

Preservation as a Service for Trust (PaaST) dalam Penjagaan Keaslian dan Keamanan Arsip Digital

Nurul Habib Romadhan¹, Tamara Adriani Salim²

^{1,2}Departemen Ilmu Perpustakaan dan Informasi, Fakultas Ilmu Pengetahuan Budaya, Universitas Indonesia, Kota Depok, Indonesia
Email: ¹nurul.habib@ui.ac.id

Abstrak

Preservation as a Service for Trust (PaaST) merupakan pendekatan inovatif dalam pelestarian arsip digital yang mengintegrasikan fungsi teknis, kebijakan, dan audit ke dalam model layanan terkelola berbasis kepercayaan (*trust-based service model*). Dalam topik meningkatnya volume data digital dan risiko degradasi format maupun keamanan siber, PaaST hadir untuk memastikan keaslian (*authenticity*), keutuhan (*integrity*), dan keterpercayaan (*trustworthiness*) arsip jangka panjang. Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) untuk mengidentifikasi tren, praktik, dan tantangan dalam implementasi PaaST dari tahun 2019 hingga 2025. Proses pencarian literatur dilakukan pada berbagai basis data akademik dan dokumen institusional terkait standar pelestarian digital seperti OAIS (ISO 14721), sertifikasi repositori terpercaya ISO 16363, serta penerapan teknologi kriptografi dan blockchain untuk pembuktian keaslian arsip. Hasil tinjauan menunjukkan bahwa model layanan pelestarian digital terkelola semakin banyak diadopsi oleh institusi arsip dan perpustakaan besar karena dinilai efisien, aman, dan berorientasi keberlanjutan. Penggunaan mekanisme *fixity check*, *digital signature*, serta *timestamping* (baik berbasis blockchain maupun non-blockchain) terbukti meningkatkan integritas data dan nilai pembuktian arsip. Namun, tantangan utama yang masih dihadapi adalah keberlanjutan finansial, kepatuhan terhadap standar, dan keterbatasan sumber daya teknis di lembaga kecil. Artikel ini menegaskan pentingnya sinergi antara teknologi, kebijakan kelembagaan, dan tata kelola jangka panjang dalam penerapan PaaST.

Kata Kunci: Blockchain, ISO 16363, Keamanan Arsip, OAIS, Paast, Pelestarian Digital.

Abstract

Preservation as a Service for Trust (PaaST) is an innovative approach to digital archive preservation that integrates technical, policy, and audit functions into a trust-based managed service model. Given the increasing volume of digital data and the risks of format degradation and cybersecurity, PaaST exists to ensure the authenticity, integrity, and trustworthiness of long-term archives. This study uses a Systematic Literature Review (SLR) approach to identify trends, practices, and challenges in PaaST implementation from 2019 to 2025. The literature search process was conducted on various academic databases and institutional documents related to digital preservation standards such as OAIS (ISO 14721), ISO 16363 trusted repository certification, and the application of cryptography and blockchain technology for authenticating archives. The review results indicate that the managed digital preservation service model is increasingly being adopted by large archives and libraries because it is considered efficient, secure, and sustainability-oriented. The use of fixity check mechanisms, digital signatures, and timestamping (both blockchain-based and non-blockchain-based) has been proven to improve data integrity and the evidentiary value of archives. However, key challenges remain: financial sustainability, compliance with standards, and limited technical resources in small institutions. This article emphasizes the importance of synergy between technology, institutional policies, and long-term governance in PaaST implementation.

Keywords: Article, PaaST, Blockchain, Content, Formatting, Digital Preservation, ISO 16363, OAIS, Security,

PENDAHULUAN

Pada era digital saat ini, nilai arsip tidak lagi bergantung pada keberadaan fisiknya, melainkan pada keberlangsungan, keaslian, dan keteraksesannya dalam jangka panjang sebagai bagian dari warisan organisasi maupun masyarakat. Transformasi menuju arsip digital membawa tantangan yang berbeda dibandingkan arsip konvensional, terutama karena risiko obsolesensi format, degradasi media digital, serta ketidakpastian teknologi yang terus berubah. Kegagalan dalam menjaga keberlanjutan arsip digital dapat berakibat fatal, mulai dari hilangnya bukti hukum hingga mudurnya memori kolektif organisasi atau bangsa. Dalam topik ini, semakin banyak lembaga yang dihadapkan pada kebutuhan untuk mengelola arsip “lahir digital” (born-digital) maupun arsip hasil digitalisasi secara profesional dan berkelanjutan. Model layanan pelestarian digital (Preservation as a Service) pun muncul sebagai respons terhadap kebutuhan efisiensi, skala, dan keandalan dalam menjaga arsip digital. Akan tetapi, kualitas layanan tersebut tidak hanya diukur dari kecanggihan teknologinya, melainkan juga dari tingkat kepercayaan (trust) yang dapat diberikan kepada penyedia layanan untuk menjamin autentisitas dan integritas arsip (Zahara & Salim, 2022).

Dalam pengelolaan arsip digital, tantangan utama tidak lagi sekadar berkaitan dengan risiko *obsolescence*, degradasi media, atau perubahan teknologi, melainkan pada bagaimana menjaga tingkat kepercayaan (trust), autentisitas, dan integritas arsip dalam jangka panjang. Keandalan arsip digital sebagai bukti dan memori kolektif hanya dapat dipertahankan apabila sistem pelestarian mampu menjamin bahwa arsip tetap utuh, tidak berubah tanpa jejak, serta dapat dipahami secara topiktual oleh pengguna di masa depan (Johnston, 2020). Dalam topik tersebut, *Open Archival Information System* (OAIS) yang tertuang dalam ISO 14721 menjadi kerangka dasar pelestarian digital modern, terutama karena menekankan pentingnya bukti keaslian, dokumentasi, dan pemahaman berkelanjutan atas informasi (CCSDS, 2012).

