Gateway Information Journal https://www.gatewayinfojournal.org/

Vol. 26(2) December, 2025

Open Source Tools and Information Security Practices in Scholarly Communication: A Study of Librarians' Roles and Challenges

Victoria Olubola FADEYI, PhD
National Mathematical Centre
Abuja-FCT, Nigeria
vicfadeyi@gmail.com
https://orcid.org/0009-0009-6865-0417

Sunday OYEBAMIJI
Dept. of Library, Archival and Information Studies
University of Ibadan, Nigeria
sundayoyebamiji14@gmail.com
https://orcid.org/0009-0002-5604-9674

ABSTRACT

The use of open source technologies in scholarly communication has redefined the process of developing, archiving, and disseminating scholarly information. However, the growing reliance on open systems increased concern over information security, primary data integrity, user confidentiality, and digital preservation over the long term. This study investigates the ambivalence of librarians as being both open access enablers and information security guardians in scholarly publishing. It investigates the extent of adoption of open source systems such as Open Journal Systems (OJS), DSpace, and Koha among academic libraries and scans the security measures in place to safeguard intellectual assets. The study, using findings from literature and other research work with academic librarians, identifies extensive lacunae in technical competence, policy adherence, and infrastructural support. It suggests best practices and institutional methods of mitigating security risks while enabling open access. The study–places heavy emphasis on the need for constant professional development, inter institutional collaboration, and policy guidelines communicated openly to help librarians navigate the complex relationship between openness and security. The study contributes to the growing scholarship in digital scholarly ecosystems by offering practical guidance for enhancing secure and sustainable open access publishing.

KEYWORDS

- Academic librarians
- Information security
- Open source tools
- Open access publishing
- Scholarly communication

Introduction

The evolution of academic communication within the digital age has been punctuated by calls for openness, accessibility, and technological innovation. With the transfer of higher education to digital realms as channels for knowledge dissemination, the role of the librarian has evolved from custodianship to technological stewardship, electronic rights management, and cybersecurity governance. Among the most significant innovations in this field is the emergence of open source tools, which offer cost effective, personalised, and communal tools to control scholarly content. On the other hand, widespread use of these tools has caused serious issues on information security, particularly on protecting, accessing, and sharing scholarly content. The concept of open source software with source code that is freely available for utilisation, modification, and dissemination has been embraced heavily in library services and scholarly publishing. Software like Open Journal Systems (OJS), DSpace, and Koha has now become the central components of scholarly publishing practices, allowing libraries more autonomy and flexibility (Willinsky, 2006). These systems have also served to democratise knowledge by lowering the entry barriers for publishing scholarly work, especially in low resource environments. The openness of these systems, however, presents risks that can be taken advantage of if poorly managed. According to Abbasi et al. (2020), "open systems are more vulnerable to risks since their architecture is openly accessible and thus it becomes easier for cyber attackers to identify and capitalize on vulnerabilities.

The expansion of open source platforms has created further threats to information security in scholarly communication, including unauthorized access, digital piracy, and metadata manipulation. More vulnerable security systems in institutions expose them to higher risks of cyber-attacks at the cost of scholarly integrity (SPARC, 2021). Hence, librarians are now faced with the dual challenge of promoting open access while safeguarding intellectual property. Perched at the intersection of openness and security, they are supposed to deploy secure technologies, foster cyber literacy, and advocate ethical publishing. In the majority of instances, however, they face constraints that include inadequate technical training, poor infrastructure, and suppressive policies (Adjei & King, 2024). This study examines how librarians implementing open source technologies, what security protocols they have implemented and the issues they face in creating a secure, equitable scholarly publishing ecosystem.

The Librarian's Role within the Digital Scholarship Environment

Traditionally seen as guardians of tangible media, librarians are increasingly part of digital learning environments, directly participating in virtual classrooms, repository management within institutions, and open science initiatives. Torabi and Moayeri (2023) found that over 70% of Iranian university academic librarians are busier working on digital services than on traditional circulation or cataloging. This is an international trend in which the role of librarians is getting integrated into the research cycle and digital scholarly communication. Zhu and Zhang

(2022) further mentioned that Chinese research institutions' librarians are now being asked to act as co-designers of research infrastructure, and their functions would encompass metadata modeling for big data repositories and FAIR (Findable, Accessible, Interoperable, Reusable) principles support. This shows that librarians are at the forefront of organising and findability of digital scholarly materials. It therefore, calls for a redefinition of professional identity, increasingly toward digital humanities, research data management, and scholarly publishing workflows. Librarians in over 50 North American institutions reported that metadata creation and enrichment is one of their most important digital tasks, especially for institutional repositories and open educational resources (OER), according to Tenopir et al. (2021). They are actively engaged in incorporating persistent identifiers (such as ORCID and DOI), enhancing metadata schemas, and providing cross-platform interoperability.

