Digital Library and Digital Preservation in the Knowledge System

Dr. S. Antony Arockiavathy[1], Dr. S. Aravind[2]

[1]Librarian, Yadava college (Autonomous), Madurai

[2]Librarian & Head of The Department, GTN College (Autonomous)

DOI: https://doi.org/10.47772/IJRISS.2026.101000409

Received: 30 September 2026; Accepted: 05 October 2026; Published: 04 November 2026

ABSTRACT

The transition from print-based collections to networked, machine-readable knowledge resources has made the digital library one of the central infrastructures of contemporary scholarship, public information access, and institutional memory. Digital libraries integrate content acquisition, structured metadata, storage, and discovery services into a coherent knowledge system, while digital preservation ensures that the resulting digital objects remain authentic, intact, and renderable long after the software and hardware that first created them have become obsolete. This paper reviews the conceptual architecture of digital libraries, the metadata and interoperability standards that support knowledge organization, and the preservation reference models -- principally the Open Archival Information System (OAIS) -- that govern long-term custodianship of digital content. Recent research on preservation sustainability, decentralized replication, cloud adoption, AI-assisted curation, and blockchain-based integrity verification is reviewed and synthesized into comparative tables and figures covering repository platforms, preservation strategies, and open challenges. The review shows that no single strategy or platform is sufficient in isolation; durable knowledge systems instead combine OAIS-aligned workflows, standardized preservation metadata, and emerging technologies to achieve both discoverability and longevity. The paper concludes by outlining future directions, including AI-assisted metadata generation, federated and cloud-based preservation, and blockchain-supported integrity verification, as pathways toward more resilient digital knowledge infrastructures.

Keywords: Digital Library, Digital Preservation, Knowledge System, OAIS Reference Model, Metadata Standards, Institutional Repository, Cloud Preservation, Semantic Web, Long-Term Access, LOCKSS, Blockchain.

1. INTRODUCTION

Libraries have historically served as the primary institutions through which societies organize, store, and transmit recorded knowledge. The emergence of computing, networked communication, and large-scale digitization has extended this role into the digital domain, giving rise to the digital library: an organized collection of digital objects together with the services, metadata, and infrastructure needed to create, manage, and provide access to that content. Unlike a simple online document repository, a digital library is a knowledge system in the fuller sense -- it combines content, structured description, retrieval mechanisms, and a user community into an integrated whole, echoing the function though not the physical form of a traditional library.

Early conceptual work on distributed digital object services proposed naming, storage, and access mechanisms that allow heterogeneous digital collections to interoperate across institutional boundaries. Building on such foundations, later initiatives established low-barrier protocols for metadata harvesting, enabling independently operated repositories to expose their holdings to shared discovery layers. These developments allowed digital libraries to evolve from isolated, institution-specific catalogues into networked knowledge infrastructures capable of supporting cross-institutional search, citation linking, and resource sharing.

A knowledge system, however, is only as durable as its capacity to keep information usable over time. Digital objects are fundamentally different from their print counterparts: they require an unbroken chain of compatible hardware, software, and file-format support to remain renderable, and they cannot survive the kind of "benign

neglect" that allows a paper document to remain legible after decades in storage. This dependency creates the central problem addressed by digital preservation -- the planned, active management of digital content to ensure continued accessibility, authenticity, and integrity across generations of technology. Digital preservation is therefore not a one-time technical safeguard but an ongoing organizational commitment, encompassing fixity checking, format monitoring, redundant storage, and periodic migration or emulation of content as underlying systems change.

Institutional repositories, built on platforms such as DSpace, EPrints, Fedora, and Islandora, have become the most common operational form of the digital library within universities, research institutes, and cultural heritage organizations, providing infrastructure for depositing, describing, and disseminating research outputs, theses, and archival materials. Layered on top of these repositories, preservation systems such as Archivematica and preservation networks such as LOCKSS and CLOCKSS implement formal reference models -- most notably the Open Archival Information System (OAIS) -- to standardize how digital content is ingested, stored, monitored, and eventually delivered to end users. Figure 1 summarizes the core components that together constitute a digital library knowledge ecosystem.