Sebagai respons terhadap kebutuhan untuk menjaga kepercayaan tersebut, model *Preservation as a Service for Trust* (PaaST) hadir sebagai pendekatan inovatif yang mengintegrasikan aspek teknis, kebijakan kelembagaan, serta mekanisme audit dalam satu kerangka pelestarian yang komprehensif. PaaST mengedepankan prinsip bahwa penyedia layanan pelestarian digital tidak hanya bertanggung jawab atas penyimpanan dan migrasi format, tetapi juga atas akuntabilitas, transparansi operasional, serta pemenuhan standar profesional yang menjamin integritas arsip (Pacheco et al., 2023). Pendekatan ini menjadi semakin relevan mengingat berbagai penelitian menunjukkan bahwa teknologi semata, termasuk penggunaan *distributed ledger technology* seperti blockchain, tidak cukup untuk menegakkan autentisitas tanpa dukungan kebijakan, metadata yang memadai, dan validitas sertifikasi digital (Stančić & Bralić, 2021).

Urgensi kepercayaan dalam pelestarian digital turut diperkuat oleh standar internasional seperti ISO 16363 mengenai *Trustworthy Digital Repositories* (TDR), yang menegaskan bahwa repositori digital harus menunjukkan kapasitas tata kelola, dokumentasi kebijakan, auditabilitas, dan stabilitas jangka panjang untuk dapat dinilai sebagai tepercaya (Sağlık, 2023). Selain itu, instrumen seperti *Levels of Preservation* dari NDSA menggarisbawahi bahwa kepercayaan tidak dapat dibangun tanpa pengukuran kinerja, pelaporan, serta penerapan praktik pelestarian yang dapat diverifikasi. Dalam kaitan ini, PaaST memfasilitasi integrasi antara standar teknis dan kewajiban institusional melalui *Service Level Agreements* (SLA), audit periodik, serta mekanisme pelaporan yang memastikan bahwa setiap arsip tetap autentik, utuh, dan aman selama siklus hidupnya.

Dengan demikian, penelitian ini menempatkan PaaST sebagai kerangka kunci dalam upaya menjaga kepercayaan pada arsip digital, sekaligus mengkaji bagaimana integrasi layanan pelestarian, kebijakan tata kelola, dan mekanisme audit dapat memperkuat autentisitas serta integritas arsip jangka panjang. Pendekatan tersebut sejalan dengan kebutuhan lembaga modern yang harus memastikan bahwa arsip digital, baik yang *born-digital* maupun hasil digitalisasi, dapat dipertahankan sebagai bukti yang sah, kredibel, dan berfungsi sebagai warisan informasi bagi generasi mendatang.

METODE

Penelitian ini menggunakan pendekatan *Systematic Literature Review* (SLR) sebagai metode utama untuk memperoleh pemahaman komprehensif mengenai perkembangan, implementasi, dan tantangan konsep *Preservation as a Service for Trust* (PaaST) dalam konteks keaslian (*authenticity*) dan keamanan (*security*) arsip digital. Metode SLR dipilih karena mampu menyusun serta mengevaluasi temuan-temuan ilmiah sebelumnya secara sistematis dan objektif, sehingga memungkinkan identifikasi pola penelitian, kesenjangan, dan arah pengembangan konsep PaaST ke depan (Kitchenham & Charters, 2007). Untuk menjaga konsistensi dengan keseluruhan naskah, rentang waktu pencarian literatur ditetapkan pada tahun 2019 - 2025, sesuai dengan perkembangan terbaru dalam pelestarian digital dan kebijakan tata kelola repositori digital modern.

Proses pencarian literatur dilakukan pada lima basis data akademik bereputasi internasional Scopus, IEEE Xplore, SpringerLink, ScienceDirect, dan Google Scholar dengan menggunakan kombinasi kata kunci berbasis *Boolean* yang mencakup istilah “*Preservation as a Service for Trust*”, “*PaaST*”, “*Digital Preservation Service*”, “*Authenticity*”, “*Integrity*”, “*Security*”, dan “*Trustworthy Digital Repository*”. Kriteria inklusi ditetapkan secara sederhana dan eksplisit untuk memastikan hanya literatur yang memiliki relevansi langsung dengan model PaaST serta isu keaslian dan keamanan arsip digital yang disertakan. Artikel yang dibahas harus menguraikan konsep PaaST, layanan preservasi digital berbasis model layanan (*service-based preservation*), atau mekanisme validasi autentisitas dan keamanan. Sementara itu, kriteria eksklusi mencakup artikel yang hanya membahas penyimpanan *cloud* tanpa perspektif preservasi, publikasi tanpa metodologi yang jelas, artikel berbahasa non-Inggris, serta tulisan opini yang tidak didukung data empiris. Penetapan kriteria tersebut penting untuk memastikan bahwa analisis dilakukan pada karya ilmiah yang relevan, kredibel, dan berkontribusi langsung pada pemahaman PaaST sebagai kerangka preservasi digital.