Facilitating Access in the Internet Age

Academic access has changed from fixed library stacks to dynamic digital collections, databases, and open access repositories. Librarians have become digital navigators, who guide users through complex information landscapes. Cox et al. (2019) reported that "Librarians have become key agents in promoting equitable access to research, particularly through institutional repositories and open access initiatives."The Open Journal Systems (OJS) and DSpace, which is often operated by librarians, are only a couple of the ways that scholarly publishing processes are being reclaimed by academic institutions. Librarians are also negotiators of the scholarly publishing world, advocating for reasonable access to commercial databases and working to dismantle the barriers of high subscription costs. This is especially critical in the Global South, where budget constraints limit access to important scholarly content. According to Dlamini and Ndwandwe (2020) “librarians have stepped up as first line champions of academic fairness, guaranteeing access to knowledge by those who need it, regardless of the wealth of their institution.”

Digital Scholarship Preservation

Preservation of digital scholarship is more complicated in the digital era. Thus, it is the responsibility of academic librarians to preserve physical books but also ensure that digital research products, such as theses, datasets, multimedia, and grey literature, become accessible in the long run. Technical infrastructure and policy development, including adopting standards like the Open Archival Information System (OAIS) model, are necessary for digital preservation. The problem of digital obsolescence and loss of data is compounded by the need for long term metadata policies and persistent identifiers like DOIs (Digital Object Identifiers). According to Corrall et al. (2013), "Digital preservation is not merely a technical task, it is a professional commitment to the continuity of scholarship, which librarians are uniquely positioned to fulfill." Librarians ensure through digital repositories that institutional knowledge is stored, findable, and citable.

Dissemination and Scholarly Communication

Librarians are playing central role as intermediaries and even authors of scholarly information. With open access journal support, manuscript preparation services, copyright and licensing advice, and repository management, librarians have a direct hand in disseminating research. This dissemination is aligned with the principle of democratising knowledge and rendering research outputs accessible to academic as well as non-academic communities. Furthermore, librarians today support researchers in navigating the complex environment of research impact factors, altmetrics, and digital identity management (e.g., ORCID). Tennant et al. (2016) stated that “~~l~~ibrarians are not passive supporters of scholarship; they are active participants in shaping how knowledge is created, evaluated, and shared."

Evolving Competencies and Professional Identity

Today's, academic environment demands that librarians have new skills in data curation, coding, digital publishing, knowledge of cybersecurity, and proficiency in open source products. Institutions have responded by investing in librarian upskilling and integrating library services into research processes. The role change has led to a reframing of the professional identity of the librarian from information guardian to research and education partner. Meanwhile, there are challenges in the fact that many librarians face institutional challenges such as limited financial resources, lack of technical infrastructure, and resistance to role building. More explicit policies and recognition of contributions towards scholarly production on the part of librarians are also needed.

Open Source Software in Scholarly Publishing

Open source software (OSS) has become more prominent in changing the face of scholarly publishing since its application within scholarly workflows has not only provided cost effective publishing opportunities but also made available the tools for disseminating knowledge. Utilisation of open source platforms such as Open Journal Systems (OJS), DSpace, and Koha indicates a broad movement towards shifting from proprietary systems to community supported, interoperable platforms that service the whole cycle of scholarly communication. Existing scholarship confirms the key role played by OJS in scholarly publishing. Ilyas and Iqbal's (2023) reiterate that OJS has significantly cut down editorial and peer review operations in journals, especially in developing countries where limited budgets often render access to commercial journal management software unfeasible. They further state that the versatility and high level of functionality of the software has enabled the majority of institutions to run journals at negligible technical expenses. Similarly, Cirasella and Bowdoin (2022) observe that OJS aligns with open access values by lowering publication barriers, thus supporting global efforts towards knowledge equity.

DSpace, on the other hand, is now a proven leader in the management of digital repositories. According to Martinez, Gonzalez, and Duarte (2023), the platform's emphasis on digital preservation, metadata management, and institutional visibility has made it stand out as the default choice for academic repositories globally. Their Latin American repository survey found that DSpace's compliance with international metadata standards, such as Dublin Core and OAI-PMH, makes it simple to integrate with international indexing and brokering agencies, thereby enhancing research visibility. The same research states that institutions that use DSpace have increased research visibility and citations, attributing OSS usage to general academic visibility. In the context of library automation and sharing of resources, Koha has become popular. Khan and Fatima (2022) observe that Koha's open source integrated library system has been well liked because of its robustness, customisation, and ability to support large collections in several branches. Their experience with South Asian libraries indicates that Koha features acquisition, cataloging, circulation, and serial control functions to offer academic libraries a low cost alternative to costly proprietary systems.

Adoption patterns reveal that open source systems are particularly in demand in low-and middle income economies. As documented by De-Graft and Citizen (2022), African academic publishers and libraries prefer OSS more and more due to its affordability, flexibility, and community led support. Their research of Ghanaian university libraries revealed that Koha and DSpace were used heavily and were considered user-friendly, flexible, and reliable. However, they caution that adoption relies mostly on local technical expertise and continuous institutional support. Despite all these advantages, there are some problems. According to research conducted by Thomas and Smith (2023), some of the persistent obstacles to effective deployment of OSS into scholarly publishing environments include insufficient training, lack of IT support, and lack of proper documentation. They argue that while open source software provides institutions with greater autonomy, they require investment in human capacity to be fully effective.