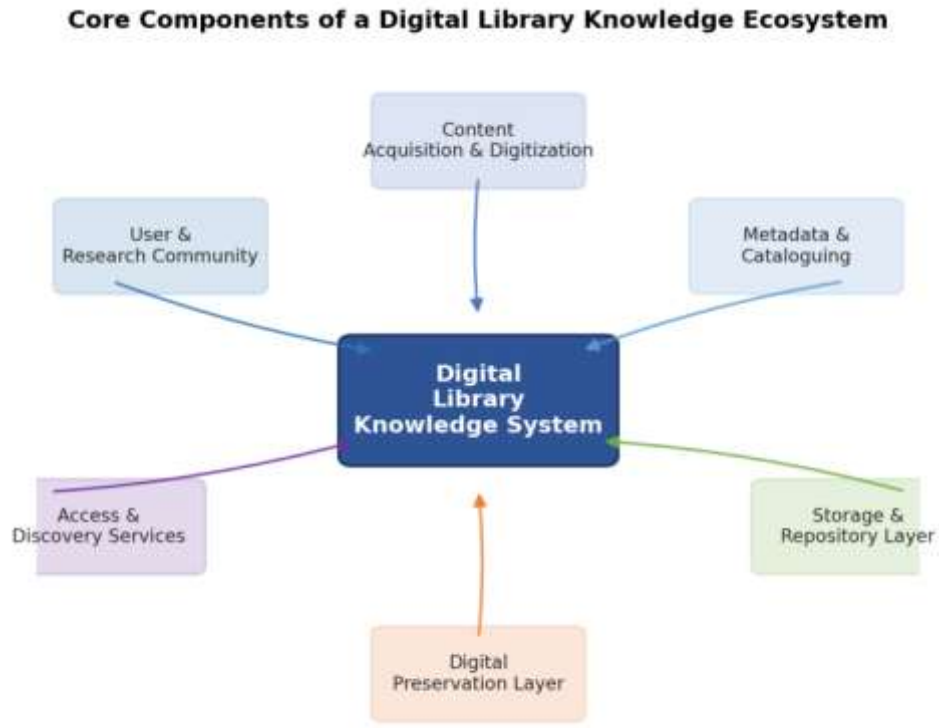

Fig 1. Core Components of a Digital Library Knowledge Ecosystem

Despite substantial progress, digital libraries and preservation systems continue to face persistent limitations: metadata schemes vary across institutions and disciplines, complicating interoperability; preservation actions such as migration and emulation carry cost and fidelity trade-offs; and rapid technological change continues to outpace the resources available to many memory institutions. This review synthesizes current research on digital library and preservation practice, and evaluates how architectural models, standards, and preservation strategies combine to support digital libraries as sustainable knowledge systems, before identifying gaps that future research and practice should address.

2. RELATED WORKS

Recent research on digital libraries and digital preservation reflects growing attention to preservation sustainability, decentralized infrastructure, artificial intelligence, cloud adoption, and trust technologies. Ahmad, Rafiq, and Arif (2024) conducted a systematic literature review of global digital preservation trends and found a strong worldwide preference among libraries, archives, and memory institutions for in-house preservation activity over outsourcing digital preservation to third-party vendors [1]. In the African context,

Akinola, Oso, Shorunke, and Oyadele (2024) examined preservation of theses and dissertations at selected Nigerian universities, reporting reliance on refreshing, replication, and migration strategies, negligible use of emulation, and recurring barriers of inadequate funding, limited skilled staff, and weak infrastructure [2]. Broader institutional change was traced by Adarkwah et al. (2024), who documented the transformation of academic libraries across Africa before and after COVID-19 and into the generative-AI era, showing an accelerating shift toward digitized, AI-augmented library services [3].

Pasqui (2024) reviewed two decades of digital curation and long-term preservation practice in libraries, tracing the field's evolution from early preservation milestones toward newer challenges tied to Open Science and continuously changing scholarly-publishing infrastructure [4]. Complementing this historical perspective, Harisanty, Obille, Anna, Purwanti, and Retrialisca (2024) carried out a bibliometric analysis of artificial-intelligence applications in cultural-heritage preservation, mapping a rapidly growing research area concerned with using AI to preserve, curate, and predict the value of heritage collections [5].

Infrastructure-focused studies have examined how preservation networks sustain content over time in practice. Kjellström (2025) studied the LOCKSS ("Lots of Copies Keep Stuff Safe") decentralized preservation methodology and showed that the same replication logic used to protect licensed scholarly archives is also adapted, in modified form, by unauthorized "shadow libraries" to keep their collections resilient against takedown -- illustrating both the strength and the dual-use nature of distributed replication as a preservation strategy [6]. From a technology-adoption perspective, M. Ibrahim, Ahmad, and Sallehudin (2025) reviewed the technological, organizational, and human factors that determine whether university libraries successfully adopt cloud computing for digital preservation, identifying system reliability, management support, and staff attitude as decisive adoption factors [7].