Proses seleksi dilakukan berdasarkan alur *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) yang mencakup tahapan identifikasi, penyaringan (*screening*), penentuan kelayakan (*eligibility*), dan inklusi (Moher et al., 2020). Artikel yang lolos pada tahap akhir dianalisis berdasarkan fokus penelitian, pendekatan metodologis, serta kontribusinya terhadap pembahasan mengenai keaslian, integritas, dan keamanan arsip digital.

Tahap analisis data dilakukan menggunakan teknik *thematic coding* untuk mengidentifikasi tema-tema kunci yang muncul dari literatur terpilih. Proses pengodean dilakukan melalui penelaahan mendalam terhadap setiap artikel untuk menemukan hubungan antar konsep, termasuk integrasi model OAIS dengan PaaST, mekanisme *fixity checking*, penerapan standar ISO 16363, serta strategi keberlanjutan layanan preservasi digital. Hasil pengodean menghasilkan empat tema utama yang menjadi dasar pembahasan penelitian ini, yaitu *trust framework*, *authenticity validation*, *security mechanisms*, dan *service sustainability* (Braun & Clarke, 2021). Untuk memastikan validitas dan reliabilitas temuan, proses pengodean dilakukan oleh dua peneliti secara independen, kemudian dibandingkan untuk mencapai kesepakatan analitis. Dengan pendekatan sistematis dan terstruktur ini, penelitian diharapkan mampu memberikan gambaran utuh mengenai peran PaaST dalam memperkuat keaslian, integritas, dan keamanan arsip digital dalam ekosistem preservasi modern.

HASIL DAN PEMBAHASAN

Pemaparan Hasil Penelitian

Tabel 1. Ringkasan Temuan Sistematis Review: Penerapan Preservation as a Service for Trust (PaaST) dalam Pelestarian Arsip Digital

No	Temuan Utama	Deskripsi	Referensi
1	Kerangka Kepercayaan (Trust Framework)	PaaST mengintegrasikan aspek teknis, kebijakan, dan tata kelola untuk membangun kepercayaan terhadap repositori digital. Kepercayaan dihasilkan tidak hanya dari sistem teknologi yang aman tetapi juga dari kebijakan, audit, dan dokumentasi proses preservasi yang dapat diverifikasi.	Abrams, 2023; National Archives, 2025
2	Keaslian (Authenticity) & Integritas (Integrity)	Pemeriksaan <i>fixity</i> (checksum, hashing) dan penggunaan <i>preservation metadata</i> menjadi kunci dalam mendeteksi perubahan tak sah. Integrasi teknologi <i>blockchain</i> memungkinkan pencatatan perubahan pada arsip dalam <i>immutable ledger</i> , memperkuat autentikasi dan <i>provenance data</i> .	Phillips et al., 2021; Becker et al., 2021
3	Keamanan Arsip Digital (Security)	Keamanan mencakup aspek teknis (akses kontrol, enkripsi, pemantauan sistem) dan kebijakan kelembagaan (manajemen risiko, audit, tanggung jawab hukum). PaaST menuntut lembaga memiliki <i>security policy framework</i> selaras ISO 27001.	Conway & Hedstrom, 2021
4	Keberlanjutan Layanan (Service Sustainability)	Keberlanjutan bergantung pada pendanaan jangka panjang, kolaborasi antar lembaga, dukungan kebijakan, interoperabilitas, dan kapasitas SDM. PaaST memerlukan model bisnis jelas dan integrasi dengan platform pelestarian digital lainnya.	Sharma & Kumar, 2022

5	Tantangan Implementasi	Standardisasi, interoperabilitas, dan kesiapan infrastruktur lintas institusi menjadi hambatan utama. Kompleksitas integrasi keamanan dan audit lintas platform menjadi tantangan signifikan, meski potensi integrasi cloud preservation berbasis AI dan <i>distributed ledger</i> tinggi.	Sharma & Kumar, 2022; Becker et al., 2021
6	Kebijakan & Praktik Kelembagaan	PaaST memperkuat kepercayaan publik terhadap arsip digital melalui transparansi, auditabilitas, kolaborasi, dan literasi digital pengelola arsip. Keberhasilan model ini ditentukan oleh kesiapan institusional dan tata kelola yang mendukung.	National Archives, 2025

Hasil telaah sistematis menunjukkan bahwa *Preservation as a Service for Trust* (PaaST) berfungsi sebagai model layanan pelestarian digital generasi baru yang mengintegrasikan aspek teknologi, kebijakan, dan tata kelola untuk menghasilkan repositori digital yang dapat dipercaya (*trusted digital repository*). PaaST menerapkan mekanisme pelestarian berbasis layanan di mana setiap proses preservasi terekam dalam *verifiable preservation activity logs* yang dapat diaudit oleh auditor internal, lembaga pengawas, maupun pihak ketiga menggunakan standar audit seperti ISO 16363 (Abrams, 2023). Integrasi teknologi dilakukan melalui penerapan prinsip *Open Archival Information System* (OAIS/ISO 14721) sebagai kerangka desain fungsional sistem, sedangkan ISO 16363 dipakai sebagai kerangka sertifikasi keandalan repositori. Dengan demikian, OAIS mendefinisikan bagaimana sistem bekerja, sementara ISO 16363 membuktikan bahwa sistem tersebut benar-benar dapat dipercaya melalui audit formal. Temuan ini mempertegas bahwa kerangka kepercayaan dalam PaaST dibangun secara simultan melalui infrastruktur teknologi, kebijakan preservasi, serta transparansi proses yang dapat diverifikasi (National Archives, 2025).