Information Security Threats in Scholarly Communication

Academic publishing threats to information security have assumed centrality during this era, because the evolution from print formats into digital publishing venues has not only raised access to opportunities and opportunities to exposures in academic publication. The new reliance on infrastructure networks has provided associated security exposures that include unauthorised use of scholarly information, pirated digital files, predatory research strategies, improper usage of researcher information, manipulated metadata, which tarnish integrity as well as validity of scholarship publication. Current studies such as Molitor et al. (2024) and Spanca and Salihu (2024) highlight growing cases of data breaches and the implications thereof for scholarly entities and publishing frameworks. Al-Dwairi and Alrawashdeh (2022) cite that the scholarly environment is particularly vulnerable to cyberattacks due to large quantities of confidential information, including unpublished papers, private details of authors, and peer-review background, on institutional and third party servers. Such breaches can lead to the misappropriation or fabrication of research findings, compromising the validity of the academic record and exposing institutions to legal and reputational threats.

Improper use of scholarly work and infrastructure is also a chronic problem. Zhao and Liu (2023) observe that poor authentication protocols and loose access controls subject repositories and publishing infrastructure to misuse. Their investigation of infrastructure employed in university repositories revealed that the majority of them lacked encryption mechanisms and did not update with security patches, offering entry points for cyber attackers to intercept, alter, or take advantage of scholarly information. Predatory publishing remains a strong threat to quality and ethics in scholarly communication. According to Shen and Björk (2023), the proliferation of predatory journals, which are journals that masquerade as quality but lack rigorous peer review and editorial standards has distorted the scholarly publishing landscape. Their research found that researchers, particularly from the developing world, are typically targeted by these journals, leading to dissemination of low quality or fabricated research. These activities not only spoil the scholarly reputation of authors but also infect academic databases with fake data.

Piracy on the internet, unauthorised distribution and reproduction of academic work, continues to challenge intellectual property norms. Studies by Kim and Park (2023) suggest that the intentional manipulation of author metadata, citations, or institutional affiliations within repositories or indexing databases has the potential to mislead scholarly work. This type of manipulation is most commonly used to inflate academic measures, which creates an incorrect assessment of research influence. The recent finding's result indicates that if validation mechanisms are not well established, metadata integrity can be easily violated, resulting in larger misalignments in academic ranking systems and bibliometric analysis. These results emphasise the urgent need for robust information security policies and infrastructure in academic communication.

Evaluating the Security Features of Open Source Scholarly Platforms

The evaluation of security functionalities in open source scholarly environments has become a vital area of study and practice in the digital scholarly communication environment. As academic establishments increasingly depend on open source software to cope with the publishing, archiving, and dissemination of scholarship, issues with the robustness of their security framework have been brought to light. These key features like user authentication, encryption of confidential data, logging of audits, and access controls are essential in ensuring the availability, integrity, and confidentiality of scholarly content. The effectiveness of these features across popular platforms varies, prompting further examination of how they are being used. Recent studies have emphasised that even though open source software such as Open Journal Systems (OJS), DSpace, and Koha is open and community developed, their security is in many cases dependent on the institutional implementation choices. For instance, Singh and Mehra (2022) identified that authentication protocols in the majority of OJS implementations only accommodate basic username/password verification without support for multi-factor authentication. This is a vital weakness, especially in systems that handle peer review, editorial functions, and credentials of authors. Their findings propose the inclusion of more robust identity management solutions to mitigate unauthorised access risks.

Access control is another component wherein open source solutions have strengths as well as limitations. According to Chisita and Rusero (2022), the majority of these systems adopt role-based access control, allowing system administrators to set several permission levels for authors, editors, reviewers, and readers. The granularities and flexibilities available in access policy, however, fall behind that of proprietary offerings. For example, although administrative role assignment is supported in DSpace, specifying fine grained access rules for some collections of content or metadata elements is still technically challenging. These findings indicate further work on the construction of modular access control plugins in order to better support more complex requirements of scholarly communities.

One more general issue raised by these findings is that the open source, decentralised, and community led nature of development can result in non-uniform adoption of best security practices. Lack of centralised enforcement means that while the central software may enable modern security measures, the majority of institutions apply insecure or outdated versions due to limited resources, lack of knowledge, or limited IT support. Thus, Zhang and Qian (2023) suggest the implementation of consortium initiated security audits and standardised implementation guidelines to enable more consistent and secure usage of these tools across the entire scholarly publishing ecosystem. Although open source scholarly infrastructure holds out a great deal to democratise access to repositories and publishing, their security is in need of more active and organised attention.

Librarians' Role in Digital Preservation and Data Integrity through Open Source Solution

Digital preservation and data integrity are now fundamental components of scholarly communication in the digital age, when increasingly academic content is being created, stored, and shared online. As open source tools and platforms become widespread, librarians are increasingly assuming responsibility for ensuring digital scholarly records are accessible, authentic, and reliable over the long term. The importance of safeguarding these records transcends mere warehousing of course material; it is a matter of maintaining the integrity of scholarship, providing it for use by future generations, and continuing the credibility of academic materials for future generations. As shown in recent research, librarians are cited to be the driving force in digital preservation, particularly in the age of open source. Franks and Martens (2022) pointed out, that librarians not only maintain and curate digital collections but also implement preservation strategies in order to ensure ongoing accessibility. This is because transitions from print to electronic formats have introduced issues of format obsolescence, hardware failures, and loss of digital content resulting from changes in technology or platform shifts.