On the retrieval and knowledge-organization side, Kreutz, Blum, Schaer, Schenkel, and Weyers (2023) proposed a formal process-modelling approach for evaluating digital library search systems, offering a more rigorous alternative to ad hoc usability testing [8]. Kroll, Pirklbauer, Kalo, Kunz, Ruthmann, and Balke (2024) introduced a narrative query-graph discovery system for entity-interaction-aware document retrieval, extending digital library search beyond simple keyword matching toward relationship-aware discovery [9]. Finally, Athavale and Patel (2024) examined blockchain technology as a mechanism for maintaining the authenticity and credibility of digital information, reflecting growing interest in tamper-evident integrity verification for archival and recordkeeping contexts [10]. Table 1 summarizes these ten studies alongside their principal contribution and reported limitation.

Study	Focus Area	Key Contribution	Reported Limitation
Ahmad et al. (2024) [1]	Preservation Practice	Systematic review shows a global preference for in-house over outsourced digital preservation.	Findings are drawn from published literature rather than direct institutional audits.
Akinola et al. (2024) [2]	Case Study - Theses/Dissertations	Documents use of refreshing, replication, and migration; negligible emulation use.	Findings limited to selected Nigerian universities.
Adarkwah et al. (2024) [3]	Academic Libraries in Africa	Traces post-COVID and generative-AI transformation of library services.	Broad continental scope limits depth on any single institution.
Pasqui (2024) [4]	Digital Curation History	Reviews two decades of curation practice amid Open Science pressures.	Primarily descriptive; limited empirical measurement.
Harisanty et al. (2024) [5]	AI in Heritage Preservation	Bibliometric mapping of AI applications in cultural-heritage preservation (2001-2023).	Bibliometric method captures publication trends, not implementation outcomes.
Kjellström (2025) [6]	Decentralized Replication (LOCKSS)	Shows LOCKSS-style replication sustains both licensed archives and shadow libraries.	Webometric method traces link structure, not preservation fidelity.
M. Ibrahim et	Cloud Preservation	Identifies reliability, management	Literature-review

al. (2025) [7]	Adoption	support, and staff attitude as adoption drivers.	methodology; not a field deployment study.
Kreutz et al. (2023) [8]	Search System Evaluation	Proposes formal process modelling for evaluating digital library search systems.	Evaluation framework tested on a limited set of systems.
Kroll et al. (2024) [9]	Narrative Query Discovery	Introduces entity-interaction-aware retrieval beyond keyword search.	Added relational complexity increases computational cost.
Athavale & Patel (2024) [10]	Blockchain Integrity	Proposes blockchain-based authenticity and credibility verification for digital records.	Practical scalability and governance of blockchain ledgers remain open questions.

Table 1. Comparison of Representative Recent Studies on Digital Library and Preservation Practice

Taken together, these studies converge on a common insight: digital libraries and digital preservation are complementary rather than separate concerns, and current research is pushing this relationship in three directions simultaneously -- toward greater institutional sustainability (in-house capacity, cloud adoption), toward greater infrastructural resilience (decentralized replication), and toward greater intelligence and trust (AI-assisted curation, relationship-aware retrieval, blockchain integrity). A digital library that lacks a preservation layer risks losing its content to format obsolescence or media failure, while a preservation system without discovery and access services fails to function as a usable knowledge resource for its intended community. The remainder of this paper develops a consolidated framework that connects these two concerns and reviews how current platforms and strategies implement it.

3. CONCEPTUAL FRAMEWORK AND METHODOLOGY

This review follows a structured literature-synthesis methodology. Recent peer-reviewed articles on digital library architecture, preservation sustainability, and preservation infrastructure (reviewed in Section 2) were mapped onto a single reference framework covering four layers: (i) digital library system architecture, (ii) metadata and knowledge organization, (iii) the OAIS preservation reference model, and (iv) preservation strategies and evaluation metrics. Comparative tables and figures were then constructed to synthesize qualitative ratings and reported findings, in the same manner that comparative reviews in software and information-systems research typically summarize heterogeneous primary studies.

3.1 Digital Library System Architecture

At the architectural level, a digital library system is generally composed of three interacting layers: a digital object store that holds the bitstreams of text, image, audio, and dataset files; a metadata store that holds descriptive, structural, technical, and administrative information about each object; and a service layer that mediates ingestion, search, browsing, and delivery between these stores and the end user. Reference architectures formalize this separation into repository, naming, indexing, collection, and user-interface services, allowing individual services to be replaced or scaled independently as demand grows. Contemporary repository platforms implement this layered model with varying degrees of modularity: DSpace and EPrints bundle storage, indexing, and interface into a single deployable application, whereas Fedora exposes only the repository storage layer and expects institutions to build or select a separate access interface, an approach later adopted by Fedora-based projects such as Islandora and Hydra.

