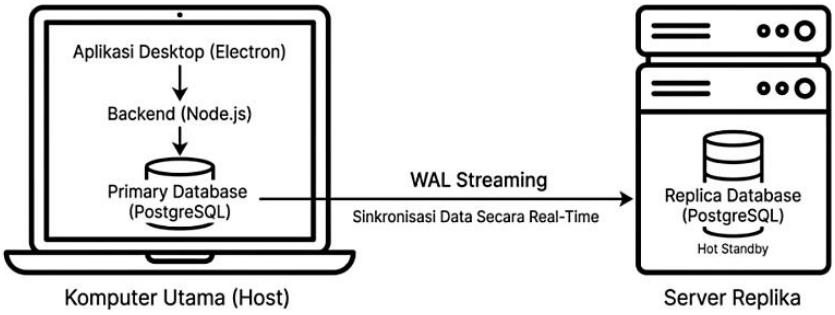
Tabel 1. Hasil Pengujian Integritas Berkas dan Audit Log

No	Komponen Diuji	Skenario	Output Aktual
1	*Cryptographic Hashing*	Verifikasi berkas asli	Hash cocok, status valid
2	*Cryptographic Hashing*	Verifikasi berkas yang dimanipulasi	Hash tidak cocok, status tidak valid terdeteksi
3	*Immutable Audit Log*	Verifikasi rantai *hash* tanpa manipulasi	Rantai *hash* valid
4	*Immutable Audit Log*	Verifikasi setelah salah satu entri diubah langsung di basis data	Ketidakcocokan *hash* terdeteksi pada posisi entri yang diubah

Hasil pada Tabel 1 menunjukkan bahwa kedua mekanisme berhasil mendeteksi seluruh manipulasi yang diujikan, baik pada berkas digital maupun pada rekaman aktivitas pengguna. Kemampuan ini melengkapi prosedur pengarsipan fisik yang telah berjalan dengan menyediakan bukti teknis dan objektif atas keaslian representasi digital arsip, yang dapat digunakan sebagai pendukung pembuktian hukum sejalan dengan prinsip autentisitas arsip elektronik.

3.3 Implementasi Replikasi *Primary-Replica Database*

Ketersediaan data arsip didukung melalui arsitektur *Primary-Replica database* yang diimplementasikan menggunakan PostgreSQL dengan mekanisme *Write-Ahead Logging* (WAL) streaming, sebagaimana diilustrasikan pada Gambar 4.



Gambar 4. Diagram Arsitektur *Primary-Replica* Database

Gambar 4 menunjukkan bahwa seluruh permintaan dari desktop client diproses oleh basis data primary, yang kemudian mereplikasi setiap perubahan data ke basis data replica secara real-time melalui mekanisme *WAL streaming*. Basis data replica berada dalam mode *hot standby*, yaitu hanya menerima dan menerapkan WAL record tanpa memproses transaksi tulis dari pengguna secara langsung.

Tabel 2 menunjukkan ringkasan hasil pengujian replikasi yang dilakukan pada dua skenario, yaitu sinkronisasi data pada kondisi normal dan sinkronisasi data setelah basis data replica sempat tidak aktif untuk sementara waktu.

Tabel 2. Hasil Pengujian Replikasi Database

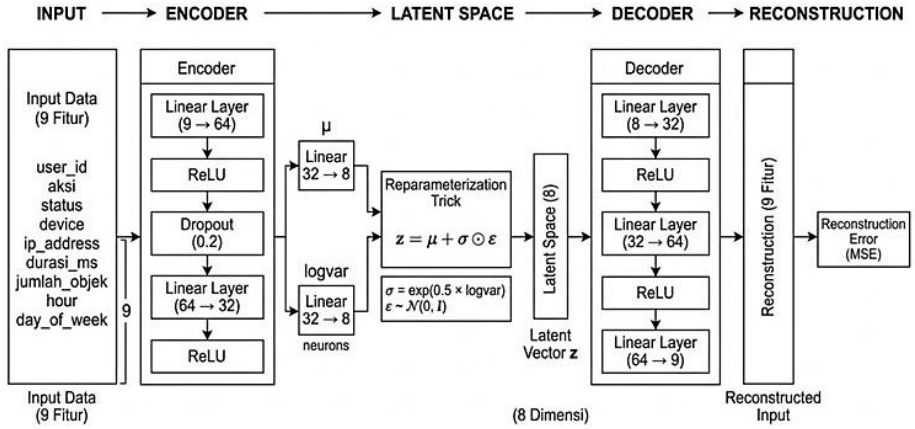
No	Skenario	Output Aktual
1	Sinkronisasi data pada kondisi normal	Data tersinkronisasi ke replica secara real-time
2	Sinkronisasi data setelah replica dinyalakan kembali	Data yang tertunda selama replica tidak aktif tersinkronisasi otomatis begitu replica aktif kembali