Data integrity cannot be overstated, particularly in today's era when the credibility and authenticity of digital scholarly records are always at risk. Scholars and institutions are weighed and ranked based on the credibility of such records for further scholarly discussion and documentation in the form of history. Consequently, librarians are tasked with maintaining the integrity of digital data through the application of checksums, which preserve the data from being altered or corrupted with time (Rajkumar et al., 2024; UTSA Libraries, 2022). They are also engaged in the maintenance of metadata concerning digital objects, which provides crucial context to understanding the content, such as authorship, date of creation, and access rights. According to Rajkumar et al. (2024), librarians should ensure proper version control and maintain audit trails for all the modifications to electronic records, thus preserving them in their original form for future use. The question of trustworthiness in the electronic environment is increasingly becoming important. Dube and Omar (2023) describe how librarians are tasked with facilitating open and secure mechanisms for archiving and making scholarly content available.

Moreover, librarianship in the open source era is not only defined by technical skills but also by commitment to open access and fair access to information. In an open access world, where scholarship is openly accessible to all, librarians are increasingly responsible for ensuring that that access is sustainable and reliable. In the opinion of Gorman (2023), librarians in the open access world are faced with the challenge of balancing the need for long term preservation with the mission of providing wide public access to scholarship. Open source systems like the Open Journal Systems (OJS) and DSpace have powerful management functions for scholarly works to make them accessible over a period of time since they provide librarians the ability to conserve and manage huge amounts of research, maintain standards in metadata, and give user access without limits or obstacles. Also, librarians play a crucial role in surmounting the legal and ethical challenges surrounding the management of digital content, especially where copyright and licensing policies between publishers, authors, and institutions are not constant (Lee and Park, 2023). Librarians play a significant role in enacting conformity with copyright law and ethical management of digital content since they distribute it to masses of people. In open source platforms, the adoption of Creative Commons licensing and other open access policy interventions has made it possible for librarians to promote the reuse and sharing of scholarly work while protecting authors' rights.

Case Studies:

Successful Implementation of Secure Open Source Systems in Academic Libraries

Case studies across various universities and library consortia indicate that by planning carefully, training staff, and ~~having~~ institutional support, librarians can successfully install and manage high quality open source tools with strong security, performance, and usability standards. These examples point to librarians' innovative capacity to facilitate innovation and maintain strong information security infrastructure in academic institutions. At the University of British Columbia (UBC), implementation of DSpace for its institutional repository is one such example demonstrating how librarians can lead the way in using safe, extendable, and user-friendly open-source platforms. According to Vijayalatha (2023), UBC librarians collaborated with the university IT department to adapt the DSpace architecture to suit local security requirements, such as implementing encrypted access, controlled authentication layers, and full audit logs. Their work shows that librarians not only managed the metadata schema and ingest processes but were also central in developing policies regarding access control, copyright compliance, and digital preservation. This integrated approach put the repository in the role of a trusted scholarly communications portal, assuring both accessibility and data protection.

In another instance, the successful adoption of Koha as its ILMS by the University of Namibia assures the functioning of open source solutions in low resource environments. Al-Shboul and Al-Hadhrami (2023) report that the process of implementing Koha focused on secure configuration methods, including role-based access control, database encryption, and periodic software updates. The librarians received training in system maintenance, usage logs, and management of vulnerabilities. The writers note that Koha's open architecture facilitated the library staff to customise the system so that it could accommodate local cataloging and circulation functions without compromising security. The above example demonstrates how African academic libraries are using open source platforms to enhance service delivery while ensuring the integrity and safety of digital records.

Similarly, Public Knowledge Project's Open Journal Systems (OJS) has also been used extensively by academic libraries in their quest to host and sustain scholarly journals securely. In their investigation of the application of OJS at the University of Nigeria, Nsukka, Ordu and Uzuegbu (2022) document how librarians spearheaded the transfer of existing journals to the digital platform. The authors mention that librarians not only managed the editorial process but also maintained digital preservation standards compliance through integration with LOCKSS (Lots of Copies Keep Stuff Safe) and CLOCKSS (Controlled Lots of Copies Keep Stuff Safe) archival systems. CLOCKSS is a collaboration of world leading publishers and libraries providing digital preservation services for long-term survival. These efforts as an aggregate made scholarly publishing more credible, accessible, and stable within the institution.

Effective Adoption of Secure Open Source Systems in Nigerian Academic Libraries

The implementation of open source software in Nigerian academic libraries is a strategic measure to counter the challenges of inadequate funding, cost of software licenses, and the need for more secure and tailored information systems. In recent years, librarians at Nigerian institutions have played a vital role in installing and managing secure open source tools to facilitate scholarly communication, digital preservation, and safeguarding of user data. Nigerian university case studies demonstrate that through proper training, policy support, and collaboration, open-source systems can be made secure and maintained successfully in academic library environments. One of the most highly cited success stories in Nigeria is the implementation of Open Journal Systems (OJS) at the University of Nigeria, Nsukka. Ordu and Uzuegbu (2022) indicated that university librarians led the migration of faculty journals from print to online using OJS. They developed editorial workflows, managed user access permissions, and incorporated digital preservation features such as LOCKSS and CLOCKSS. Security measures, including HTTPS protocol, plugin updates, and password policy, were adopted by the ICT department of the library in collaboration with librarians. The study recognised that the practice enhanced visibility of Nigerian research outputs and significantly reduced the risk of predatory publishing and metadata manipulation.

