TINJAUAN SISTEMATIS KEAMANAN SISTEM PENGARSIPAN DIGITAL PADA APLIKASI LAYANAN PUBLIK: SYSTEMATIC LITERATURE REVIEW

Nadia Martogi Pasaribu, Isidorus Anung Prabadhi, Rasona Sunara Akbar
Manajemen Teknologi Keimigrasian, Politeknik Imigrasi dan Pemasyarakatan Indonesia
Jl. Satria – Sudirman, Tanah Tinggi, Kec. Tangerang, Kota Tangerang, Banten 15119
psrbnadia13@gmail.com

ABSTRAK

Transformasi digital dalam layanan publik telah mendorong peralihan sistem pengarsipan dari berbasis dokumen fisik menuju sistem digital yang lebih efisien dan terintegrasi. Namun, digitalisasi tersebut juga menimbulkan berbagai risiko keamanan, seperti kebocoran data, akses tidak sah, serta ancaman terhadap integritas dan keberlangsungan arsip. Penelitian ini bertujuan untuk mengidentifikasi, mengevaluasi, dan menyintesis literatur terkait keamanan sistem pengarsipan digital pada aplikasi layanan publik dalam rentang tahun 2021–2026. Metode yang digunakan adalah Systematic Literature Review (SLR) dengan pendekatan PRISMA untuk memastikan proses seleksi dan sintesis literatur dilakukan secara sistematis dan transparan. Hasil penelitian menunjukkan bahwa keamanan arsip digital bersifat multidimensi, yang tidak hanya dipengaruhi oleh aspek teknis, tetapi juga oleh tata kelola, kepatuhan regulasi, serta tingkat kepercayaan pengguna. Tema utama yang ditemukan meliputi autentisitas, integritas, *trust*, serta ketahanan sistem. Selain itu, pemanfaatan teknologi seperti *blockchain*, enkripsi, *hashing*, *cloud computing*, dan kecerdasan buatan terbukti berkontribusi dalam meningkatkan keamanan, meskipun implementasinya masih menghadapi berbagai keterbatasan. Penelitian ini menyimpulkan bahwa keamanan sistem pengarsipan digital memerlukan pendekatan terintegrasi antara kontrol teknis, kebijakan organisasi, dan tata kelola untuk mendukung layanan publik yang aman dan akuntabel.

Kata kunci : *pengarsipan digital, keamanan sistem, arsip elektronik, layanan publik, Systematic Literature Reviewsini*

1. PENDAHULUAN

Transformasi digital telah mendorong perubahan signifikan dalam penyelenggaraan layanan publik, khususnya dalam pengelolaan arsip yang sebelumnya berbasis dokumen fisik menjadi sistem pengarsipan digital yang lebih efisien dan terintegrasi. Penerapan sistem pengarsipan digital memungkinkan proses pencatatan, penyimpanan, distribusi, hingga penemuan kembali arsip dilakukan secara cepat dan sistematis, serta meningkatkan efisiensi dan aksesibilitas informasi [8].

Selain itu, sistem ini berperan penting dalam mendukung transparansi dan akuntabilitas lembaga publik. Namun demikian, digitalisasi arsip juga menghadirkan tantangan baru, terutama terkait aspek keamanan, seperti kebocoran data, akses tidak sah, manipulasi dokumen, serta gangguan terhadap keberlangsungan layanan publik [3][6].

Dalam konteks layanan publik, kegagalan keamanan pada sistem pengarsipan digital tidak hanya berdampak pada aspek teknis, tetapi juga dapat memengaruhi akuntabilitas kelembagaan dan tingkat kepercayaan masyarakat [5].

Dalam konteks layanan publik, keamanan arsip digital tidak hanya berkaitan dengan perlindungan data, tetapi juga mencakup aspek autentisitas, integritas, keterlacakan, serta nilai pembuktian arsip sebagai dasar pertanggungjawaban administratif dan hukum [11][13].

Berbagai penelitian menunjukkan bahwa ancaman terhadap sistem pengarsipan digital tidak hanya bersifat teknis, tetapi juga dipengaruhi oleh faktor tata kelola, regulasi, serta kesiapan sumber daya manusia [12].

Selain itu, perkembangan teknologi seperti *cloud computing*, *blockchain*, dan kecerdasan buatan turut memperluas kompleksitas dalam pengelolaan keamanan arsip digital [2][8][15], sehingga memerlukan pendekatan yang lebih komprehensif dan terintegrasi.

Permasalahan utama dalam penelitian ini adalah belum adanya pemahaman yang komprehensif mengenai bagaimana keamanan sistem pengarsipan digital dikaji dalam literatur, khususnya dalam konteks layanan publik. Perbedaan fokus penelitian—baik dari aspek teknis, tata kelola, maupun regulasi—menunjukkan adanya kesenjangan pengetahuan (*research gap*) yang perlu disintesiskan secara sistematis [4][14].

Hal ini menyebabkan belum adanya gambaran utuh mengenai faktor-faktor yang memengaruhi keamanan arsip digital serta pendekatan yang paling efektif dalam mengelolanya.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengidentifikasi, mengevaluasi, dan menyintesis literatur terkait keamanan sistem pengarsipan digital pada aplikasi layanan publik dalam rentang tahun 2021–2026. Penelitian ini difokuskan pada analisis tema-tema utama, pendekatan keamanan yang digunakan, serta kecenderungan hasil penelitian terkait autentisitas, integritas, kepercayaan (*trust*), regulasi, dan keberlanjutan sistem pengarsipan digital.

Untuk mencapai tujuan tersebut, penelitian ini menggunakan pendekatan *Systematic Literature*

Review (SLR) dengan metode PRISMA. Pendekatan ini dipilih karena mampu memberikan proses penelusuran, seleksi, dan sintesis literatur secara sistematis, transparan, dan dapat dipertanggungjawabkan. Melalui metode ini, diharapkan diperoleh pemahaman yang komprehensif mengenai keamanan sistem pengarsipan digital serta dapat dirumuskan kerangka konseptual yang relevan sebagai dasar pengembangan sistem pengarsipan digital yang aman, andal, dan akuntabel dalam mendukung layanan publik.

2. TINJAUAN PUSTAKA

2.1. Pengarsipan Digital

Pengarsipan digital merupakan proses pengelolaan arsip dalam bentuk elektronik yang mencakup penciptaan, penyimpanan, pengelolaan, serta pemeliharaan arsip digital dalam suatu sistem informasi. Dalam konteks layanan publik, pengarsipan digital berperan sebagai sarana penyimpanan informasi yang mendukung transparansi, akuntabilitas, serta efisiensi dalam pengelolaan administrasi pemerintahan [11].