Hasil pengujian pada Tabel 2 menunjukkan bahwa arsitektur *Primary-Replica database* mampu menjaga ketersediaan data arsip digital secara otomatis tanpa memerlukan intervensi manual, termasuk pada kondisi basis data replica sempat tidak aktif. Mekanisme ini melengkapi mekanisme pengamanan arsip fisik yang telah berjalan dengan menyediakan salinan data digital yang selalu diperbarui, sehingga mendukung keberlangsungan akses informasi arsip meskipun terjadi gangguan pada server utama.

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1345-1355
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10906

3.4 Implementasi Deteksi Anomali Berbasis VAE

Sebagai lapisan pengawasan tambahan, algoritma *Variational Autoencoder* (VAE) diimplementasikan untuk menganalisis pola aktivitas pengguna yang tercatat pada audit log secara periodik. Alur kerja model VAE ditunjukkan pada Gambar 5.



Gambar 5. Diagram Alur Kerja Deteksi Anomali Berbasis VAE

Gambar 5 menunjukkan bahwa data audit log terlebih dahulu melalui tahap ekstraksi fitur sebelum diproses oleh *encoder* untuk menghasilkan representasi laten (*latent space*) yang lebih ringkas. Representasi laten tersebut kemudian direkonstruksi kembali oleh *decoder* menjadi data dengan dimensi asli. Selisih antara data asli dan data hasil rekonstruksi dihitung sebagai *reconstruction error*, yang selanjutnya dibandingkan dengan nilai *threshold* pada Persamaan (1) untuk menghasilkan skor anomali. Skor anomali beserta tingkat risikonya disampaikan kepada administrator sebagai laporan, tanpa disertai kewenangan untuk mengambil tindakan otomatis apa pun terhadap sistem maupun data arsip. (Iqbal & Qureshi, 2023)

Pengujian fungsional VAE dilakukan menggunakan enam skenario aktivitas, meliputi aktivitas normal, login dari perangkat baru, login dari alamat IP berbeda, akses arsip dalam jumlah tidak wajar, penghapusan data dalam jumlah besar, serta pengujian respons sistem terhadap anomali. Seluruh enam skenario dinyatakan berhasil, dengan sistem menghasilkan klasifikasi dan laporan sesuai dengan skenario pengujian. Sistem juga terbukti konsisten hanya menghasilkan laporan tanpa mengambil tindakan otomatis, sesuai dengan posisi VAE sebagai alat bantu pengawasan pasif. Pengujian nonfungsional VAE mengevaluasi performa model menggunakan *confusion matrix*, kurva ROC, serta metrik Precision, Recall, F1-Score, dan AUC-ROC, dengan hasil ditunjukkan pada Tabel 3.

Tabel 3. Hasil Evaluasi Performa Model VAE

Metrik	Target	Hasil Aktual	Keterangan
Precision	> 0,80	0,6944	Belum memenuhi target
Recall	> 0,75	1	Memenuhi target
F1-Score	> 0,77	0,8197	Memenuhi target
AUC-ROC	> 0,85	1	Memenuhi target

Tabel 3 menunjukkan bahwa model VAE mencapai Recall sebesar 1,0000, F1-Score sebesar 0,8197, dan AUC-ROC sebesar 1,0000 pada data pengujian yang digunakan. Recall sebesar 1,0000 menunjukkan bahwa seluruh aktivitas yang dikategorikan sebagai anomali pada data pengujian berhasil terdeteksi sehingga tidak ditemukan *false negative*. AUC-ROC sebesar 1,0000 menunjukkan bahwa pada data pengujian tersebut model mampu memberikan pemisahan skor yang sangat baik antara aktivitas normal dan anomali. Namun, hasil tersebut perlu dipahami berdasarkan jumlah dan karakteristik data pengujian yang digunakan dan belum dapat dijadikan dasar untuk menyimpulkan kemampuan generalisasi model pada kondisi operasional yang lebih beragam.