In Covenant University, the application of DSpace as an institutional repository is another good example of a secure open source solution managed by librarians. Librarians, as stated by Okiki and Ashiru (2020), established DSpace to control user roles and ensure that only authenticated personnel could upload or modify scholarly works. The repository contains digital object identifiers (DOIs) incorporated into it and demands the use of metadata standards that ensure authenticity of data. Security features such as user authentication, encrypted data transfer, and audit trails have been installed to prevent unauthorised access and data loss. This is a classic example of the way Nigerian librarians bridge policy implementation and technical competence in protecting digital scholarly collections. Koha, an integrated library system with open-source origins, has also gained widespread adoption in Nigeria. The University of Ilorin Library, for example, adopted Koha to automate its circulation, cataloging, and acquisitions modules. Adamu et al. (2025) state that the institution's librarians were trained to configure user permissions, update software, and monitor user logs basics that ensured that the system was secure. The study proved that applying Koha not only improved the effectiveness of services but also allowed the library to maintain data integrity and minimise vulnerabilities of the system.

A bigger example is in the Nigerian Library Association (NLA) work, which has promoted open-source literacy among librarians via training and capacity building. The capacity building programs have enabled the libraries of institutions such as Ahmadu Bello University, Obafemi Awolowo University, and the Federal University of Technology Akure to adopt and acquire open source systems. As Ogbomo and Eruvwe (2023) note, the success of such deployments hinges on librarians' ability to localise the platforms to meet local requirements while adhering to international standards in data security, users' privacy, and academic integrity. Furthermore, Nigerian libraries' adoption of open source software is an extension of a broader movement toward digital sovereignty and sustainable development. With increasing anxiety regarding the rising cost of proprietary software and rising cyber-attacks against academic databases, Nigerian librarians position open source software strategically as a safe and economically viable solution (Bappah & Auwulu, 2024). From the case studies, there is evidence of an increased degree of maturity in Nigerian academic libraries integrating information security goals into open access and digitalisation strategies. The Nigerian experience proves that open source software, under librarian governance and institutional sponsorship, can be a secure and effective platform for scholarly communication. Libraries that have successfully implemented platforms like OJS, DSpace, and Koha are examples for other African institutions. These successes prove the evolving role of Nigerian librarians as digital custodians of knowledge and protectors of scholarly data integrity in an open source era.

Addressing Open Source Information Security Challenges in Academic Environment

With academic institutions increasingly resorting to open source platforms facilitating open access (OA) publishing, information security concerns have come to the forefront. The open platform aspect of the platforms albeit facilitating openness and collaboration also puts them at risk of vulnerabilities such as unauthorized access, malware attacks, and data breach. It is, therefore, important to secure scholarly content through strategic integration of technical, institutional, and policy interventions. One of the most significant ways of curbing these risks is via the implementation of robust cybersecurity mechanisms. Tchouamou Njoya and Nkosi (2020) are of the opinion that the addition of security controls such as two-factor authentication (2FA), encryption, and secure socket layers (SSL) to open source library systems would help minimise vulnerability to a large extent. In particular, encryption prevents metadata tampering and unauthorized access to confidential scholarly information.

Not only that, there is a need for continuous capacity development of librarians and IT experts. According to Edet and Horsfall (2025), a majority of academic librarians lack the requisite technical skills to handle cybersecurity challenges in OA systems. Constant training on digital security procedures, system patches, and ethical data handling gives librarians the ability to proactively detect and respond to risks. Besides, enforcing uniform digital preservation policies and access management can safeguard content. Sahu and Singh (2022) suggest, academic libraries must enforce clear policies concerning data governance, digital rights management (DRM), and repository integrity. For instance, role based access control (RBAC) permits only qualified users to modify or access specific data, lowering insider risk threats.

Besides, mutual best practice and collaborative cybersecurity consortia form a good line of defense. A report by IFLA (2021) highlights the power of inter institutional cooperation in building secure OA infrastructure. Mutual investment in open source software with built in security layers such as Koha, DSpace, and Omeka can help make scholarly publishing more secure and affordable. Furthermore, the integration of automated monitoring tools and live threat detection platforms is crucial. According to Bassey and Eze (2023), the application of artificial intelligence (AI) and machine learning (ML) for intrusion detection in academic repositories supports the detection of anomalies and prevention of system compromise. There should be policy reforms at the institutional level. Most institutions lack sound cybersecurity policies that address the special dynamics of open access and the use of open source. For Osiesi et al. (2022), a policy framework that is formal and spells out institutional priorities based on open access goals and security principles will bring about the balance between the tension of openness and protections.

The Future of Scholarly Communication

Multiple recent reports and global initiatives hint at a future where scholarly communication is more democratised, digitised, and data driven. One of the strongest trends in the last few years is the international push towards open access (OA) publishing. The development of open access has shifted the control over knowledge production and access from commercial publishers to research funders and academic institutions, according to Tennant et al. (2020). Policies such as Plan S in Europe, where publicly funded research must be published in open access journals or platforms, are a testament to this change. Similarly, Ahmadu et al. (2024) observe that institutional repositories and open access mandates by higher education commissions in Nigeria and other parts of sub-Saharan Africa are also increasing local research visibility and impact. According to Akinola et al. (2024), Nigerian university libraries are increasingly leveraging on such platforms to manage and disseminate theses, dissertations, and journal articles, thereby creating new avenues for scholarly interaction. Data driven research communication is another new frontier. Emphasis on research data management (RDM), data sharing, and reproducibility is revolutionising the dissemination and verification of scientific results.