Arsip digital tidak hanya berfungsi sebagai media penyimpanan data, tetapi juga sebagai bukti administratif dan hukum yang harus dijaga keaslian serta keutuhannya.

Seiring dengan perkembangan teknologi informasi, pengarsipan digital mengalami transformasi dari sistem konvensional menuju sistem berbasis teknologi seperti *cloud computing*, *blockchain*, dan *electronic records management* [8][15].

Hal ini menunjukkan bahwa pengelolaan arsip digital tidak hanya berkaitan dengan penyimpanan data, tetapi juga dengan bagaimana sistem tersebut mampu menjamin keamanan, aksesibilitas, serta keberlanjutan arsip dalam jangka panjang.

2.2. Keamanan Sistem Informasi

Keamanan sistem informasi merupakan upaya untuk melindungi data dan sistem dari ancaman yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi [3].

Dalam konteks pengarsipan digital, keamanan sistem menjadi aspek yang sangat penting karena berkaitan langsung dengan perlindungan data yang bersifat sensitif dan memiliki nilai pembuktian.

Ancaman terhadap sistem pengarsipan digital dapat berupa kebocoran data, akses tidak sah, manipulasi dokumen, serta gangguan terhadap keberlangsungan sistem. Oleh karena itu, diperlukan penerapan kontrol keamanan yang mencakup autentikasi, enkripsi, kontrol akses, serta *audit trail* untuk memastikan bahwa sistem dapat berfungsi secara aman dan andal [6].

Keamanan sistem informasi tidak hanya bergantung pada teknologi, tetapi juga pada kebijakan organisasi dan kesadaran pengguna terhadap pentingnya perlindungan data.

2.3. Autentisitas dan Integritas Arsip Digital

Autentisitas dan integritas merupakan dua konsep utama dalam pengelolaan arsip digital. Autentisitas berkaitan dengan keaslian arsip, yaitu kemampuan sistem untuk menjamin bahwa arsip yang disimpan merupakan arsip yang benar dan tidak mengalami perubahan sejak pertama kali dibuat. Sementara itu, integritas berkaitan dengan keutuhan data, yaitu kemampuan sistem untuk menjaga agar arsip tidak mengalami perubahan atau kerusakan yang tidak sah.

Dalam praktiknya, autentisitas dan integritas arsip digital dijaga melalui penggunaan metadata, sistem *audit trail*, serta teknologi seperti hashing dan enkripsi [13].

Konsep *trustworthy digital repository* juga menjadi penting dalam memastikan bahwa sistem pengarsipan digital dapat dipercaya dalam menjaga keaslian dan keutuhan arsip [5].

Dengan demikian, autentisitas dan integritas menjadi fondasi utama dalam keamanan arsip digital.

2.4. Tata Kelola dan Regulasi Arsip Digital

Tata kelola arsip digital mencakup kebijakan, prosedur, serta standar yang digunakan dalam pengelolaan arsip elektronik. Dalam layanan publik, tata kelola yang baik diperlukan untuk memastikan bahwa pengarsipan digital dilakukan secara sistematis, terstruktur, dan sesuai dengan regulasi yang berlaku [12].

Regulasi memiliki peran penting dalam mengatur bagaimana arsip digital dikelola, disimpan, serta dilindungi dari berbagai risiko. Tanpa adanya regulasi yang jelas, sistem pengarsipan digital berpotensi mengalami kelemahan dalam pengawasan dan pengendalian [14].

Oleh karena itu, integrasi antara teknologi dan kebijakan menjadi hal yang sangat penting dalam membangun sistem pengarsipan digital yang aman dan akuntabel.

2.5. Teknologi dalam Keamanan Arsip Digital

Perkembangan teknologi memberikan berbagai solusi dalam meningkatkan keamanan sistem pengarsipan digital. Teknologi seperti *blockchain* digunakan untuk menjaga keaslian data melalui sistem yang tidak dapat diubah (*immutable*), sedangkan enkripsi digunakan untuk melindungi kerahasiaan data [15].

Selain itu, hashing digunakan untuk memastikan integritas dokumen, sementara *cloud computing* memberikan fleksibilitas dalam penyimpanan dan akses data [8].

Di sisi lain, penggunaan teknologi seperti kecerdasan buatan (*artificial intelligence*) juga mulai diterapkan dalam pengelolaan arsip digital, terutama dalam proses klasifikasi, pencarian, dan analisis data [2].

Meskipun demikian, penggunaan teknologi ini juga memiliki tantangan tersendiri, seperti risiko

keamanan data, ketergantungan sistem, serta isu kepercayaan pengguna. Oleh karena itu, pemanfaatan teknologi harus diimbangi dengan kebijakan dan pengawasan yang memadai.

2.6. Kerangka pemikiran

Berdasarkan kajian teori yang telah diuraikan, dapat disimpulkan bahwa keamanan sistem pengarsipan digital dipengaruhi oleh beberapa faktor utama, yaitu aspek teknis (teknologi keamanan), aspek tata kelola (kebijakan dan regulasi), serta aspek kepercayaan pengguna terhadap sistem [4].

Ketiga aspek tersebut saling berkaitan dan membentuk suatu sistem keamanan yang terintegrasi. Dengan demikian, penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) untuk menganalisis hubungan antara faktor-faktor tersebut dalam konteks layanan publik, sehingga diperoleh pemahaman yang komprehensif mengenai keamanan sistem pengarsipan digital.

2.7. Penelitian terdahulu

Penelitian mengenai keamanan sistem pengarsipan digital telah berkembang pesat dalam beberapa tahun terakhir, dengan fokus yang beragam mulai dari aspek teknis hingga tata kelola. Studi yang dilakukan oleh Aliakbar et al. [1] menunjukkan bahwa pengelolaan arsip elektronik memiliki peran penting dalam mendukung *business continuity* pemerintahan, khususnya dalam menghadapi situasi pasca bencana. Hal ini menegaskan bahwa keamanan arsip digital tidak hanya berkaitan dengan perlindungan data, tetapi juga dengan keberlanjutan layanan publik.