Temuan kedua menunjukkan bahwa aspek keaslian (*authenticity*) dan integritas (*integrity*) arsip digital menjadi pusat dari seluruh arsitektur PaaST. Hampir seluruh studi menekankan perlunya verifikasi *fixity* melalui *checksum* dan *cryptographic hashing* untuk mendeteksi perubahan yang tidak sah pada arsip digital (Phillips et al., 2021). PaaST menggabungkan pemeriksaan *fixity* tersebut dengan *preservation metadata* yang mencatat setiap intervensi, sehingga jejak perubahan dapat diidentifikasi secara transparan. Selain itu, beberapa penelitian mengemukakan pemanfaatan teknologi *blockchain* untuk mencatat *provenance* arsip dalam *immutable ledger*, sehingga tidak ada entitas yang dapat mengubah catatan autentikasi tanpa meninggalkan jejak (Becker et al., 2021). Integrasi *fixity* - metadata - blockchain ini memberikan mekanisme verifikasi berlapis yang secara signifikan meningkatkan kepercayaan terhadap identitas, keaslian, dan nilai bukti arsip digital yang dikelola dalam layanan PaaST.

Temuan ketiga berfokus pada keamanan (*security*) arsip digital yang dikembangkan melalui kombinasi pengendalian teknis dan kebijakan kelembagaan. Dari sisi teknis, repositori PaaST menerapkan *access control*, enkripsi data, dan *continuous system monitoring* untuk mencegah akses tidak sah maupun gangguan sistemik (Conway & Hedstrom, 2021). Sementara itu, kebijakan kelembagaan meliputi kerangka *security policy*, analisis risiko, audit keamanan, dan penetapan tanggung jawab hukum yang selaras dengan standar keamanan informasi seperti ISO 27001. Integrasi kedua aspek ini menciptakan model keamanan komprehensif yang bukan hanya memfokuskan pada infrastruktur digital, tetapi juga pada akuntabilitas kelembagaan, sehingga memperkuat kepercayaan publik terhadap repositori digital berbasis PaaST.

Selanjutnya, temuan keempat menyoroti keberlanjutan layanan (*service sustainability*) sebagai elemen krusial dalam implementasi PaaST. Studi oleh (Sharma & Kumar, 2022) menunjukkan bahwa keberlanjutan layanan sangat dipengaruhi oleh ketersediaan pendanaan jangka panjang, kolaborasi antar lembaga, serta dukungan kebijakan pemerintah yang konsisten. Karena PaaST dioperasikan sebagai *service-based model*, maka repositori membutuhkan model bisnis yang terstruktur, diversifikasi sumber daya, serta interoperabilitas dengan platform pelestarian digital lainnya. Interoperabilitas ini penting karena memungkinkan repositori untuk menangani pertukaran data, migrasi format, dan integrasi antarsistem tanpa mengorbankan keaslian atau keamanan arsip. Hasil studi sistematis juga menunjukkan bahwa kompetensi sumber daya manusia, khususnya dalam memahami aspek teknis verifikasi, enkripsi, dan manajemen metadata, menentukan kelangsungan layanan PaaST di masa depan.

Di sisi lain, sejumlah tantangan implementasi turut diidentifikasi. Tantangan seperti kurangnya standarisasi protokol audit, keterbatasan interoperabilitas, dan rendahnya kesiapan institusional dalam mengadopsi model layanan berbasis kepercayaan berdampak langsung pada menurunnya transparansi dan dapat melemahkan fungsi *trust-building* yang menjadi inti dari PaaST (Sharma & Kumar, 2022). Misalnya, tanpa standarisasi audit yang seragam, log aktivitas preservasi tidak dapat diverifikasi secara konsisten antar platform, sehingga menurunkan tingkat auditabilitas. Namun demikian, studi internasional yang

berhasil mengimplementasikan *trusted digital repository* berbasis OAIS dan ISO 16363 seperti proyek *National Archives ERA 2.0* di Amerika Serikat menunjukkan bahwa tantangan tersebut dapat diatasi melalui pengembangan protokol audit terpadu, integrasi *distributed ledger*, dan pemanfaatan *cloud preservation* berbasis AI untuk meningkatkan presisi verifikasi (Becker et al., 2021). Praktik-praktik ini memberikan gambaran bahwa PaaST dapat diimplementasikan secara efektif ketika didukung oleh kebijakan nasional, infrastruktur digital yang memadai, serta kolaborasi lintas lembaga.

Dalam konteks kelembagaan, PaaST berpotensi menjadi solusi strategis bagi lembaga arsip, perpustakaan digital, dan institusi pendidikan tinggi dalam memperkuat keandalan repositori digital. Transparansi, auditabilitas, serta kolaborasi antar-lembaga menjadi pilar utama yang mendukung peningkatan kepercayaan publik terhadap arsip digital (National Archives, 2025). Penerapan PaaST juga mendorong peningkatan literasi digital pengelola arsip, khususnya terkait *authenticity verification*, enkripsi, migrasi format, dan manajemen risiko sehingga nilai autentik arsip tetap terjaga. Secara keseluruhan, hasil kajian ini menunjukkan bahwa PaaST merupakan pendekatan pelestarian digital yang komprehensif dan berorientasi masa depan. Melalui integrasi antara kepercayaan, keaslian, keamanan, dan keberlanjutan, PaaST menghadirkan model preservasi yang sesuai dengan kebutuhan organisasi modern yang mengelola data jangka panjang. Tantangan implementasi menuntut kolaborasi multidisipliner antara ahli arsip, teknologi informasi, dan pembuat kebijakan, sehingga PaaST dapat menjadi fondasi utama dalam membangun repositori digital yang terpercaya, aman, dan berkelanjutan di era transformasi digital.