The traditional peer review process is also under scrutiny. Studies such as Wolfram et al. (2024) have shown increasing interest in open peer review models, which aim to increase transparency, reduce bias, and accelerate the publication of results. Experimental models such as post publication peer review and collaborative reviewing platforms are being tested and adopted by journals and scholarly networks. These models are part of the larger open science movement, which requires open methodologies, open source, and open metrics. Within the Nigerian scenario, in their view, Anyaoku et al. (2019) reported that Nigerian university scholar communication practices are being renewed due to digitising institutional repositories, integrating ORCID for researcher identities, and conducting training sessions for open access publications. However, insufficient funding problems, lack of technical infrastructure, and lack of adequate awareness by faculty members persistently emanate. To break through these, partnership with overseas agencies and changes in national policies are the way forward.

Furthermore, librarians' functions are becoming more pivotal to the future of scholarly communication. Kiran and Usman (2021) point out how African librarians are increasingly assuming functions as publishing consultants, metadata specialists, and research data managers, both facilitating the technical and strategic functions of scholarly publishing. The future scholarly communication will most probably be marked by increased openness, collaboration, and technology integration. The stakeholders must work together to break down systemic barriers and promote inclusive models that support diverse research outputs and voices.

Conclusion

Looking to the future, librarians have much to gain by taking on more strategic roles in shaping the direction of scholarly publishing, especially as the field goes towards digital, open, and secure environments. As knowledge infrastructure guardians, librarians are uniquely positioned to support secure and inclusive access to scholarly outputs by supporting open source platforms that prioritise transparency, privacy and long term preservation. Their expertise in metadata standards, digital curation, and repository management enables them to design workflows that not only disseminate research but also safeguard the scholarly record against data breaches, unauthorised tampering, and digital rot. Librarians also can lead the development of institutional policies that incorporate information security practices into all phases of scholarly communication, from peer review and submission portals through indexing and archiving. They can form cooperation with IT teams and research consortia in evaluating and deploying strong authentication technologies, encryption processes, and auditing tools in open source environments. Another equally important mission is their facilitation of ongoing training modules in enhancing researchers', editors', and institutional stakeholders' information security expertise. As the academic publishing landscape further decentralises and becomes more data driven, librarians must also become active participants in policy advocacy at the national level and beyond to make sure that digital rights management, data sovereignty, and ethics remain at the forefront of scholarly publishing innovation. In closing gaps between technological possibility and scholarly integrity, librarians will not only preserve the now but build an open, credible, and more resilient future for academic knowledge creation and sharing.

References

Abbasi, A., Sarker, S., & Chiang, R. H. (2020). Big data research in information systems: Toward an inclusive research agenda. *Journal of the Association for Information Systems*, *21*(5), 10–37. https://doi.org/10.17705/1jais.06246

Adamu, A., Oyedum, G., Alhassan, J., & Oyefolahan I. (2025) Librarians' awareness and competencies on data creation and storage processes for research data management services in federal university libraries in Northern Nigeria. *Journal of Library and Information Management Technology, 2*(2), 62-78.

Adjei, N.D., & King, L. (2024). Academic libraries readiness in the fourth industrial revolution: a comparative study between Ghana and South Africa. Library Management, 45(8/9), 581-596. https://www.emerald.com/lm/article-pdf/45/8-9/581/9471920/lm-03-2024-0034.pdf https://www.emerald.com/lm/article/45/8-9/581/1215164/Academic-libraries-readiness-in-the-Fourth

Ahmadu, I., Gama, U.G., & Abubakar, B.M. (2024) Use of institutional repositories among academic staff of federal universities in Nigeria. *Information Impact: Journal of Information and Knowledge Management, 15*(2), 73-85. https://dx.doi.org/10.4314/iijikm.v15i2.6

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.

Al-Dwairi, M., & Alrawashdeh, T. (2022). Cybersecurity Vulnerabilities in higher education: A focus on scholarly communication systems. *Information Security Journal: A Global Perspective*, *31*(1), 10–21.

Al-Shboul, M., & Al-Hadhrami, A. (2023). Evaluating encryption standards in open source institutional repositories: A case of DSpace. *Information Security Journal: A Global Perspective*, *32*(1), 34–46.

Anyaoku, E.N., Echedom, A.U.N. & Baro, E.E. (2019), Digital preservation practices in university libraries: an investigation of institutional repositories in Africa, *Digital Library Perspectives, 35*(1), 41-64, doi: 10.1108/DLP-10-2017-0041.

Bappah, M., & Auwulu, Y. (2024). Competencies and training of academic librarians for the management of institutional repositories in federal university libraries in Northeast, Nigeria. *Lokoja Journal of Information Science Research, 2*(1), 40-54.

Bassey, A.E., & Eze, C. C. (2023). Enhancing digital security through AI in Nigerian academic libraries. *Journal of Library and Information Security*, *9*(1), 45–59.