Dalam konteks teknologi, penelitian oleh Dalimunthe dan Ikhwan [3] serta Manurung dan Harliana [10] menunjukkan bahwa penerapan teknik *hashing* dan enkripsi seperti AES mampu meningkatkan integritas dan kerahasiaan arsip digital. Selain itu, studi oleh Stančić dan Bralić [15] serta Wang dan Yang [16] mengkaji penggunaan *blockchain* dalam pengelolaan arsip digital yang mampu meningkatkan *immutability* dan *traceability*, meskipun masih menghadapi tantangan dalam implementasi praktis.

Dari perspektif tata kelola dan kepercayaan, penelitian oleh Faniel et al. [4] dan Frank [5] menekankan pentingnya konsep *trustworthy digital repository* dalam menjaga keaslian dan keandalan arsip digital. Sementara itu, Pacheco et al. [13] menunjukkan bahwa metadata memiliki peran penting dalam menjaga autentisitas arsip digital, khususnya dalam konteks deskripsi arsip.

Penelitian lain juga menyoroti peran teknologi modern dalam pengelolaan arsip digital. Canning dan Jaillant [2] mengkaji pemanfaatan kecerdasan buatan dalam pengolahan arsip pemerintah, sedangkan Julaihi et al. [8] dan Ncube dan Matlala [12] membahas praktik *electronic records management* berbasis *cloud computing* yang memberikan efisiensi, namun juga menimbulkan tantangan baru terkait keamanan dan kepercayaan.

Dari aspek regulasi, Seelakate [14] menegaskan bahwa kerangka hukum yang adaptif sangat diperlukan dalam pengelolaan arsip elektronik di sektor publik. Selain itu, Jaillant [7] juga menunjukkan bahwa aksesibilitas arsip digital harus diimbangi dengan penguatan keamanan agar tidak mengurangi nilai autentisitas dan keutuhan arsip.

Berdasarkan berbagai penelitian tersebut, dapat disimpulkan bahwa keamanan sistem pengarsipan digital merupakan isu multidimensi yang mencakup aspek teknis, tata kelola, regulasi, serta kepercayaan pengguna. Namun demikian, masih terdapat kesenjangan penelitian terkait integrasi antar aspek tersebut, khususnya dalam konteks layanan publik. Oleh karena itu, penelitian ini berupaya mengisi kesenjangan tersebut melalui pendekatan *Systematic Literature Review* untuk menghasilkan pemahaman yang lebih komprehensif mengenai keamanan arsip digital.

Tabel 2. Perbandingan Penelitian Terdahulu

No	Penulis & Tahun	Fokus Penelitian	Metode / Pendekatan	Temuan Utama	Keterbatasan
1	Aliakbar et al. (2026) [1]	Arsip elektronik & business continuity	Studi konseptual	Arsip digital mendukung keberlanjutan layanan pascabencana	Belum membahas aspek teknis keamanan secara detail
2	Canning & Jaillant (2025) [2]	AI dalam arsip pemerintah	Analisis konseptual	AI meningkatkan efisiensi pengelolaan arsip	Risiko keamanan dan etika belum optimal
3	Dalimunthe & Ikhwan (2026) [3]	Hashing untuk integritas data	Implementasi sistem	Hashing menjaga keutuhan data arsip	Terbatas pada aspek teknis
4	Faniel et al. (2024) [4]	Trust pada repository digital	Studi empiris	Kepercayaan pengguna penting dalam sistem arsip	Tidak membahas aspek regulasi
5	Frank (2022) [5]	Trustworthy digital repository	Analisis audit	Standar repository penting untuk keamanan	Fokus pada audit, bukan implementasi luas
6	Indraka & Romli (2024) [6]	Enkripsi AES pada arsip	Implementasi	AES efektif menjaga kerahasiaan data	Tidak membahas integrasi sistem
7	Jaillant (2022) [7]	Aksesibilitas arsip digital	Studi literatur	Akses arsip perlu diimbangi keamanan	Kurang fokus pada teknologi
8	Julaihi et al. (2024) [8]	Cloud record-keeping	Studi sistem	Cloud meningkatkan efisiensi penyimpanan	Risiko keamanan dan trust

No	Penulis & Tahun	Fokus Penelitian	Metode / Pendekatan	Temuan Utama	Keterbatasan
9	Kareklas & Chaleplioglou (2025) [9]	Blockchain dalam arsip	Analisis konseptual	Blockchain meningkatkan immutability	Implementasi kompleks
10	Manurung & Harliana (2025) [10]	Enkripsi arsip digital	Implementasi	Enkripsi meningkatkan keamanan dokumen	Fokus terbatas pada sistem lokal
11	McLeod & Lomas (2023) [11]	Digital records sebagai evidence	Studi konseptual	Arsip digital sebagai bukti hukum	Tidak membahas kontrol keamanan
12	Ncube & Matlala (2024) [12]	Electronic records management	Studi literatur	ERM dipengaruhi faktor organisasi	Kurang fokus pada teknologi
13	Pacheco et al. (2023) [13]	Metadata & autentisitas	Analisis model	Metadata penting untuk keaslian arsip	Tidak membahas keamanan sistem
s14	Seelakate (2025) [14]	Regulasi arsip elektronik	Studi kebijakan	Regulasi penting dalam keamanan arsip	Terbatas pada konteks negara tertentu
15	Stančić & Bralić (2021) [15]	Blockchain arsip digital	Analisis teknologi	Blockchain meningkatkan integritas	Keterbatasan fleksibilitas data
16	Wang & Yang (2021) [16]	Blockchain recordkeeping	Studi pengembangan	Blockchain meningkatkan traceability	Implementasi belum luas

3. METODE PENELITIAN

Penelitian ini merupakan *Systematic Literature Review* (SLR) dengan menggunakan protokol PRISMA 2020 (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*). Pendekatan ini digunakan untuk memastikan proses identifikasi, seleksi, dan sintesis literatur dilakukan secara sistematis, transparan, dan dapat ditelusuri kembali. Proses penelitian diklasifikasikan ke dalam beberapa tahap sebagai berikut.

3.1. Tahap 1: Kriteria Kelayakan

Kriteria inklusi (*inclusion criteria*) digunakan untuk menentukan literatur yang relevan dengan topik penelitian, yaitu:

a. *IC1:* Artikel penelitian asli yang dipublikasikan dalam bahasa Inggris atau bahasa Indonesia.
b. *IC2*: Artikel diterbitkan dalam rentang tahun 2021–2026.
c. *IC3*: Artikel membahas keamanan sistem pengarsipan digital, *electronic records management*, *digital repository*, atau *recordkeeping system*.
d. *IC4*: Artikel memiliki fokus pada aspek autentisitas, integritas, tata kelola, teknologi keamanan, atau keberlanjutan arsip digital.