3.2 Metadata, Interoperability, and Knowledge Organization

Metadata is the connective layer that turns a collection of digital files into a searchable, citable, and preservable knowledge resource. Descriptive metadata, most commonly expressed using the fifteen-element Dublin Core set, records author, title, subject, and date information to support discovery. Structural and packaging metadata, expressed through the Metadata Encoding and Transmission Standard (METS), links page images, text files, and descriptive records into a single coherent digital object that can be transferred between systems. Where richer semantic relationships are required, Resource Description Framework (RDF)

triples and lightweight ontologies allow digital library metadata to be published as linked open data, enabling cross-repository querying and supporting knowledge-organization tasks such as faceted browsing and concept-based search. These semantic approaches represent an important convergence point between digital libraries and broader knowledge-management systems, since they allow institutional repositories to participate in shared, machine-interpretable knowledge graphs rather than remaining isolated metadata silos.

3.3 Digital Preservation Reference Model (OAIS)

The Open Archival Information System (OAIS) is the dominant conceptual model for digital preservation. OAIS defines six functional entities: Ingest, which accepts Submission Information Packages (SIPs) from producers and validates and transforms them into Archival Information Packages (AIPs); Archival Storage, which manages the long-term storage and fixity of AIPs; Data Management, which maintains descriptive and administrative databases; Access, which generates Dissemination Information Packages (DIPs) for consumers; Administration, which manages system operations; and Preservation Planning, which monitors technology change and recommends migration or other preservation actions. Figure 2 illustrates how these functional entities connect within a combined digital library and preservation architecture.

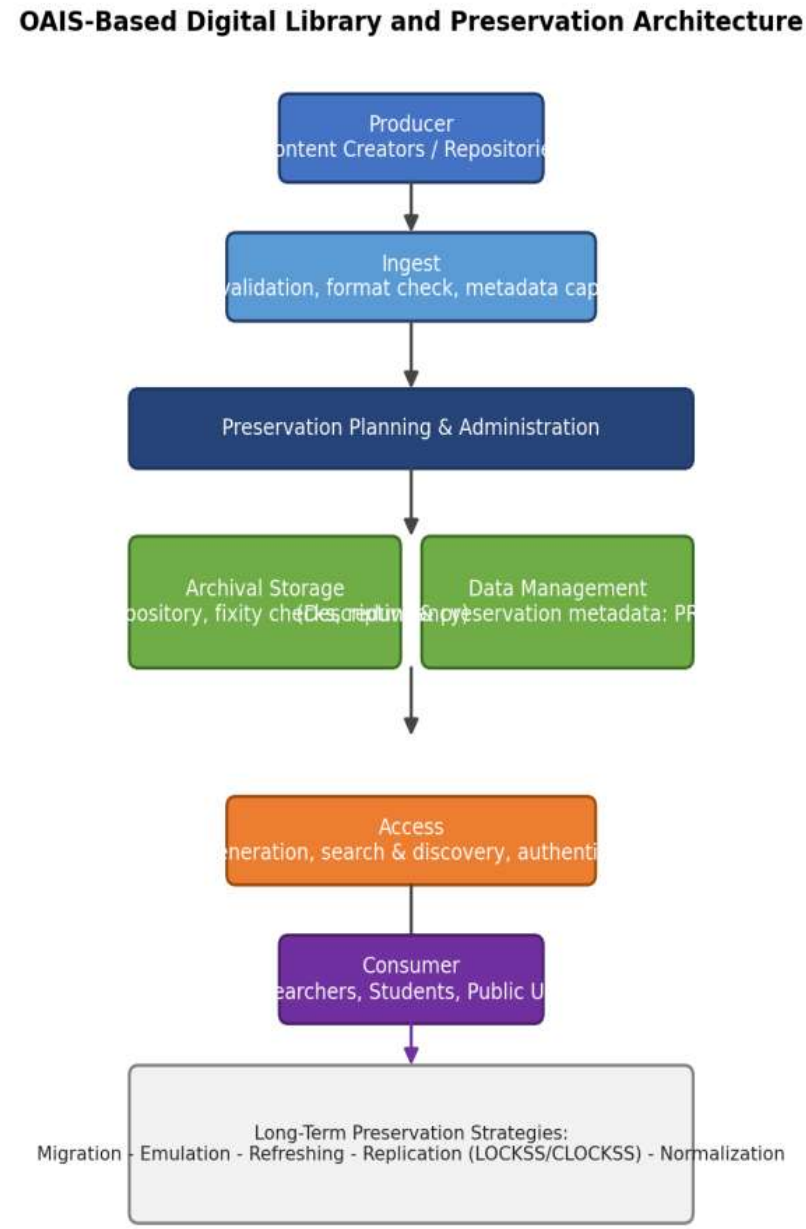

Fig 2. OAIS-Based Digital Library and Preservation Architecture

OAIS deliberately avoids prescribing specific software or storage technologies, functioning instead as a common vocabulary that allows heterogeneous archives -- from national libraries to institutional repositories -- to describe their preservation workflows in comparable terms. This is one reason the model has been adopted so broadly: repository software such as Archivematica explicitly implements OAIS functional entities using a microservices design pattern, while other preservation systems apply the same model within proprietary environments. Preservation metadata schemas extend OAIS by specifying exactly which preservation events, agents, rights statements, and fixity values must be recorded for each digital object, giving institutions an implementable schema rather than an abstract model alone.