Tabel 2. Ringkasan Hasil Kajian Literatur tentang PaaST (2019 - 2024)

No	Penulis & Tahun	Judul Penelitian	Fokus Kajian	Temuan Utama
1	Abrams (2023)	<i>Understanding OAIS and Digital Repository Trustworthiness</i>	Model OAIS & Trust	OAIS menjadi dasar desain repositori terpercaya dalam PaaST.
2	Phillips et al. (2021)	<i>Changing Practices in Fixity</i>	Integritas Digital	Fixity check penting dalam menjaga keaslian arsip digital.
3	Becker et al. (2021)	<i>Executable Archives and Software Integrity</i>	Blockchain & Provenance	Blockchain memperkuat jejak autentikasi arsip digital.
4	Conway & Hedstrom (2021)	<i>Risk Management in Digital Repositories</i>	Keamanan dan Audit	ISO 16363 dan ISO 27001 meningkatkan keamanan sistem PaaST.
5	Sharma & Kumar (2022)	<i>Digital Preservation in Digital Libraries: A Systematic Review</i>	Keberlanjutan Layanan	Kolaborasi lintas institusi penting bagi keberlanjutan PaaST.
6	National Archives (2025)	<i>16363 Reasons to Trust</i>	Audit Keandalan	Audit berbasis ISO 16363 meningkatkan kepercayaan terhadap arsip digital.

Berdasarkan Tabel 2, hasil kajian literatur mengenai *Preservation as a Service for Trust* (PaaST) pada periode 2019–2024 menunjukkan bahwa penguatan keaslian dan keamanan arsip digital membutuhkan integrasi menyeluruh antara kerangka konseptual, mekanisme teknis, dan standar internasional yang saling melengkapi. Model *Open Archival Information System* (OAIS, ISO 14721) berperan sebagai kerangka fungsional dalam merancang arsitektur repositori, terutama melalui spesifikasi fungsi *ingest*, *archival storage*, *data management*, *preservation planning*, dan *access*, yang menjadi dasar interoperabilitas dan pengendalian proses preservasi (Abrams, 2023). Dalam konteks PaaST, kerangka ini tidak hanya mengatur bagaimana informasi diorganisasi, tetapi juga bagaimana aktivitas preservasi direkam sehingga dapat diaudit. Aktivitas tersebut diwujudkan melalui *verifiable preservation logs* yang mencatat setiap tindakan preservasi, termasuk perubahan bitstream, proses *fixity check*, hingga prosedur migrasi format, yang kemudian dapat diperiksa oleh auditor internal maupun eksternal sesuai standar sertifikasi.

Integritas digital menjadi komponen kunci dalam menjaga keaslian arsip, di mana mekanisme *fixity check* berfungsi memverifikasi konsistensi hash sepanjang siklus hidup arsip digital. Teknologi *blockchain* memperluas fungsi tersebut dengan menyediakan *immutable provenance ledger* yang memungkinkan pihak ketiga menelusuri jejak autentikasi secara transparan dan tidak dapat dimodifikasi, sehingga meningkatkan kepercayaan pada proses preservasi digital (Phillips et al., 2021; Becker et al., 2021). Integrasi antara *fixity check* dan *blockchain* dalam PaaST memberikan lapisan verifikasi ganda: *fixity* menjaga integritas teknis, sementara *blockchain* menjamin integritas historis perubahan. Keamanan layanan PaaST diperkuat melalui

standar ISO 16363 sebagai kerangka audit dan sertifikasi repositori terpercaya, yang menilai kemampuan suatu sistem dalam mengelola risiko, menjaga integritas, serta menyediakan bukti keandalan proses secara berkelanjutan (Conway & Hedstrom, 2021). Hubungan OAIS dan ISO 16363 bersifat komplementer: OAIS menyediakan desain dan fungsi sistem, sedangkan ISO 16363 mengevaluasi apakah implementasi tersebut memenuhi persyaratan kepercayaan (*trustworthiness*) sebuah *trusted digital repository*. Selain itu, integrasi dengan ISO 27001 mendukung keamanan informasi melalui kontrol akses, enkripsi, dan manajemen insiden, sehingga memperkuat *trust* pengguna terhadap layanan preservasi (National Archives, 2025).

Kajian literatur juga menegaskan bahwa keberlanjutan layanan PaaST sangat dipengaruhi oleh kolaborasi lintas institusi, termasuk penyedia layanan *cloud*, lembaga kearsipan nasional, dan institusi akademik. Kolaborasi ini memungkinkan berbagi infrastruktur, penyusunan protokol audit bersama, serta adopsi praktik terbaik internasional yang telah berhasil diterapkan, seperti model *Digital Preservation Network* (DPN) dan *MetaArchive Cooperative*, yang mengandalkan jejaring konsorsium untuk redundansi, interoperabilitas, dan pembuktian kepercayaan (Sharma & Kumar, 2022).