Artikel yang tidak memenuhi kriteria tersebut, bersifat opini, atau tidak memiliki metodologi yang jelas tidak dimasukkan dalam analisis.

3.2. Tahap 2: Sumber Literatur

Pencarian literatur dilakukan pada beberapa basis data ilmiah, yaitu Google Scholar, IEEE Xplore, Scopus, dan Crossref. Selain itu, metode *snowballing* juga diterapkan dengan menelusuri daftar pustaka dari artikel yang telah memenuhi kriteria untuk menemukan literatur tambahan yang relevan

3.3. Tahap 3: Pemilihan Literatur

Proses pencarian menggunakan kombinasi kata kunci, antara lain: “digital archive security”, “electronic records management”, “trusted digital repository”, “blockchain recordkeeping”, “cloud record-keeping”, “public sector records”. Operator Boolean yang digunakan adalah: ("digital archive security" OR "electronic records management") AND ("blockchain" OR "cloud" OR "security") AND ("public sector" OR "government"). Proses penyaringan dilakukan secara bertahap melalui: Identifikasi (judul), Screening (abstrak), Eligibility (teks lengkap), Inclusion (artikel terpilih).

3.4. Tahap 4: Pengumpulan Data

Data dikumpulkan menggunakan formulir ekstraksi data terstruktur yang mencakup informasi seperti judul, penulis, tahun, metode penelitian, fokus kajian, serta temuan utama. Berdasarkan hasil penelusuran, diperoleh sejumlah artikel yang kemudian disaring sesuai kriteria. Artikel yang lolos seleksi selanjutnya dianalisis lebih lanjut dan disajikan dalam bentuk tabel sintesis (Tabel 1).

Tabel 1. Hasil Seleksi Literatur

Sumber	Studi Ditemukan	Kandidat	Dipilih
Google Scholar	45	18	6
IEEE Xplore	18	9	4
Scopus	112	7	3
Crossref	15	10	3
Total	**90**	**44**	**16**

Berdasarkan Tabel 1, proses penelusuran literatur menghasilkan 90 artikel dari berbagai basis data ilmiah. Setelah dilakukan penyaringan berdasarkan judul dan abstrak, diperoleh 44 artikel yang memenuhi kriteria awal. Selanjutnya, melalui tahap evaluasi kelayakan dan kualitas, sebanyak 16 artikel dipilih untuk dianalisis secara mendalam dalam penelitian ini.

3.5. Tahap 5: Pemilihan Item Data

Data yang diekstraksi dalam penelitian ini meliputi aspek-aspek utama yang berkaitan dengan keamanan sistem pengarsipan digital, yaitu arsitektur sistem, teknologi yang digunakan (seperti enkripsi, hashing, blockchain, dan *cloud computing*), pendekatan autentisitas dan integritas arsip, tata kelola dan regulasi, serta ketahanan sistem (*continuity* dan *disaster recovery*). Selain itu, data juga mencakup metode penelitian, konteks penerapan, serta temuan utama dari setiap artikel yang dianalisis.

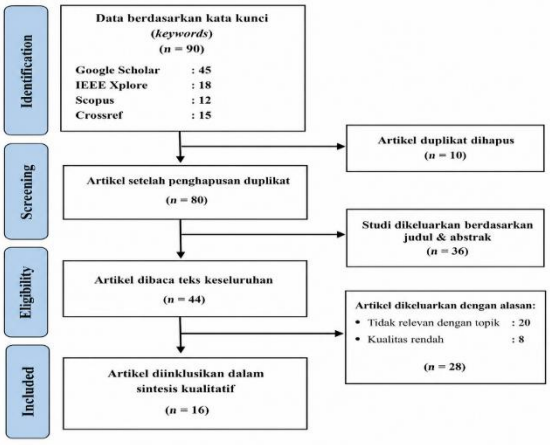
Untuk memastikan fokus analisis yang terarah, penelitian ini merumuskan beberapa pertanyaan penelitian (*Research Questions*) yang disajikan pada Tabel 2.

Tabel 2. Pertanyaan Penelitian

Kode	Pertanyaan Penelitian
RQ1	Apa saja pendekatan keamanan yang digunakan dalam sistem pengarsipan digital (teknologi, autentisitas, integritas)?
RQ2	Bagaimana peran tata kelola dan regulasi dalam mendukung keamanan arsip digital pada layanan publik?
RQ3	Teknologi apa yang paling banyak digunakan dalam pengamanan arsip digital dan bagaimana efektivitasnya?
RQ4	Apa saja research gap yang ditemukan dalam pengelolaan keamanan sistem pengarsipan digital?

Berdasarkan Tabel 2, pertanyaan penelitian difokuskan untuk mengidentifikasi pendekatan keamanan, peran tata kelola, pemanfaatan teknologi, serta kesenjangan penelitian yang masih terdapat dalam sistem pengarsipan digital. Pertanyaan-pertanyaan ini menjadi dasar dalam proses sintesis dan analisis literatur untuk menghasilkan pemahaman yang komprehensif mengenai keamanan arsip digital dalam konteks layanan publik..

4. HASIL DAN PEMBAHASAN



Gambar 1. Diagram Alur Seleksi Literatur PRISMA 2020

Dari 44 artikel yang diinklusikan, sebanyak 16 artikel dengan skor kualitas tertinggi dipilih untuk dilakukan sintesis secara mendalam. Diagram alur seleksi PRISMA 2020 disajikan pada Gambar 1, sedangkan ringkasan artikel terpilih disajikan pada Tabel 4.

4.1. Hasil seleksi Literatur

Bagian ini menyajikan hasil seleksi artikel yang relevan dengan tema keamanan sistem pengarsipan digital pada aplikasi layanan publik. Proses seleksi dilakukan menggunakan pendekatan PRISMA melalui tahapan *identification*, *screening*, *eligibility*, dan *inclusion*. Berdasarkan hasil seleksi, diperoleh 16 artikel yang memenuhi kriteria inklusi dan digunakan sebagai sumber utama dalam penelitian ini.

Artikel yang terpilih berasal dari rentang publikasi tahun 2021 sampai 2026 dan menunjukkan adanya peningkatan perhatian akademik terhadap isu keamanan arsip digital. Literatur yang dipilih mencakup berbagai tema, seperti *trustworthy digital repository* [5], *electronic records management* [12], *metadata authenticity* [13], *blockchain recordkeeping* [15], *cloud record-keeping* [8], hingga penggunaan kecerdasan buatan dalam pengelolaan arsip pemerintah [2].