A basic fixity check, used throughout OAIS-compliant systems to confirm that a digital object has not been altered or corrupted, can be expressed as a comparison of cryptographic hash values computed at ingest and at a later verification point:

$$H(f_{original}) = H(f_{current}) \quad (1)$$

Where H is a cryptographic hash function (for example, SHA-256) and f is the preserved digital object. If the two hash values diverge, the Archival Storage entity flags the object for corruption remediation, typically by restoring it from a redundant replica.

3.4 Preservation Strategies and Techniques

Four preservation techniques recur throughout current practice. Refreshing copies digital content onto new storage media before the original media degrades, addressing physical bit rot without altering the file format itself. Migration converts digital objects from an obsolete or at-risk format into a current, well-supported format, trading some risk of fidelity loss for continued renderability under modern software. Emulation instead preserves the original file unchanged and recreates the software and hardware environment needed to render it, avoiding format-conversion loss at the cost of maintaining emulation infrastructure. Replication, exemplified by the LOCKSS peer-to-peer model, distributes multiple independent copies of content across geographically separate nodes so that no single point of failure -- technical, organizational, or legal -- can result in permanent loss. Institutions rarely rely on a single technique; OAIS-compliant systems typically combine replication and fixity checking for baseline integrity with periodic migration or format normalization applied selectively to at-risk content, increasingly supported by cloud-based storage infrastructure.

3.5 Evaluation Metrics for Digital Library and Preservation Systems

Because digital libraries must remain both discoverable and preservable, their evaluation draws on two complementary metric families. Retrieval effectiveness is assessed using standard information-retrieval measures -- precision, recall, and F1-score -- applied to search and metadata-matching tasks:

$$\text{Precision} = TP / (TP + FP) \quad (2)$$

$$\text{Recall} = TP / (TP + FN) \quad (3)$$

$$F1 = 2 \times (\text{Precision} \times \text{Recall}) / (\text{Precision} + \text{Recall}) \quad (4)$$

Where TP, FP, and FN denote true positive, false positive, and false negative matches between a user query and the metadata-indexed collection. Preservation effectiveness, by contrast, is typically assessed through operational indicators: fixity-check pass rate, replica count per object, mean time to format-risk detection, and successful-migration rate. Together, these two metric families allow a digital library knowledge system to be evaluated on both its immediate usability and its long-term survivability.

4. REVIEW AND DISCUSSION

This section synthesizes the reviewed framework into comparative tables and figures covering repository platforms, preservation strategies, performance-oriented standards, and open challenges.

Institutional repository platforms differ considerably in how closely they align with the OAIS model, how easily they can be deployed, and how large a support community backs them. Table 2 and Figure 3 summarize a qualitative comparison of five widely adopted platforms.

Platform	Primary Role	OAIS Orientation	Notable Strength
DSpace	Institutional repository (all-in-one)	Partial; commonly paired with external preservation tools	Large global adoption and community support
Fedora	Repository storage layer	Strong; designed for flexible preservation-oriented storage	Highly flexible, requires custom front-end
EPrints	Open-access repository	Partial; focused on scholarly deposit workflows	Simple deployment for research output
Islandora	Fedora-based access and management layer	Strong (inherits Fedora's model)	Rich support for complex digital collections
Archivematica	Dedicated preservation processing system	Full; explicitly implements OAIS entities via microservices	Purpose-built OAIS compliance and metadata export