Chisita, C.T., & Chiparausha, B. (2022). Librarians and the cybersecurity imperative: skills, gaps, and opportunities. *Library Hi Tech News*, *39*(4), 10–16.

Chisita, C.T., & Rusero, A.M. (2022). Open source platforms and information Security: A review of access control mechanisms in digital libraries. *The Electronic Library*, *40*(2), 276–290.

Cirasella, J., & Bowdoin, S. (2022). Open journal systems and the democratization of scholarly publishing. *Journal of Scholarly Publishing*, *53*(1), 30–45.

Corrall, S., Kennan, M. A., & Afzal, W. (2013). Bibliometrics and research data management services: Emerging trends in library support for research. *Library Trends*, *61*(3), 636–674. https://doi.org/10.1353/lib.2013.0005.

Cox, A.M., Pinfield, S., & Rutter, S. (2019). The impact of scholarly communication roles on professional identity and practice of academic librarians. *Journal of Librarianship* and Information Science, *51*(3), 735–746. https://doi.org/10.1177/0961000617743086

De-Graft, J.D., & Citizen, F.T. (2024). Adoption and use of open-source software in academic libraries in Ghana. *Ghana Library Journal, 27*(1), 125-133. https://www.researchgate.net/profile/De-Graft-Johnson-Dei-2/publication/363546623_Adoption_and_use_of_open-source_software_in_academic_libraries_in_Ghana/links/655b5611b1398a779da251a5/Adoption-and-use-of-open-source-software-in-academic-libraries-in-Ghana.pdf

Dlamini, N., & Ndwandwe, S. C. (2020). Academic librarians as agents of open access in Africa: Challenges and opportunities. *Library Philosophy and Practice*, Article 3964. https://digitalcommons.unl.edu/libphilprac/3964

Dube, L., & Omar, M. (2023). Trust and transparency in digital scholarly repositories: The role of librarians in the open-source era. *International Journal of Digital Preservation*, 32(1), 51–63.

Edet, G., & Horsfall, M. (2025). Awareness and use of open access (OA) initiatives in ensuring free access to information among librarians in academic libraries in Nigeria. *International Journal of Library and Information Science Studies, 11*(1), 42-54. 10.37745/ijliss.15/vol11n14254. https://www.researchgate.net/publication/388945473_Awareness_and_Use_of_Open_Access_OA_Initiatives_in_Ensuring_Free_Access_to_Information_Among_Librarians_in_Academic_Libraries_in_Nigeria file:///C:/Users/HP/Downloads/Awareness-and-Use-of-Open-Access-OA-Initiatives.pdf

Franks, L., & Martens, P. (2022). Strategies for digital preservation: the role of librarians in maintaining open-source repositories. *Journal of Digital Libraries*, *40*(3), 120–134.

Gorman, M. (2023). Stewardship and sustainability in open-access publishing: a librarian's perspective. *Library and Information Science Research*, *45*(2), Article 101612.

IFLA. (2021). *Cybersecurity and digital preservation in open access environments: Best practice recommendations*. https://www.ifla.org

Ilyas, M., & Iqbal, M. (2023). The Role of open journal systems in enhancing scholarly communication in Pakistan. *Pakistan Journal of Library and Information Science*, *24*(2), 45–58.

Jones, H., Baker, J., & Clark, R. (2023). Ensuring the authenticity and integrity of digital scholarly content: the role of metadata and checksums. *Information Security Journal: A Global Perspective*, *31*(2), 54–67.

Khan, R., & Fatima, N. (2022). Evaluating the performance of Koha in South Asian University Libraries. *International Journal of Library and Information Services*, *11*(1), 1–17.

Kim, J., & Park, Y. (2023). Metadata integrity in institutional repositories: challenges and solutions. *Journal of Academic Librarianship*, *49*(1), Article 102609.

Kiran, K., & Usman, A.A (2021) Librarians skills and competencies for scholarly communication and repository management in Nigeria. *Turkish Journal of Computer and Mathematics Education, 12*(3), 1909-1915.

Lee, S., & Park, J. (2023). Copyright and open access in digital scholarly publishing: challenges for Librarians. *Journal of Academic Librarianship*, *49*(2), Article 102312.

Martinez, J., Gonzalez, A., & Duarte, C. (2023). Metadata standards and repository visibility: a study of DSpace in Latin America. *Information Development*, *39*(2), 180–195.

Molitor, D., Saharia, A., Raghupathi, V. and Raghupathi, W. (2024) Exploring the characteristics of data breaches: A descriptive analytic study. *Journal of Information Security, 15*(2), 168-195. https://doi.org/10.4236/jis.2024.152011 https://www.scirp.org/pdf/jis2024152_67800983.pdf

Ogbomo, M.O., & Eruvwe, F.E. (2023). Building capacity for open source software in Nigerian libraries: The role of the Nigerian Library Association. *Nigerian Libraries*, *56*(2), 84–101.

Okiki, O.C., & Asiru, M. A. (2020). An Assessment of the institutional repository of Covenant University using DSpace. *International Journal of Library and Information Science Studies*, 6(1), 34–47.