Temuan ini menunjukkan bahwa kajian keamanan arsip digital berkembang secara multidimensi, mencakup aspek teknis, tata kelola, serta kepercayaan terhadap sistem.

Daftar artikel yang memenuhi kriteria inklusi disajikan pada Tabel 3 berikut.

Tabel 3. Daftar Jurnal Terpilih

No.	Judul	Tahun
1	Digital Archives Relying on Blockchain: Overcoming the Limitations of Data Immutability	2021
2	Research and Development of Blockchain Recordkeeping at the National Archives of Korea	2021
3	Risk in Trustworthy Digital Repository Audit and Certification	2022
4	How Can We Make Born-Digital and Digitised Archives More Accessible? Identifying Obstacles and Solutions	2022
5	Record DNA: Reconceptualising Digital Records as the Future Evidence Base	2023
6	A Metadata Model for Authenticity in Digital Archival Descriptions	2023
7	Digital Record-Keeping Practices: Electronic Records and Archives in the Cloud	2024
8	Electronic Records Management amidst the Seismic Shift in the Dynamic Infosphere	2024
9	Keamanan Arsip Kelurahan Bumijo Menggunakan Metode Advanced Encryption Standard (AES 128) Berbasis Web	2024
10	An Empirical Examination of Data Reuser Trust in a Digital Repository	2024
11	AI to Review Government Records: New Work to Unlock Historically Significant Digital Records	2025

No.	Judul	Tahun
12	Innovations and Contradictions in Applying Blockchain Technology in Records Management under GDPR	2025
13	Legislation and Electronic Records Management in the Thai Public Sector: Challenges and Opportunities in the Digital Age	2025
14	Implementasi Enkripsi AES dalam Sistem Arsip Surat di KONI Provinsi Sumatera Utara	2025
15	Implementasi Sistem Informasi Pengelolaan Arsip Elektronik dengan Algoritma Hashing untuk Integritas Data	2026
16	Arsip Elektronik sebagai Tulang Punggung Kelangsungan Pemerintahan Pascabencana	2026

Berdasarkan Tabel 3, perkembangan literatur menunjukkan adanya peningkatan perhatian terhadap keamanan arsip digital pada periode 2024 sampai 2025. Penelitian pada periode awal lebih banyak membahas isu *trust*, audit *repository*, dan akses arsip digital, sedangkan penelitian terbaru mulai menekankan aspek autentisitas metada, regulasi pengelolaan arsip elektronik, *blockchain, artificial intelligence*, enkripsi, *hashing*, serta ketahanan arsip digital terhadap ancaman siber

4.2. Sintesis Literatur

Sintesis literatur dilakukan terhadap artikel-artikel yang telah memenuhi kriteria inklusi untuk mengidentifikasi pola, tema dominan, pendekatan penelitian serta temuan utama terkait keamanan sistem pengarsipan digital pada layanan publik. Analisis dilakukan dengan meninjau fokus kajian, metode penelitian, konteks objek penelitian, dan hasil utama dari setiap artikel.

Hasil sintesis literatur disajikan pada Tabel 4 berikut.

Tabel 4. Sintesis Literatur Terpilih

Penulis	Fokus Kajian	Objek/Konteks	Metode	Temuan Utama
Stančić & Bralić (2021)	Blockchain untuk arsip digital dan isu immutability	Arsip digital dan preservasi jangka panjang	Analisis konseptual	Blockchain meningkatkan jejak autentik, tetapi arsip tetap memerlukan fleksibilitas pembaruan metadata dan relasi antardokumen.
Wang & Yang (2021)	Blockchain recordkeeping dan audit trail	National Archives of Korea	Laporan pengembangan dan R&D	Blockchain dipakai untuk memperkuat audit trail dan autentisitas arsip audiovisual, namun implementasinya tetap menuntut desain recordkeeping yang matang.
Frank (2022)	Risiko pada trustworthy digital repository	Audit dan sertifikasi repository digital	Wawancara dan analisis dokumen	Risiko arsip digital tidak hanya teknis, tetapi juga sosial dan organisasional. Audit repository perlu menilai tata kelola, proses, dan persepsi risiko.
Jaillant (2022)	Akses arsip born-digital dan hambatan keamanan	Born-digital dan digitised archives	Studi analitis	Keterbatasan akses, privasi, hak cipta, dan masalah teknis menunjukkan bahwa availability arsip digital harus diseimbangkan dengan kontrol keamanan dan kepatuhan.
McLeod & Lomas (2023)	Record DNA dan bukti digital	Konsep digital records sebagai evidence base	Analisis konseptual	Keamanan arsip harus menjaga bukti digital agar tetap autentik, kontekstual, dan dapat dipakai sebagai dasar akuntabilitas di masa depan.
Pacheco et al. (2023)	Metadata model untuk authenticity	Deskripsi arsip digital	Mixed methods	Metadata yang kaya dan terstruktur menjadi kunci pembuktian autentisitas dan trustworthiness arsip digital.
Julaihi et al. (2024)	Cloud record-keeping dan kepercayaan	Electronic records and archives in the cloud	Literature review	Cloud memperluas efisiensi penyimpanan, tetapi menimbulkan isu trust, kedaulatan data, kepatuhan, dan preservasi jangka panjang.
Ncube & Matlala (2024)	Kesenjangan e-records management di sektor publik	Departemen pemerintah di Afrika Selatan	Systematic literature review	Masalah utama berada pada keterampilan SDM, dukungan manajemen, kebijakan, dan kepatuhan. Faktor tata kelola sama pentingnya dengan teknologi.
Indraka & Romli (2024)	Enkripsi AES untuk keamanan arsip web	Arsip Kelurahan Bumijo	Pengembangan sistem dan pengujian	AES-128 efektif meningkatkan kerahasiaan file arsip berbasis web, meskipun evaluasi pengguna menunjukkan sistem masih perlu penyempurnaan.
Faniel, Robert, & Yakel (2024)	Trust pengguna pada digital repository	Data repository	Survei kuantitatif	Kepercayaan pengguna dipengaruhi oleh integrity, identification, dan structural assurance. Artinya, keamanan repository juga ditentukan oleh persepsi pengguna.