Nilai Precision sebesar 0,6944 menunjukkan bahwa sebagian aktivitas yang diprediksi sebagai anomali masih merupakan aktivitas normal (*false positive*). Kondisi ini perlu diperhatikan karena peringatan yang terlalu sering terhadap aktivitas yang sebenarnya normal dapat meningkatkan beban verifikasi administrator dan berpotensi menurunkan efektivitas pengawasan. Dengan demikian, keberhasilan Recall dalam mendeteksi seluruh anomali belum menunjukkan bahwa model telah optimal dalam membatasi *false positive*. Kondisi tersebut kemungkinan dipengaruhi oleh keterbatasan volume dan variasi data pelatihan yang tersedia, sehingga pola aktivitas normal yang belum cukup beragam dapat menyebabkan aktivitas yang valid tetapi jarang muncul memperoleh *reconstruction error* yang relatif tinggi.

Perbaikan terhadap Precision dapat dilakukan melalui beberapa pendekatan teknis. Pertama, nilai *threshold* dapat dikalibrasi menggunakan data validasi untuk memperoleh batas klasifikasi yang lebih sesuai dengan karakteristik data, kemudian dievaluasi berdasarkan keseimbangan antara Precision dan Recall. Kedua, penambahan variasi aktivitas normal pada data pelatihan dapat membantu model mempelajari pola perilaku normal secara lebih representatif

TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1345-1355
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10906

sehingga mengurangi kemungkinan aktivitas normal diklasifikasikan sebagai anomali. Ketiga, evaluasi terhadap fitur audit log dan konfigurasi model dapat dilakukan untuk mengetahui fitur atau parameter yang berkontribusi terhadap peningkatan *false positive*. Pada tingkat operasional, hasil deteksi tetap diposisikan sebagai indikator yang memerlukan verifikasi administrator dan tidak digunakan sebagai dasar pengambilan tindakan otomatis terhadap data maupun akun pengguna. Pendekatan tersebut memungkinkan sistem mempertahankan kemampuan deteksi terhadap anomali sekaligus membatasi dampak *false positive* terhadap proses pengawasan.

3.5 Hasil Pengujian Fungsional Sistem Secara Keseluruhan

Selain pengujian pada masing-masing komponen, dilakukan pula pengujian menyeluruh terhadap fungsi-fungsi utama sistem melalui User Acceptance Testing dan pengujian API. Tabel 4 merangkum hasil pengujian tersebut.

Tabel 4. Ringkasan Hasil Pengujian Fungsional Sistem

Jenis Pengujian	Jumlah Skenario/Endpoint	Berhasil	Persentase
User Acceptance Testing	13	13	100%
Pengujian API (Postman)	16	16	100%

Tabel 4 menunjukkan bahwa seluruh skenario UAT dan *endpoint* API yang diuji berjalan sesuai dengan *output* yang diharapkan, mencakup fungsi autentikasi, manajemen arsip berdasarkan tahapan pra penuntutan, penuntutan, dan eksekusi, manajemen status retensi, peminjaman arsip, audit log, replikasi data, hingga deteksi anomali. Hasil ini menunjukkan bahwa sistem yang dikembangkan telah berfungsi sebagaimana kebutuhan yang dirumuskan pada tahap *Communication* dan *Quick Plan*.

3.6 Pembahasan

Hasil implementasi menunjukkan bahwa kelima komponen sistem, yaitu autentikasi berlapis, cryptographic hashing, immutable audit log, replikasi Primary-Replica database, dan deteksi anomali berbasis VAE, dapat diintegrasikan ke dalam satu sistem informasi arsip berkas perkara yang beroperasi pada lingkungan intranet. Penelitian sebelumnya pada bidang pengelolaan arsip digital menunjukkan bahwa digitalisasi dapat mendukung pengelolaan arsip dan transformasi layanan pemerintahan, termasuk melalui pengembangan sistem pengelolaan arsip dan penerapan pengarsipan elektronik pada sektor publik (Damanik et al., 2024; Rahman et al., 2024; Soulthoni & Itasari, 2025). Berbeda dengan penelitian yang berfokus pada pengelolaan dan transformasi arsip digital tersebut, penelitian ini mengintegrasikan pengelolaan arsip berkas perkara dengan lapisan keamanan, ketahanan data melalui replikasi basis data, serta deteksi anomali aktivitas pengguna dalam satu sistem.