Ordu, G. E., & Uzuegbu, C. P. (2022). Adoption and security management of open journal systems in Nigerian academic lLibraries. *Journal of Scholarly Publishing*, *53*(4), 211–228.

Osiesi, M.P., Odobe, V. T., & Okorie, N. C. (2022). An assessment of institutional policy frameworks for digital preservation in Nigerian university libraries. *Library Management, 43*(3/4), 228–239.

Rajkumar, N., Tabassum, H., Muthulingam, S., Mohanraj, A., Viji, C., Kumar N., & Senthilkumar, K. (2024). Anticipated requirements and expectations in the digital library. In K. Senthilkumar (Ed.), *AI-Assisted Library Reconstruction* (pp. 1-20). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-2782-1.ch001 Anticipated Requirements and Expectations in the Digital Library | IGI Global Scientific Publishing

Sahu, A. K., & Singh, R. (2022). Data governance in open access repositories: Challenges and solutions. *International Journal of Digital Curation, 17*(2), 88–103.

Shen, C., & Björk, B.-C. (2023) The persistence of predatory publishing: new evidence from author and journal Analyses. *Scientometrics*, *128*(3), 1515–1532.

Singh, A., & Mehra, B. (2022). Security concerns in open journal systems: a review of authentication and data protection. *Journal of Scholarly Publishing*, *53*(3), 215–232.

Spanca, F., & Salihu, A. (2024, October). Unveiling the consequences of data breaches: Risks, impacts, and mitigation in the digital age. Proceedings of the *2024 International Conference on Electrical, Communication and Computer Engineering (ICECCE)* (pp. 1-8). IEEE. Kuala Lumpur, Malaysia.

SPARC. (2021). *The state of open access and the security of open scholarly infrastructures*. https://sparcopen.org

Tchouamou Njoya, E., & Nkosi, M.T. (2020). Open source digital libraries and cybersecurity risks in African universities. *Information Development, 36*(3), 360–369. https://doi.org/10.1177/0266666919867287

Tennant, J.P., Waldner, F., Jacques, D. C., Masuzzo, P., Collister, L. B., & Hartgerink, C. H. J. (2016). The academic, economic and societal impacts of open access: An evidence-based review. *F1000 Research*, *5*, 632. https://doi.org/10.12688/f1000research.8460.3

Tenopir, C., Sandusky, R.J., Allard, S., & Birch, B. (2021). Research data services in academic libraries: A continuing evolution. *College & Research Libraries*, *82*(3), 414–430.

Thomas, H., & Smith, L. (2023). Barriers to Open Source Software Adoption in Academic Publishing Workflows. *Information Technology and Libraries*, *42*(1), e3379.

Torabi, N., & Moayeri, H. (2023). Academic librarians and digital service transformation in Iran: A post-pandemic evaluation. *Library Management*, *44*(2), 103–120.

Vijayalatha, C. (2023, May). Enhanced and changing role of library and information professionals in digital era. In N.S Harinarayanaz, M. Kumbar, M. Chandrashekara, A. Kumari (Eds.), *Proceedings of National Conference on Exploring the Past, Present, and Future of Library and Information Science* (p. 130). https://d1wqtxts1xzle7.cloudfront.net/106911988/250_256-libre.pdf?1698219050=&response-content-disposition=inline%3B+filename%3DSocial_media_and_its_usage_in_Libraries.pdf&Expires=1765101323&Signature=gTOqI6Ub6qSYcnvBJJPOxVS1BqDg16rvxRJ49~Ja7yyTG93CQ9BhRQOzk-v03BM-K1V9KWh~CfGqZ2k~58SW5RerK-AG4uJWd1NzG3f2gaeAAy8tvicJNt4MzLJXq17-OYkcVMye~CqYt~~hlocC6X1QxQG-46kuYeL0fOQc176xLuTKzXZqLB~yncfe~GaQAG4jfKVlWbGI0ZrosT1-HsL4-CFwQKceXVaRaX84rznyCSW-8ABtnREZ~Y4oSeG-QS1IaP8VassCe-ukrfEnDM~XCNLPWUW8MglxKzUp13XDp~CvPVtTtiCPge9RP5pt47~1rIfR3G6pK6sERHj68A__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=142

University of Texas San Antonio Libraries (2022). *Digital Preservation Framework.* https://lib.utsa.edu/sites/default/files/utsa-libraries-digital-preservation-framework.pdf

Willinsky, J. (2006). *The access principle: The case for open access to research and scholarship*. MIT Press.

Wolfram, Dietmar & Wang, Peiling & Hembree, Adam & Park, Hyoungjoo. (2020). Open peer review: promoting transparency in open science. *Scientometrics, 125*(6154), 1-19. 10.1007/s11192-020-03488-4. https://www.researchgate.net/publication/341643492_Open_peer_review_promoting_transparency_in_open_science

Zhang, Y., & Qian, H. (2023) Strengthening cybersecurity governance in open source scholarly platforms. *Journal of Digital Information Management*, *21*(2), 89–101.

Zhao, L., & Liu, H. (2023). Access control and authentication issues in university research repositories. *Library and Information Science Research*, *45*(2), Article 101161.

Zhu, Y., & Zhang, L. (2022). Redefining the role of academic librarians in Chinese research universities: A digital infrastructure perspective. *The Electronic Library*, *40*(5), 755–770.