Penulis	Fokus Kajian	Objek/Konteks	Metode	Temuan Utama
Canning & Jaillant (2025)	AI untuk seleksi dan pengelolaan government records	Government records dan born-digital records	Studi konseptual terapan	AI dapat mempercepat appraisal dan pengelolaan records, tetapi implementasinya harus tetap menjaga kontrol, akuntabilitas, dan preservasi jangka panjang.
Kareklas & Chaleplioglou (2025)	Blockchain dan kontradiksi dengan GDPR	Records management dan perlindungan data	Literature review	Blockchain menjanjikan keamanan dan integritas tinggi, tetapi berpotensi berbenturan dengan prinsip perlindungan data dan hak penghapusan.
Seelakate (2025)	Regulasi e-records di sektor publik	Sektor publik Thailand	Analisis legislasi	Kerangka hukum yang mutakhir menjadi fondasi pengelolaan arsip elektronik yang aman, akuntabel, dan berkelanjutan.
Manurung & Harliana (2025)	Enkripsi AES pada sistem arsip surat	KONI Provinsi Sumatera Utara	Studi kasus deskriptif	AES efektif melindungi kerahasiaan surat digital dan memperkuat login terproteksi, tetapi pengelolaan kunci enkripsi masih menjadi titik rawan.
Dalimunthe & Ikhwan (2026)	Hashing SHA-256 untuk integritas arsip	Sistem informasi pengelolaan arsip elektronik	Pengembangan sistem dan pengujian	Hashing mampu mendeteksi perubahan sekecil apa pun pada dokumen, sehingga sangat relevan untuk verifikasi keaslian dan akuntabilitas arsip digital.
Aliakbar et al. (2026)	Arsip elektronik untuk continuity pascabencana	Pemerintahan pascabencana	Studi kasus dan kajian literatur	Cloud storage, alih media, dan kesiapan kebijakan mendukung continuity pemerintahan, tetapi implementasi masih terkendala budaya organisasi, biaya, dan regulasi.

Berdasarkan hasil sintesis pada Tabel 4, keamanan arsip digital tidak lagi dipahami hanya sebagai perlindungan file atau server, tetapi telah berkembang menjadi pendekatan multidimensi yang mencakup *authenticity*, *integrity*, *trust*, *regulatory compliance*, dan *continuity* [5][13].

Literatur menunjukkan bahwa keamanan arsip digital berkaitan erat dengan kemampuan sistem dalam menjaga keaslian, keutuhan, keterlacakan, serta nilai pembuktian arsip digital secara berkelanjutan.

Hasil sintesis juga menunjukkan adanya perkembangan fokus penelitian dari waktu ke waktu. Literatur pada periode awal lebih banyak membahas *trustworthy digital repository*, audit repository, dan akses arsip digital [5][7].

Sementara itu, penelitian terbaru mulai menekankan penggunaan teknologi seperti *blockchain*, *cloud record-keeping*, *artificial intelligence*, enkripsi AES, hashing SHA-256, serta *disaster recovery* dalam pengelolaan arsip digital layanan publik [2][8][10][15].

Selain aspek teknis, literatur juga menunjukkan bahwa tata kelola organisasi, regulasi, kompetensi sumber daya manusia, serta tingkat kepercayaan pengguna menjadi faktor yang sangat memengaruhi keamanan sistem pengarsipan digital [12][14].

Dengan demikian, keamanan arsip digital tidak dapat dipahami hanya dari sisi teknologi, tetapi juga harus dipandang sebagai bagian dari tata kelola layanan publik secara menyeluruh.

4.3. Autentisitas, Integritas, dan Trust

Hasil sintesis menunjukkan bahwa autentisitas dan integritas merupakan aspek paling fundamental dalam keamanan sistem pengarsipan digital. Arsip digital tidak hanya harus terlindungi dari akses tidak sah, tetapi juga harus mampu mempertahankan keaslian, konteks, serta nilai pembuktiannya dalam jangka panjang [13].

Dalam konteks ini, konsep *trustworthy digital repository* menjadi penting karena menekankan bahwa keamanan arsip digital berkaitan erat dengan tingkat kepercayaan terhadap sistem [5].

Beberapa penelitian menunjukkan bahwa metadata memiliki peran penting dalam menjaga autentisitas arsip, sedangkan teknologi seperti *hashing* digunakan untuk memastikan integritas dokumen [3][13].

Selain itu, persepsi kepercayaan pengguna terhadap sistem juga dipengaruhi oleh kemampuan sistem dalam menjaga konsistensi data serta menyediakan *audit trail* yang transparan [4].

Dengan demikian, keamanan arsip digital tidak hanya bersifat teknis, tetapi juga berkaitan dengan aspek kepercayaan pengguna terhadap sistem pengarsipan digital secara keseluruhan.

4.4. Tata kelola dan Regulasi

Selain aspek teknis, keamanan arsip digital sangat dipengaruhi oleh tata kelola organisasi dan regulasi yang berlaku. Hasil penelitian menunjukkan bahwa lemahnya kebijakan, kurangnya dukungan manajemen, serta keterbatasan kompetensi sumber daya manusia menjadi faktor utama yang menghambat implementasi sistem pengarsipan digital yang aman [12].

Regulasi yang tidak mutakhir juga dapat menyebabkan kesenjangan dalam pengelolaan arsip elektronik, terutama dalam menghadapi perkembangan teknologi yang cepat [14].

Oleh karena itu, diperlukan kerangka kebijakan yang jelas, standar pengelolaan arsip digital, serta mekanisme pengawasan yang efektif. Hal ini menunjukkan bahwa keamanan arsip digital harus dipandang sebagai bagian dari sistem tata kelola layanan publik secara keseluruhan, tidak hanya sebagai persoalan teknis semata.

4.5. Teknologi Pengamanan Arsip Digital

Perkembangan teknologi memberikan berbagai solusi dalam meningkatkan keamanan sistem pengarsipan digital. *Blockchain* menjadi salah satu teknologi yang banyak dibahas karena mampu meningkatkan *immutability* dan *audit trail* arsip digital [15].

Namun demikian, implementasi *blockchain* masih memiliki keterbatasan, terutama terkait fleksibilitas data dan kepatuhan terhadap regulasi perlindungan data [9].

Selain itu, teknologi enkripsi seperti AES digunakan untuk menjaga kerahasiaan dokumen, sedangkan *hashing* seperti SHA-256 digunakan untuk memastikan integritas data [6][10].