Tantangan implementasi mencakup isu standardisasi antarsistem, keterbatasan interoperabilitas metadata, dan kesiapan institusi dalam menerapkan protokol audit, yang secara langsung berdampak pada transparansi dan akuntabilitas layanan PaaST. Misalnya, kurangnya keseragaman protokol *fixity* atau prosedur audit menyebabkan aktivitas preservasi sulit diverifikasi oleh pihak eksternal, sehingga mengurangi tingkat *trust* terhadap repositori. Selain itu, perbedaan tingkat kematangan infrastruktur antar lembaga dapat menghambat integrasi penuh dengan sistem berbasis PaaST. Sejumlah literatur menunjukkan bahwa tantangan ini dapat diatasi melalui penerapan mekanisme audit berlapis, penggunaan *shared preservation workflows*, serta adopsi standar terbuka yang memungkinkan sistem saling berbagi metadata dan log aktivitas secara aman. Secara keseluruhan, sintesis hasil kajian menegaskan bahwa keberhasilan PaaST tidak hanya bergantung pada penerapan standar teknis, tetapi juga pada integrasi mekanisme validasi (*fixity* dan *provenance*), penerapan kerangka audit (ISO 16363), serta kesiapan institusional dalam memastikan transparansi proses preservasi. Kombinasi elemen-elemen ini membentuk fondasi repositori digital yang terpercaya, aman, dan berkelanjutan, sekaligus memberikan arah bagi pengembangan model PaaST yang adaptif terhadap dinamika teknologi dan regulasi di masa mendatang.

Summary of Key Research Findings

Tabel 3. *Summary of Key Research Findings*

No	Category of Findings	Key Research Outcomes	References
1	Trust Framework	Kerangka kepercayaan menjadi fondasi PaaST, menggabungkan teknologi, tata kelola, dan dokumentasi proses preservasi; setiap aktivitas pelestarian tercatat dalam log yang dapat diverifikasi	Abrams, 2023; National Archives, 2025
2	Authenticity & Integrity	Pemeriksaan <i>fixity</i> (checksum, hashing) dan <i>preservation metadata</i> digunakan untuk mendeteksi perubahan; blockchain memperkuat autentikasi dan <i>provenance record</i>	Phillips et al., 2021; Becker et al., 2021
3	Security	Keamanan mencakup aspek teknis (akses, enkripsi, monitoring) dan kebijakan kelembagaan (audit, manajemen risiko, kepatuhan hukum)	Conway & Hedstrom, 2021
4	Service Sustainability	Keberlanjutan layanan bergantung pada pendanaan jangka panjang, kolaborasi antar lembaga, dukungan kebijakan, interoperabilitas sistem, dan kapasitas SDM	Sharma & Kumar, 2022; Becker et al., 2021
5	Policy & Institutional Practice	PaaST mendorong transparansi, auditabilitas, dan kolaborasi; memperkuat literasi digital pengelola arsip serta kesiapan institusional	National Archives, 2025

Hasil telaah menunjukkan bahwa *Preservation as a Service for Trust* (PaaST) menempatkan kerangka kepercayaan (*trust framework*) sebagai fondasi utama dalam pelestarian arsip digital, di mana keandalan repositori dibuktikan melalui dokumentasi proses, jejak audit, serta kepatuhan terhadap standar internasional seperti OAIS (ISO 14721) dan ISO 16363 (Abrams, 2023; National Archives, 2025). Dalam model PaaST, OAIS berfungsi sebagai kerangka fungsional yang mengatur alur penerimaan, penyimpanan, pengelolaan, dan penyajian arsip digital, sementara ISO 16363 menyediakan standar audit untuk menilai kepercayaan dan kesiapan repositori digital. Integrasi kedua standar tersebut memastikan bahwa setiap

aktivitas preservasi dapat diverifikasi melalui *verifiable preservation logs*, yaitu catatan aktivitas yang otomatis direkam dalam sistem dan dapat diperiksa oleh auditor internal maupun lembaga sertifikasi eksternal pada interval tertentu. Proses audit dilakukan menggunakan parameter keandalan, integritas, dan keamanan sesuai pedoman ISO 16363, sehingga tingkat kepercayaan dapat diukur secara objektif.

Keaslian dan integritas arsip dijaga melalui pemanfaatan teknologi *fixity* dan *blockchain*, yang bekerja secara komplementer dalam model PaaST. *Fixity check* melalui perhitungan *cryptographic hash* memastikan bahwa tidak ada perubahan pada bita arsip sejak pertama kali disimpan. Sementara itu, *blockchain* menyediakan rantai rekaman permanen (*immutable ledger*) atas setiap intervensi pada arsip, termasuk pembaruan metadata, migrasi format, atau tindakan preservasi lainnya (Phillips et al., 2021; Becker et al., 2021). Dengan demikian, integrasi kedua teknologi ini meningkatkan bukti autentisitas dan *non-repudiation*, karena setiap perubahan selalu tercatat dan tidak dapat dihapus tanpa meninggalkan jejak. Keamanan sistem ditingkatkan melalui kombinasi kontrol teknis seperti *access control lists*, *multi-factor authentication*, dan teknologi enkripsi serta kebijakan kelembagaan yang mengatur prosedur akses, pengelolaan risiko, dan penanganan insiden (Conway & Hedstrom, 2021).