Table 2. Comparison of Institutional Repository and Preservation Platforms

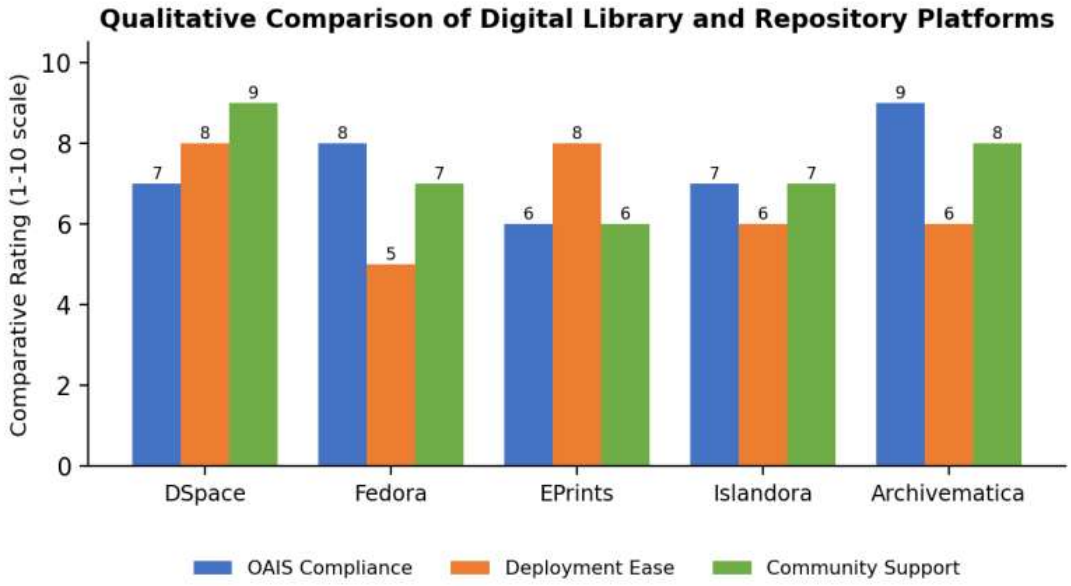

Fig 3. Qualitative Comparison of Digital Library and Repository Platforms

As Figure 3 shows, no platform maximizes all three dimensions simultaneously. Archivematica scores highest on OAIS compliance because it was purpose-built around the reference model, but this specialization means it is typically deployed alongside, rather than instead of, an access-oriented repository such as DSpace or Islandora. DSpace and EPrints score highest on deployment ease and community support respectively, reflecting their long adoption history and out-of-the-box configurability, but neither implements the full OAIS functional set natively. This reinforces the pattern already observed in Table 1: durable digital library knowledge systems are typically assembled by combining an access-oriented repository with a dedicated preservation layer rather than expecting a single platform to satisfy both roles.

Preservation strategy selection shows a similar pattern of complementarity rather than substitution. Table 3 and Figure 4 summarize the relative contribution of the four core strategies discussed in Section 3.4.

Strategy	Primary Risk Addressed	Trade-off	Typical Use Case
Refreshing	Physical media decay (bit rot)	Does not address format obsolescence	Routine storage-media rotation

Migration	Software/format obsolescence	Possible loss of formatting fidelity	Converting legacy documents to current formats
Emulation	Loss of original rendering environment	Ongoing cost of maintaining emulators	Preserving complex or interactive digital objects
Replication (LOCKSS/CLOCKSS)	Single point of failure, organizational loss	Requires multiple independent custodians	Distributed preservation of e-journals and OA content

Table 3. Comparison of Core Digital Preservation Strategies

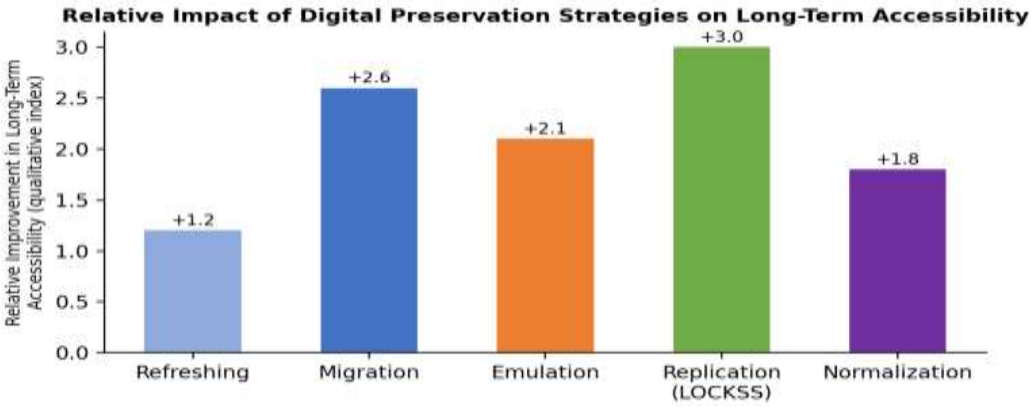

Fig 4. Relative Impact of Digital Preservation Strategies on Long-Term Accessibility

Replication shows the highest relative contribution to long-term accessibility in the synthesized comparison, consistent with the design principle that redundancy across many independently governed nodes is more robust against combined technical, economic, and legal threats than any single archive can be on its own. Migration and emulation both address format-level risk but from opposite directions -- transforming the object versus preserving the rendering environment -- and current practice generally applies them selectively, based on content complexity and available resources, rather than uniformly across an entire collection.