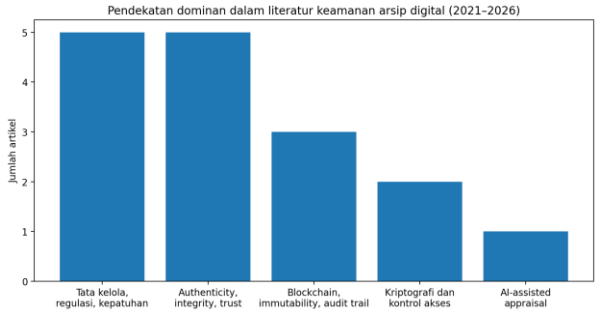
Di sisi lain, penggunaan *cloud computing* dan *artificial intelligence* memberikan efisiensi dalam pengelolaan arsip, tetapi juga menimbulkan tantangan baru terkait keamanan, kepercayaan, dan kedaulatan data [2][8].

Oleh karena itu, penggunaan teknologi harus disertai dengan evaluasi risiko serta penguatan kebijakan yang memadai agar implementasinya dapat berjalan secara aman dan berkelanjutan.

Tabel 5 Ringkasan pendekatan pengujian keamanan yang paling dominan

No.	Pendekatan dominan	Jumlah artikel	Contoh studi
1	Tata kelola, regulasi, dan kepatuhan	5	Jaillant (2022); Julaihi et al. (2024); Ncube & Matlala (2024); Seelakate (2025); Aliakbar et al. (2026)
2	Authenticity, integrity, dan trust	5	Frank (2022); McLeod & Lomas (2023); Pacheco et al. (2023); Faniel et al. (2024); Dalimunthe & Ikhwan (2026)
3	Blockchain, immutability, dan audit trail	3	Stančić & Bralić (2021); Wang & Yang (2021); Kareklas & Chaleplioglou (2025)
4	Kriptografi dan kontrol akses	2	Indraka & Romli (2024); Manurung & Harliana (2025)
5	AI-assisted appraisal	1	Canning & Jaillant (2025)

Tabel 5 memperlihatkan bahwa literatur mutakhir tidak lagi memandang pengujian keamanan arsip digital hanya sebagai persoalan enkripsi atau proteksi file semata. Sebaliknya, pengujian semakin diarahkan pada kemampuan sistem untuk memenuhi prinsip kepatuhan, akuntabilitas, autentisitas, integritas, serta kepercayaan pengguna [13][14]. Temuan ini menegaskan bahwa keamanan layanan pengarsipan digital bersifat sosioteknis karena mengintegrasikan kontrol teknis dengan kebijakan, tata kelola, serta pembuktian arsip sebagai *evidence base* [5][11].



Gambar 1. Distribusi pendekatan dominan dalam literatur keamanan arsip digital

Selain itu, pendekatan berbasis teknologi seperti *blockchain*, enkripsi, *hashing*, *cloud computing*, dan kecerdasan buatan juga menunjukkan kontribusi yang signifikan dalam mendukung keamanan arsip digital [2][8][10][15].

Namun demikian, proporsi pendekatan teknologi masih berada di bawah aspek tata kelola, yang mengindikasikan bahwa keberhasilan implementasi sistem pengarsipan digital sangat bergantung pada keseimbangan antara teknologi dan kebijakan organisasi [12][14].

Temuan ini menguatkan hasil sintesis sebelumnya bahwa keamanan arsip digital bersifat multidimensi dan memerlukan integrasi antara aspek teknis, tata kelola, serta regulasi [5][13].

Dengan demikian, pengembangan sistem pengarsipan digital tidak dapat hanya berfokus pada inovasi teknologi, tetapi juga harus memperhatikan kesiapan organisasi, kompetensi sumber daya manusia, serta mekanisme pengawasan yang berkelanjutan.

pengarsipan digital tidak dapat hanya berfokus pada inovasi teknologi, tetapi juga harus memperhatikan kesiapan organisasi, kompetensi sumber daya manusia, serta mekanisme pengawasan yang berkelanjutan

4.6. Continuity dan Disaster Recovery

Literatur terbaru menunjukkan bahwa aspek *continuity* dan *disaster recovery* menjadi bagian penting dalam keamanan arsip digital, terutama dalam konteks layanan publik [1].

Ancaman seperti serangan siber, bencana alam, dan gangguan sistem dapat menyebabkan hilangnya data atau terganggunya layanan publik. Oleh karena itu, sistem pengarsipan digital harus memiliki mekanisme cadangan (*backup system*), pemulihan data (*recovery system*), serta kebijakan keberlanjutan yang jelas.

Penggunaan teknologi seperti *cloud storage* dan *digital preservation* dapat mendukung keberlangsungan layanan, namun tetap memerlukan dukungan kebijakan dan kesiapan organisasi [8][12].

Dengan demikian, keamanan arsip digital tidak hanya berfokus pada perlindungan data, tetapi juga pada keberlanjutan layanan publik secara keseluruhan

4.7. Implikasi Penelitian

Berdasarkan hasil sintesis dan pembahasan literatur, penelitian ini menunjukkan bahwa keamanan sistem pengarsipan digital pada layanan publik memerlukan pendekatan yang terintegrasi antara aspek teknis, tata kelola, dan regulasi [5][12].

Keamanan tidak dapat hanya bergantung pada penerapan teknologi, tetapi juga harus didukung oleh kebijakan organisasi, kompetensi sumber daya manusia, serta sistem pengawasan yang efektif. Secara teoritis, penelitian ini memperluas pemahaman mengenai keamanan arsip digital sebagai konsep multidimensi yang mencakup autentisitas, integritas, kepercayaan, dan keberlanjutan sistem [13][14].

Secara praktis, hasil penelitian ini dapat menjadi dasar bagi instansi pemerintah dalam merancang sistem pengarsipan digital yang aman dan andal melalui penerapan metadata, *audit trail*, enkripsi, serta pemanfaatan teknologi seperti *blockchain* secara selektif. Selain itu, penelitian ini mengidentifikasi bahwa kajian empiris terkait keamanan arsip digital masih terbatas, sehingga penelitian selanjutnya disarankan untuk melakukan pengujian langsung pada sistem pengarsipan digital guna mengevaluasi efektivitas kontrol keamanan, integritas data, serta ketahanan sistem terhadap ancaman siber dan gangguan operasional.

4.8. Hasil

Berdasarkan hasil sintesis literatur, penelitian ini menunjukkan bahwa keamanan sistem pengarsipan digital memiliki peran penting dalam mendukung efektivitas dan keberlanjutan layanan publik. Keamanan arsip digital tidak hanya ditentukan oleh penerapan teknologi, tetapi juga dipengaruhi oleh kesesuaian sistem dengan kebutuhan organisasi, kesiapan sumber daya manusia, serta dukungan tata kelola dan regulasi yang memadai [12][14].