Keterkaitan antara komponen keamanan yang diimplementasikan dengan prinsip CIA Triad, sebagaimana dibahas oleh Harahap et al. (2023), tampak pada kontribusi masing-masing mekanisme terhadap aspek *confidentiality*, *integrity*, dan *availability*. Aspek *confidentiality* didukung melalui autentikasi berlapis dan *Role-Based Access Control* (RBAC) yang membatasi akses berdasarkan peran pengguna. Aspek *integrity* didukung melalui *cryptographic hashing* dan *immutable audit log* yang memungkinkan perubahan terhadap berkas dan catatan aktivitas terdeteksi. Sementara itu, aspek *availability* didukung melalui replikasi *Primary-Replica database* yang menyediakan salinan data pada basis data cadangan. Algoritma VAE berperan sebagai lapisan pengawasan tambahan yang mendukung keamanan sistem secara tidak langsung melalui identifikasi pola aktivitas pengguna yang menyimpang. Pemilihan VAE sejalan dengan penelitian terkini yang menerapkan *Variational Autoencoder* sebagai pendekatan *unsupervised anomaly detection* pada data multivariat dan pola perilaku, termasuk pada data konsumsi energi dan aktivitas penggunaan (Giger & Csillaghy, 2024; Lin et al., 2024; Shahid et al., 2024) Penelitian mengenai deteksi anomali berbasis log juga menunjukkan bahwa pendekatan *deep learning* dapat digunakan untuk mengenali pola aktivitas yang menyimpang pada data log, dengan performa yang dipengaruhi oleh karakteristik data, proses *preprocessing*, dan konfigurasi metode yang digunakan (Khan et al., 2024; Landauer et al., 2023). (González et al., 2022) juga menunjukkan penerapan VAE untuk mendeteksi pola perilaku yang menyimpang.

Posisi VAE sebagai alat bantu pengawasan pasif, dan bukan sebagai pengambil keputusan otomatis, menjadi pertimbangan penting dalam konteks pengelolaan arsip perkara. Sistem hanya menyampaikan skor anomali dan tingkat risiko kepada administrator, sementara keputusan tindak lanjut tetap berada di tangan administrator sebagai pihak yang berwenang, termasuk kewenangan untuk menilai dan mengabaikan hasil deteksi yang dinilai tidak relevan melalui mekanisme *override*. Pendekatan ini membatasi dampak *false positive* terhadap proses operasional karena hasil deteksi model tidak secara langsung memicu perubahan terhadap data, akun pengguna, maupun status arsip.

Secara keseluruhan, hasil pengujian menunjukkan bahwa sistem yang dikembangkan berfungsi sebagai pelengkap digital yang mendukung proses pengelolaan arsip yang telah berjalan pada instansi kejaksaan, tanpa menggantikan prosedur pengarsipan fisik maupun kewenangan pengambilan keputusan oleh pihak yang berwenang. Hasil evaluasi Precision model VAE sebesar 0,6944 yang belum mencapai target menjadi salah satu aspek yang masih memerlukan penyempurnaan. Perbaikan dapat diarahkan pada pengendalian *false positive* melalui kalibrasi nilai *threshold* menggunakan data validasi, penambahan variasi aktivitas normal pada data pelatihan, serta evaluasi terhadap fitur dan konfigurasi model. Dengan pendekatan tersebut, peningkatan Precision dapat diupayakan tanpa mengabaikan kemampuan model dalam mendeteksi aktivitas anomali yang tercermin dari nilai Recall sebesar 1,0000.


TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1345-1355
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10906

Dari sisi potensi penerapan, pendekatan integrasi lima lapisan pendukung yang digunakan dalam penelitian ini memiliki karakteristik yang dapat dipertimbangkan untuk dikembangkan pada instansi pemerintahan atau lembaga hukum lain yang memiliki kebutuhan serupa, seperti kontrol akses berlapis, integritas dokumen, akuntabilitas aktivitas pengguna, ketersediaan data, dan pengawasan aktivitas. Namun, penerapan pada lingkungan lain tetap memerlukan penyesuaian terhadap prosedur, regulasi, karakteristik arsip, infrastruktur, serta volume dan pola aktivitas pengguna pada masing-masing instansi. Oleh karena itu, hasil penelitian ini lebih tepat dipandang sebagai dasar pengembangan lebih lanjut daripada sebagai bukti bahwa sistem dapat langsung digeneralisasikan pada seluruh instansi pemerintahan atau lembaga hukum.