Despite these established strategies, current research repeatedly identifies a consistent set of operational challenges that limit the practical resilience of digital library knowledge systems. Table 4 and Figure 5 summarize these challenges and their reported relative severity.

Challenge	Description	Mitigation Approach
Format Obsolescence	Proprietary or unsupported file formats become unreadable as software evolves.	Preference for open, well-documented formats; scheduled migration
Bit Rot / Media Decay	Physical degradation of storage media causes silent data corruption.	Regular fixity checking and media refreshing
Funding & Resourcing	Preservation is an ongoing cost with no fixed endpoint, straining institutional budgets.	In-house capacity building; shared, cooperative preservation networks
Metadata Interoperability	Divergent metadata schemas across institutions hinder cross-repository discovery.	Adoption of shared descriptive and structural metadata standards
Legal / Rights Management	Copyright and licensing constraints can restrict copying, migration, or access.	Rights metadata embedded in preservation records; trigger-event access models

Table 4. Key Challenges in Digital Preservation and Reported Mitigations

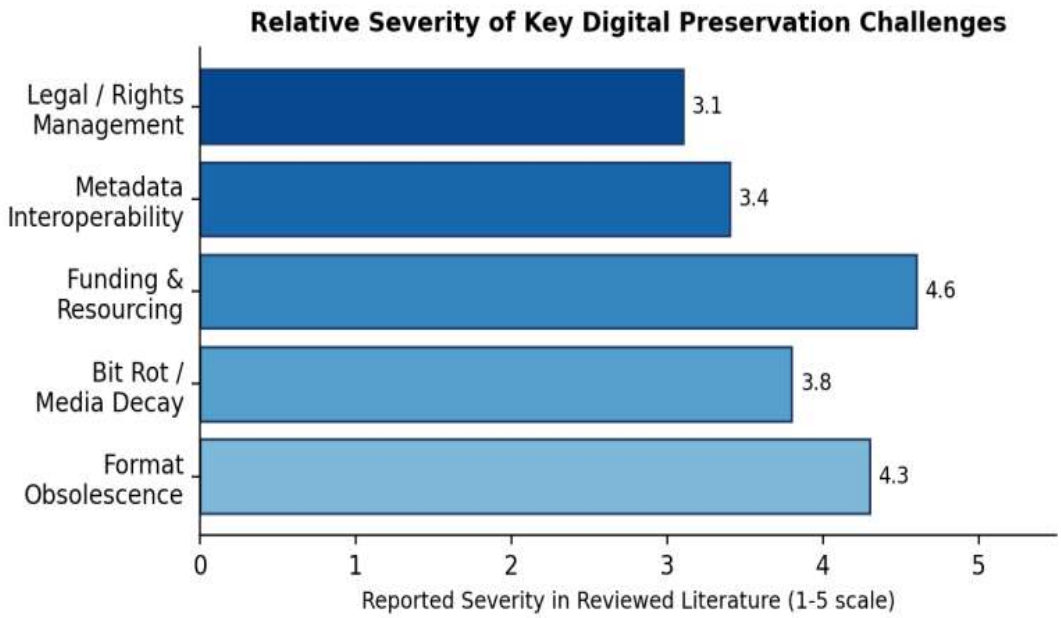

Fig 5. Relative Severity of Key Digital Preservation Challenges

Funding and resourcing emerges as the most severe reported challenge in the synthesized comparison, reflecting the consistent observation that preservation, unlike a one-time digitization project, has no natural completion point and must be sustained indefinitely against a background of shrinking institutional budgets. Format obsolescence and bit rot follow closely, both requiring continuous technical monitoring rather than a single corrective action. Metadata interoperability and rights management, while reported as somewhat less severe individually, compound the other challenges: inconsistent metadata makes it harder to identify at-risk content across a distributed collection, and unclear rights status can prevent an institution from taking the very migration or replication actions needed to preserve a digital object.

Taken together, the evidence reviewed in this section supports a layered response to preservation risk: OAIS-aligned workflows and standardized preservation metadata provide the structural foundation; distributed replication networks such as LOCKSS and CLOCKSS provide resilience against organizational and infrastructural failure; and selectively applied migration or emulation address format-level risk for specific at-risk content classes. No single platform, standard, or strategy reviewed here is sufficient on its own, which explains why mature digital library knowledge systems are consistently built as combinations of access-oriented repositories and dedicated preservation infrastructure rather than as single monolithic systems.