Sistem pengarsipan digital yang dirancang secara terintegrasi mampu menjaga autentisitas, integritas, transparansi, dan akuntabilitas informasi publik [13].

Namun demikian, efektivitas penerapan teknologi seperti *cloud computing*, *blockchain*, dan enkripsi tidak selalu konsisten apabila tidak diimbangi dengan kebijakan yang jelas dan mekanisme pengawasan yang efektif [2][8][15].

Secara teoritis, penelitian ini menegaskan bahwa keamanan arsip digital merupakan konsep multidimensi yang mencakup aspek teknis, tata kelola, kepercayaan (*trust*), kepatuhan regulasi, serta ketahanan sistem [5].

Secara praktis, hasil penelitian ini memberikan implikasi bagi instansi pemerintah untuk mengembangkan sistem pengarsipan digital melalui penerapan metadata, *audit trail*, enkripsi, *hashing*, serta pemanfaatan teknologi secara selektif sesuai kebutuhan organisasi. Selain itu, diperlukan penguatan kebijakan yang adaptif, peningkatan kapasitas sumber daya manusia, serta penerapan strategi *backup* dan *disaster recovery* guna menjamin keberlanjutan sistem. Untuk penelitian selanjutnya, disarankan dilakukan kajian empiris guna menguji efektivitas implementasi keamanan sistem pengarsipan digital dalam menghadapi ancaman siber dan dinamika layanan publik..

5. KESIMPULAN DAN SARAN

Keamanan sistem pengarsipan digital memiliki peran yang sangat penting dalam mendukung keberlangsungan layanan publik. Berdasarkan hasil analisis literatur, keamanan arsip digital tidak hanya ditentukan oleh aspek teknis, tetapi juga dipengaruhi oleh tata kelola organisasi, regulasi, serta tingkat kepercayaan pengguna terhadap sistem [12][14].

Hasil kajian menunjukkan bahwa keamanan arsip digital telah berkembang dari pendekatan teknis menjadi pendekatan multidimensi yang mencakup autentisitas, integritas, *trust*, kepatuhan regulasi, serta ketahanan sistem [5][13].

Pemanfaatan teknologi seperti *blockchain*, enkripsi, *hashing*, *cloud computing*, dan kecerdasan buatan terbukti mampu memperkuat keamanan, namun efektivitasnya sangat bergantung pada dukungan kebijakan, kesiapan organisasi, serta kompetensi sumber daya manusia [2][8][10][15].

Oleh karena itu, pengembangan sistem pengarsipan digital perlu dilakukan secara terintegrasi dengan mengombinasikan kontrol teknis, penguatan tata kelola, serta regulasi yang adaptif guna menciptakan sistem yang aman, andal, dan akuntabel. Untuk penelitian selanjutnya, disarankan dilakukan kajian empiris atau pengujian langsung pada sistem pengarsipan digital di instansi pemerintah guna mengevaluasi efektivitas implementasi keamanan, integritas data, serta ketahanan sistem terhadap ancaman siber dan gangguan operasional.

DAFTAR PUSTAKA

[1] Aliakbar, M. Z., Marpaung, B. B. P. P., Ayudhistira, J. Z., Syafiq, M. N., dan Fadil, R., 2026. Arsip elektronik sebagai pendukung *business continuity* pemerintahan pascabencana. Khazanah: Jurnal Pengembangan Kearsipan.Ding, K. and Jiang, P., 2017. RFID-

based production data analysis in an IoT-enabled smart job-shop. *IEEE/CAA Journal of Automatica Sinica*.

[2] Canning, D. dan Jaillant, L., 2025. AI to review government records: New work to unlock historically significant digital records. *AI & Society*, 40, pp. 4433–4445.

[3] Dalimunthe, J. K. dan Ikhwan, A., 2026. Implementasi sistem informasi pengelolaan arsip elektronik dengan algoritma hashing untuk integritas data. *CESS (Journal of Computer Engineering, System and Science)*, 11(1), pp. 41–50.

[4] Faniel, I. M., Robert, L. P., Jr., dan Yakel, E., 2024. An empirical examination of data reuser trust in a digital repository. *Proceedings of the Association for Information Science and Technology*.

[5] Frank, R. D., 2022. Risk in trustworthy digital repository audit and certification. *Archival Science*, 22, pp. 43–73.

[6] Indraka, A. P. dan Romli, M. A., 2024. Keamanan arsip Kelurahan Bumijo menggunakan metode Advanced Encryption Standard (AES 128) berbasis web. *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, 5(1), pp. 232–241.

[7] Jaillant, L., 2022. How can we make born-digital and digitised archives more accessible? Identifying obstacles and solutions. *Archives and Records*, 43(2), pp. 123–141.

[8] Julaihi, A. K., Jamaludin, S. N., Chik, N. K., dan Johare, R., 2024. Digital record-keeping practices: Electronic records and archives in the cloud. *International Journal of Engineering Trends and Technology*, 72(10), pp. 267–281.

[9] Kareklas, N. dan Chaleplioglou, A., 2025. Innovations and contradictions in applying blockchain technology in records management. *Records Management Journal*.

[10] Manurung, E. V. dan Harliana, P., 2025. Implementasi enkripsi AES dalam sistem arsip surat di KONI Provinsi Sumatera Utara. *Infomatek*, 27(1), pp. 95–100.

[11] McLeod, J. dan Lomas, E., 2023. Record DNA: Reconceptualising digital records as the future evidence base. *Archival Science*.

[12] Ncube, T. R. dan Matlala, M. E., 2024. Electronic records management amidst the seismic shift in the dynamic infosphere. *Records Management Journal*, 34, pp. 1–16.

[13] Pacheco, A., da Silva, C. G., dan de Freitas, M. C. V., 2023. A metadata model for authenticity in digital archival descriptions. *Archival Science*, 23, pp. 629–673.

[14] Seelakate, P., 2025. Legislation and electronic records management in the Thai public sector: Challenges and opportunities in the digital age. *Record and Library Journal*, 11(2), pp. 330–342.

[15] Stančić, H. dan Bralić, V., 2021. Digital archives relying on blockchain: Overcoming the limitations of data immutability. *Computers*, 10(8).

[16] Wang, H. dan Yang, D., 2021. Research and development of blockchain recordkeeping at the National Archives of Korea. *Computers*, 10(8).