Keterbatasan penelitian ini terutama terletak pada volume dan variasi data yang digunakan dalam pelatihan serta pengujian model VAE, sehingga Precision sebesar 0,6944 belum mencapai target yang ditetapkan dan masih terdapat *false positive*. Kondisi tersebut membatasi kemampuan penelitian dalam mengevaluasi performa model pada pola aktivitas yang lebih beragam. Selain itu, pengujian replikasi basis data dilakukan pada lingkungan virtual menggunakan satu unit perangkat keras sebagai *host*, sehingga karakteristik performa pada infrastruktur server fisik yang terpisah dan skala produksi belum dapat disimpulkan dari penelitian ini. Keterbatasan tersebut menjadi dasar pengembangan selanjutnya melalui perluasan dataset, kalibrasi *threshold* menggunakan data validasi, evaluasi konfigurasi model, serta pengujian pada infrastruktur dengan skala yang lebih representatif.

4. KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem informasi arsip berkas perkara berbasis aplikasi desktop yang beroperasi pada lingkungan intranet sebagai pelengkap digital bagi prosedur pengelolaan arsip yang telah berjalan di instansi kejaksaan. Sistem mengintegrasikan pengelolaan arsip berdasarkan tahapan pra penuntutan, penuntutan, dan eksekusi, manajemen status retensi berdasarkan Jadwal Retensi Arsip, autentikasi dua faktor berbasis TOTP yang dikombinasikan dengan *Role-Based Access Control*, *cryptographic hashing* SHA-256, *immutable audit log* dengan *hash chaining*, arsitektur *Primary-Replica database*, serta *Variational Autoencoder* sebagai alat bantu pengawasan pasif. Kontribusi utama penelitian terletak pada integrasi mekanisme pengelolaan arsip, keamanan, ketersediaan data, dan deteksi anomali berbasis pembelajaran mesin dalam satu sistem yang dirancang dengan mempertahankan kewenangan pengambilan keputusan pada administrator, sehingga hasil deteksi VAE tidak secara otomatis memengaruhi data maupun akun pengguna. Hasil pengujian menunjukkan bahwa seluruh 13 skenario User Acceptance Testing dan 16 *endpoint* API yang diuji berjalan sesuai harapan, mekanisme *cryptographic hashing* dan *immutable audit log* berhasil mendeteksi seluruh manipulasi pada data uji, serta replikasi *Primary-Replica database* berhasil menyinkronkan data pada kondisi normal maupun setelah basis data cadangan sempat tidak aktif. Model VAE mencapai Recall sebesar 1,0000, F1-Score sebesar 0,8197, dan AUC-ROC sebesar 1,0000, sedangkan Precision sebesar 0,6944 belum mencapai target 0,80 dan menunjukkan masih adanya *false positive*. Keterbatasan tersebut menunjukkan bahwa sistem, khususnya modul deteksi anomali, masih memerlukan penyempurnaan melalui perluasan dan peningkatan variasi data, kalibrasi *threshold* menggunakan data validasi, serta evaluasi konfigurasi model. Selain itu, pengujian replikasi pada lingkungan virtual belum merepresentasikan seluruh karakteristik infrastruktur produksi. Dengan demikian, hasil penelitian ini menunjukkan kelayakan pendekatan integrasi yang dikembangkan pada lingkungan pengujian yang digunakan, tetapi belum dapat digunakan untuk menggeneralisasikan kinerja sistem pada instansi lain tanpa pengujian dan penyesuaian lebih lanjut.

REFERENCES

Bawono, H. (2022). Preservasi Digital dan Pengelolaan Arsip Digital di Indonesia: Kontekstualisasi-Sintesis Dua Model Preservasi Digital. *Jurnal Kearsipan*, *17*(2), 147–169. https://doi.org/10.46836/jk.v17i2.257

Damanik, M. P., Cahyarini, B. R., Arsalam, S., Gusparirin, R., Wulan, D. R., Cahyarida, I., Ahad, M. P. Y., & Hamjen, H. (2024). Digital archives management in the public sector: A bibliometric study. *Khizanah Al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan*, *12*(2), 304–318. https://doi.org/10.24252/kah.v12i2a7

Electron. (2026). *Security*. Electron.

Elvina, E. (2023). *Sistem pengelolaan arsip digital*.

Erfan, A. (2025). *Sistem informasi arsip*.