Keberlanjutan layanan PaaST menuntut adanya pendanaan yang stabil, interoperabilitas perangkat lunak preservasi, serta peningkatan kapasitas SDM agar model ini dapat dioperasikan secara jangka panjang. Interoperabilitas diwujudkan melalui penerapan standar metadata seperti PREMIS dan METS yang memungkinkan pertukaran informasi antar-repositori (Sharma & Kumar, 2022). Selain itu, praktik transparansi, auditabilitas, dan kolaborasi antar-lembaga terbukti memperkuat tata kelola arsip digital, sebagaimana ditunjukkan oleh beberapa repositori nasional yang telah menerapkan audit ISO 16363 secara berkala (National Archives, 2025). Sejumlah studi menunjukkan bahwa integrasi PaaST dengan layanan *cloud computing*, *AI-based integrity monitoring*, dan *distributed ledger* mampu mempercepat proses verifikasi dan mendeteksi anomali arsip secara otomatis (Becker et al., 2021). Hal ini menunjukkan bahwa PaaST memiliki sifat yang adaptif dan dapat berevolusi mengikuti perkembangan teknologi.

Secara keseluruhan, PaaST menghadirkan pendekatan holistik dalam pelestarian digital dengan mengintegrasikan aspek kepercayaan, keaslian, keamanan, dan keberlanjutan. Kepercayaan dibangun melalui keselarasan antara kerangka fungsional OAIS dan kerangka audit ISO 16363, sementara integritas arsip ditegakkan melalui *fixity check*, *blockchain*, metadata teknis, dan audit berkala. Keamanan sistem dijamin melalui kombinasi mekanisme teknis dan tata kelola kelembagaan yang mengikuti standar internasional. Keberlanjutan layanan memerlukan kolaborasi lintas institusi, pendanaan jangka panjang, serta literasi digital yang memadai dari pengelola repositori. Meskipun terdapat tantangan seperti keterbatasan infrastruktur dan standarisasi lintas sistem, PaaST menawarkan kerangka layanan yang dinamis dan dapat diintegrasikan dengan teknologi *cloud preservation* serta sistem berbasis AI, sehingga berpotensi menjadi fondasi strategis dalam membangun repositori digital yang tepercaya, aman, dan berkelanjutan.

Kelemahan Penelitian

Meskipun PaaST menawarkan model pelestarian digital yang inovatif, implementasinya masih menghadapi sejumlah kelemahan struktural yang berdampak langsung pada kepercayaan (*trustworthiness*) repositori digital. Pertama, masalah standarisasi menjadi kendala karena variasi protokol audit dan mekanisme keamanan antar-lembaga mengurangi transparansi dan konsistensi bukti keandalan arsip (Sharma & Kumar, 2022). Ketidaksinkronan standar tersebut melemahkan aspek *auditability*, yang merupakan komponen utama dalam kerangka kepercayaan PaaST. Kedua, interoperabilitas antar-sistem masih terbatas akibat perbedaan format data, struktur metadata, dan arsitektur teknis, sehingga mempersulit integrasi dengan repositori lain dan menghambat pertukaran informasi preservasi secara efektif (Becker et al., 2021). Dampaknya, proses verifikasi lintas platform menjadi tidak optimal dan berpotensi menurunkan integritas proses preservasi.

Kesiapan institusional juga menjadi tantangan karena tidak semua lembaga memiliki kapasitas teknis, infrastruktur digital, maupun SDM yang kompeten untuk menerapkan PaaST secara menyeluruh (Sharma & Kumar, 2022). Integrasi teknologi canggih seperti *blockchain*, sistem keamanan berlapis, dan mekanisme audit ISO 16363 memerlukan kemampuan teknis yang tinggi dan investasi biaya yang signifikan. Selain itu, kompleksitas integrasi platform audit dan keamanan dapat menimbulkan risiko salah konfigurasi, yang pada akhirnya mengurangi tingkat kepercayaan yang ingin dibangun melalui PaaST (Phillips et al., 2021). Aspek keberlanjutan dan skalabilitas juga menjadi perhatian karena layanan ini membutuhkan pendanaan berkala, dukungan kebijakan jangka panjang, serta uji coba skala besar yang hingga kini masih terbatas (Abrams, 2023; Sharma & Kumar, 2022).

Secara keseluruhan, kelemahan-kelemahan tersebut menunjukkan bahwa PaaST masih menghadapi tantangan signifikan sebelum dapat diterapkan secara luas. Kurangnya standarisasi mengurangi transparansi audit, keterbatasan interoperabilitas menghambat verifikasi lintas sistem, dan rendahnya kesiapan institusional berpotensi menurunkan kualitas implementasi. Kompleksitas teknis menuntut penguatan kapasitas SDM dan penyusunan pedoman teknis yang lebih komprehensif. Untuk mengatasi tantangan ini, beberapa praktik internasional—seperti penerapan *CoreTrustSeal*, audit ISO 16363 reguler di *national archives*, dan penggunaan metadata PREMIS sebagai standar global—dapat dijadikan acuan untuk memperkuat kepercayaan dan meningkatkan konsistensi penerapan PaaST. Dengan memahami dan menanggapi kelemahan tersebut, pengembangan PaaST selanjutnya diharapkan dapat menghasilkan model yang lebih adaptif, mudah diintegrasikan, serta mendukung keberlanjutan pelayanan pelestarian digital.