5. CONCLUSION AND FUTURE SCOPE

This review examined the digital library as a knowledge system built from content, metadata, storage, and access services, and digital preservation as the ongoing discipline that keeps that system's content authentic and usable over time. The OAIS reference model provides the conceptual backbone connecting these two concerns, while standardized preservation metadata operationalizes it into implementable practice. The comparative review of repository platforms and preservation strategies shows a consistent pattern of complementarity: access-oriented platforms such as DSpace, EPrints, and Islandora excel at discovery and deposit workflows, while dedicated preservation systems such as Archivematica and distributed networks such as LOCKSS and CLOCKSS provide the OAIS-aligned rigor and redundancy needed for long-term survival. Persistent challenges -- format obsolescence, bit rot, funding sustainability, metadata interoperability, and rights management -- remain only partially resolved by current tools, underscoring that digital preservation is an organizational and economic commitment as much as a technical one.

Future work should explore deeper integration of artificial intelligence for automated metadata generation, format-risk prediction, and anomaly detection in fixity monitoring, reducing the manual overhead that

currently limits preservation scalability at smaller institutions. Cloud-based and federated preservation architectures offer a promising route to shared infrastructure costs across consortia, while blockchain-based fixity and provenance ledgers have been proposed as a means of providing tamper-evident integrity verification independent of any single custodian. Continued convergence between digital library metadata practice and semantic web / linked-data technologies is also likely to improve cross-repository discoverability, moving digital libraries closer to the goal of a genuinely interoperable, resilient global knowledge system.

REFERENCES

1. Ahmad, R., Rafiq, M., & Arif, M. (2024). Global trends in digital preservation: Outsourcing versus in-house practices. Journal of Librarianship and Information Science, 56(4), 1114–1125. https://doi.org/10.1177/09610006231173461
2. Akinola, A., Oso, O. O., Shorunke, O. A., &Oyadele, O. G. (2024). Preservation of theses and dissertations in the era of digitization: A case study of selected universities in Oyo state, Nigeria. Digital Library Perspectives, 40(4), 631–648. https://doi.org/10.1108/DLP-03-2024-0053
3. Adarkwah, M. A., Okagbue, E. F., Oladipo, O. A., Mekonen, Y. K., Anulika, A. G., Nchekwubemchukwu, I. S., Okafor, M. U., Chineta, O. M., Muhideen, S., & Islam, A. Y. M. A. (2024). Exploring the transformative journey of academic libraries in Africa before and after COVID-19 and in the generative AI era. The Journal of Academic Librarianship, 50(4), Article 102900. https://doi.org/10.1016/j.acalib.2024.102900
4. Pasqui, V. (2024). Digital curation and long-term digital preservation in libraries. JLIS.it, 15(1), 109–125. https://doi.org/10.36253/jlis.it-567
5. Harisanty, D., Obille, K. L. B., Anna, N. E. V., Purwanti, E., &Retrialisca, F. (2024). Cultural heritage preservation in the digital age, harnessing artificial intelligence for the future: A bibliometric analysis. Digital Library Perspectives, 40(4), 609–630. https://doi.org/10.1108/DLP-01-2024-0018
6. Kjellström, Z. (2025). Decentralized digital preservation: The LOCKSS initiative and shadow libraries. Online Information Review, 49(8), 62–81. https://doi.org/10.1108/OIR-02-2024-0088
7. M. Ibrahim, H. M., Ahmad, K., &Sallehudin, H. (2025). A cloud-based adoption model for digital preservation services for university libraries. Digital Library Perspectives, 41(4), 615–636. https://doi.org/10.1108/DLP-03-2024-0047
8. Kreutz, C. K., Blum, M., Schaer, P., Schenkel, R., & Weyers, B. (2023). Evaluating digital library search systems by using formal process modelling. In Proceedings of the ACM/IEEE Joint Conference on Digital Libraries (JCDL 2023) (pp. 143–154). IEEE. https://doi.org/10.1109/JCDL57899.2023.00029
9. Kroll, H., Pirklbauer, J., Kalo, J., Kunz, M., Ruthmann, J., & Balke, W. (2024). A discovery system for narrative query graphs: Entity-interaction-aware document retrieval. International Journal on Digital Libraries, 25(1), 3–24. https://doi.org/10.1007/s00799-023-00356-3
10. Athavale, V. A., & Patel, S. T. (2024). Use of blockchain technology for maintaining authenticity and credibility of digital information. In Z. Raza, M. Babenko, M. Sajid, M. Lapina, & V. Zolotarev (Eds.), AISMA-2023: International Workshop on Advanced Information Security Management and Applications (Lecture Notes in Networks and Systems, Vol. 1207). Springer. https://doi.org/10.1007/978-3-031-77229-0_2