Giger, M., & Csillaghy, A. (2024). Unsupervised anomaly detection with variational autoencoders applied to full-disk solar images. *Space Weather*, *22*(2), e2023SW003516. https://doi.org/10.1029/2023SW003516

Harahap, A. H., Andani, C. D., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya peranan CIA Triad dalam keamanan informasi dan data untuk pemangku kepentingan atau stakeholder. Jurnal Manajemen Pendidikan dan Digital, 1(2), 73–82. https://doi.org/10.38035/jmpd.v1.i2

Indonesia, A. N. R. (2021). *Peraturan Arsip Nasional Republik Indonesia Nomor 6 Tahun 2021*.

Indonesia, K. A. R. (2022a). *Peraturan Kejaksaan Republik Indonesia Nomor 8 Tahun 2022*.

Indonesia, K. A. R. (2022b). *Peraturan Kejaksaan Republik Indonesia Nomor 9 Tahun 2022*.

Khan, Z. A., Shin, D., Bianculli, D., & Briand, L. C. (2024). Impact of log parsing on deep learning-based anomaly detection. *Empirical Software Engineering*, *29*, 139. https://doi.org/10.1007/s10664-024-10533-w


TIN: Terapan Informatika Nusantara
Vol 7, No 3, August 2026, page 1345-1355
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin
DOI 10.47065/tin.v7i3.10906

Landauer, M., Onder, S., Skopik, F., & Wurzenberger, M. (2023). Deep learning for anomaly detection in log data: A survey. *Machine Learning with Applications*, *12*, 100470. https://doi.org/10.1016/j.mlwa.2023.100470

Lappin, J., Jackson, T., Matthews, G., & Ravenwood, C. (2021). Rival records management models in an era of partial automation. *Archival Science*, *21*, 243–266. https://doi.org/10.1007/s10502-020-09354-9

Le, V.-H., & Zhang, H. (2022). Log-based anomaly detection with deep learning: How far are we? *Proceedings of the 44th International Conference on Software Engineering*, 1356–1367. https://doi.org/10.1145/3510003.3510155

Li, L., Yan, J., Wang, H., & Jin, Y. (2021). Anomaly detection of time series with smoothness-inducing sequential variational auto-encoder. *IEEE Transactions on Neural Networks and Learning Systems*, *32*(3), 1177–1191. https://doi.org/10.1109/TNNLS.2020.2980749

Lin, R., Chen, S., He, Z., Wu, B., Zou, H., Zhao, X., & Li, Q. (2024). Electricity behavior modeling and anomaly detection services based on a deep variational autoencoder network. Energies, 17(16), 3904. https://doi.org/10.3390/en17163904

Rahman, K., Adni, D. F., & Putra Nasution, M. A. (2024). Enhancing e-government in digital transformation: Integrating archive management and digital solutions in Pekanbaru, Indonesia. *Otoritas: Jurnal Ilmu Pemerintahan*, *14*(2), 262–276. https://doi.org/10.26618/ojip.v14i2.12374

Setiawan, S., & Effiyaldi, E. (2022). *Pengelolaan arsip digital*.

Shahid, Z. K., Saguna, S., Ahlund, C., & Åhlund, C. (2024). Variational autoencoders for anomaly detection and transfer knowledge in electricity and district heating consumption. *IEEE Transactions on Industry Applications*, *60*(5), 7437–7450. https://doi.org/10.1109/TIA.2024.3425805

Soulthoni, H. P. N., & Itasari, M. (2025). The implementation of electronic-based archiving to accelerate government digitalization in Indonesia. *International Journal of Innovation in Administration and Society*, *5*(1), 49–57. https://doi.org/10.47540/ijias.v5i1.1735

Fährmann, D., Damer, N., Kirchbuchner, F., & Kuijper, A. (2022). Lightweight Long Short-Term Memory Variational Auto-Encoder for Multivariate Time Series Anomaly Detection in Industrial Control Systems. *Sensors*, 22*(8)*, 2886. https://doi.org/10.3390/s22082886

González, D., Patricio, M. A., Berlanga, A., & Molina, J. M. (2022). Variational autoencoders for anomaly detection in the behaviour of the elderly using electricity consumption data. *Expert Systems*, 39*(4)*, e12744. https://doi.org/10.1111/exsy.12744

Iqbal, T., & Qureshi, S. (2023). Reconstruction probability-based anomaly detection using variational auto-encoders. *International Journal of Computers and Applications*, 45*(3)*, 231–237. https://doi.org/10.1080/1206212X.2022.2143026

Oladejo, B., & Hadžidedić, S. (2021). Electronic records management – a state of the art review. *Records Management Journal*, 31*(1)*, 74–88. https://doi.org/10.1108/RMJ-09-2019-0059