KESIMPULAN

Berdasarkan hasil tinjauan sistematik terhadap literatur terkini, dapat disimpulkan bahwa *Preservation as a Service for Trust* (PaaST) merupakan inovasi penting dalam bidang pelestarian arsip digital yang berfokus pada pembentukan kepercayaan (*trustworthiness*) melalui layanan berbasis audit, keaslian, dan keamanan. PaaST menghadirkan model baru yang menempatkan proses preservasi sebagai bagian integral dari sistem layanan digital yang transparan dan dapat diverifikasi. Dengan mengadopsi prinsip-prinsip *Open Archival Information System* (OAIS) dan standar internasional seperti ISO 16363, konsep ini mampu menjawab tantangan pelestarian digital modern yang menuntut bukti keaslian dan integritas jangka panjang. Lebih jauh, penerapan PaaST tidak hanya menjamin kelestarian arsip digital, tetapi juga memperkuat legitimasi institusi pengelola arsip dalam memberikan jaminan keandalan terhadap informasi digital yang dikelola. Penelitian ini juga menyoroti bahwa keberhasilan penerapan PaaST sangat bergantung pada kolaborasi antara teknologi, kebijakan, dan tata kelola kelembagaan. Keaslian arsip digital tidak dapat dijaga hanya dengan pendekatan teknis seperti *fixity check* atau enkripsi, melainkan harus diperkuat dengan kebijakan manajemen risiko, audit berkala, serta dokumentasi yang sesuai dengan standar internasional. Di sisi lain, aspek keberlanjutan layanan (*service sustainability*) menuntut adanya dukungan kebijakan nasional, pembiayaan jangka panjang, dan pengembangan kapasitas sumber daya manusia yang kompeten di bidang preservasi digital. Oleh karena itu, PaaST bukan hanya kerangka teknologi, melainkan paradigma tata kelola yang menempatkan kepercayaan dan transparansi sebagai prinsip utama dalam pengelolaan arsip digital.

Sebagai saran, penelitian ini merekomendasikan agar lembaga arsip, perpustakaan digital, dan institusi pendidikan tinggi di Indonesia mulai mengeksplorasi penerapan model PaaST secara bertahap dengan menyesuaikan kapasitas infrastruktur dan regulasi yang berlaku. Pemerintah dan lembaga terkait perlu mengembangkan pedoman nasional pelestarian digital berbasis kepercayaan yang mengintegrasikan standar OAIS, ISO 16363, serta praktik terbaik internasional. Selain itu, penelitian lanjutan disarankan untuk mengkaji penerapan teknologi pendukung seperti **blockchain**, kecerdasan buatan (AI), dan *machine learning* dalam memperkuat fungsi verifikasi dan audit arsip digital. Dengan langkah-langkah tersebut, diharapkan PaaST dapat menjadi landasan kuat bagi terciptanya ekosistem arsip digital yang autentik, aman, dan berkelanjutan di masa depan.

DAFTAR PUSTAKA

- Abrams, (2023). Abrams, S. (2023). *Understanding OAIS and digital repository trustworthiness: A framework for sustainable digital preservation*. *Journal of Digital Preservation Studies*, 9(2), 55 - 72. <https://doi.org/10.1080/25730231.2023.109872>
- Abrams, S. (2023). *Understanding OAIS and digital repository trustworthiness: A framework for sustainable digital preservation*. *Journal of Digital Preservation Studies*, 9(2), 55 - 72. <https://doi.org/10.1080/25730231.2023.109872>
- Becker, C., Kulovits, H., & Rauber, A. (2021). Executable archives and software integrity in digital preservation environments. *International Journal of Digital Curation*, 16(1), 1 - 18. <https://doi.org/10.2218/ijdc.v16i1.777>
- Braun, V., & Clarke, V. (2021). *Thematic analysis: A practical guide for researchers*. SAGE Publications.
- Conway, P., & Hedstrom, M. (2021). Risk management and audit frameworks for trustworthy digital repositories. *Information Management Review*, 37(4), 287 - 303. <https://doi.org/10.1016/j.imrev.2021.100421>
- Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering* (EBSE Technical Report). Keele University.
- McLeod, J., & Lomas, E. (2023). Record DNA: reconceptualising digital records as the future evidence base. *Archival Science*. <https://doi.org/10.1007/s10502-023-09414-w>

- Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & PRISMA Group. (2020). Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 statement. *PLoS Medicine*, 18(3), e1003583. <https://doi.org/10.1371/journal.pmed.1003583>
- Moore, R. W. (2018). Digital Archives and Preservation. Dalam *Encyclopedia of Database Systems* (2nd ed.). Springer.
- National Archives. (2025). *16363 reasons to trust: Building reliable digital preservation systems*. The National Archives Technical Series. <https://www.nationalarchives.gov.uk>
- Pacheco, A., Da Silva, C. G., & De Freitas, M. C. V. (2023). A metadata model for authenticity in digital archival descriptions. *Archival Science*, 23, 629 - 673. <https://doi.org/10.1007/s10502-023-09422-w>
- Phillips, M., Bailey, J., & Owens, T. (2021). Changing practices in fixity: Integrity and authenticity in digital preservation. *D-Lib Magazine*, 27(3/4). <https://doi.org/10.1045/march2021-phillips>
- Sharma, A., & Kumar, S. (2022). Digital preservation in digital libraries: A systematic review of sustainability and policy frameworks. *Journal of Information and Knowledge Management*, 21(2), 2250018. <https://doi.org/10.1142/S0219649222500189>
- Stančić, H., & Bralić, V. (2021). Digital Archives Relying on Blockchain: Overcoming the Limitations of Data Immutability. *Computers*, 10(8), 91. <https://doi.org/10.3390/computers10080091>
- Zahara, N. R., & Salim, T. A. (2022). Preservation of Digital Archives: Systematic Literature Review. *Record and Library Journal*, 8(2), 285 - 297. <https://doi.org/10.20473/rlj.V8-I2.2022.285-297>