Journal of Library Services and Technologies, *7*(2), 142-153, June 2025
ISSN: 2636-7424. https://credence-publishing.com
DOI: http://doi.org/10.47524/jlst.v7i2.154

Integration of artificial intelligence (AI) driven security measures in library systems

Emmanuel Tunde Makinde[1], Joy Ishioma Obanigwe[2], Christiana Onyemowo Otaiku[3] and Simon Bem Tyoyila[4]
[1,4]Nile University of Nigeria, Abuja
[2]Veritas University
[3]Afe Babalola University, Ado-Ekiti, Ekiti State Nigeria
E-mail: [1]emmanuel.tunde@nileuniversity.ng, [2]obanigwej@veritas.edu.com, [3]onyemowochristiana@gmail.com, [4]Simon.tyoyila@nileuniversity.edu.ng,
Cell: [1]+23409158971648, [4]+23407034754448
[4]https://orcid.org/0009-0008-4115-2111

Abstract
With an emphasis on data protection, this research investigates the role of the systems librarian in maintaining cybersecurity within library information systems. The paper highlights the vital roles that systems librarians play in protecting sensitive user data by reviewing the body of literature on the changing state of cybersecurity in libraries using secondary research. Important cybersecurity practices like encryption, access control, and AI-powered security tools are examined, and their effectiveness in library environments is assessed. Proactive measures like frequent security audits, privacy evaluations, and ongoing professional development for library staff are also addressed, as is the moral significance of cybersecurity in libraries, with a focus on the necessity of open and transparent privacy guidelines and adherence to data protection laws like the FCCPA and GDPR. This study provides a thorough framework for systems librarians to successfully handle cybersecurity issues in digital library networks by synthesising current best practices. The findings are intended to help guide the creation of policies, strengthen data security procedures, and strengthen the systems librarian's function in creating safe, user-centred library environments.

Keywords: Cybersecurity, library information systems, systems librarian, data protection

Introduction

Due to the large amounts of sensitive user data that libraries handle, libraries have become attractive targets for cyberattacks because of their increasing reliance on cloud-based platforms and computer networks (Saha, 2024; Persadha et al., 2024). Saha (2024) highlights the seriousness of this concern by citing the 2023 cyberattack on the British Library by the Rhysida hacker group, which serves as an important example of the evolving vulnerability of even highly regarded organisations. Libraries must address several levels of risk mitigation in the face of these growing threats, including protecting user data with encryption, implementing more stringent access controls, and adhering to changing privacy laws (Persadha et al., 2024). Meanwhile, novel innovations like blockchain, biometric authentication, artificial intelligence, and machine learning are being studied for their potential to improve security and operational productivity (Akor et al., 2024). Akor et al. (2024), however, also advised that using these technologies brings with it several challenges, such as compatibility problems, privacy-related ethical considerations, and implementation expenses.

To tackle these cybersecurity issues, a comprehensive and proactive approach is needed. According to Corrado (2024), building robust library systems requires regular security audits, regular staff training, and the incorporation of cutting-edge technologies. This aligns with Tanwar's (2025) recommendation that libraries put multi-layered defence systems that incorporate human awareness, policy, and technical solutions in place. Furthermore, research conducted by Kuzma (2010) demonstrated that several European library systems

continue to be highly susceptible because of inadequate cybersecurity practices in their web applications, underscoring a more widespread problem. Building a culture of cybersecurity awareness among library employees and incorporating machine learning for real-time threat detection are essential, argues Navandar (2022). Additionally, it has been noted that the efficacy of these concepts is frequently diminished when employee-centred approaches are not incorporated (Tanwar, 2025). Developing a knowledgeable, adaptable, and security-conscious staff is as important to achieving strong digital security in libraries as implementing innovative technologies.

AI integration in digital library systems

The delivery of services is being revolutionised by incorporating Artificial Intelligence (AI) into library systems, which is changing user interactions and internal procedures. Hassana Ibrahim and Angela Okpala (2024) note that by automating traditionally tedious and lengthy operations, AI improves efficiency and the user experience. Functions like cataloguing, search optimisation, and virtual reference services increasingly utilise technologies like machine learning and natural language processing (Jan Mohd Mala, 2024). This innovation includes chatbots and AI-powered suggestions that offer library patrons individualised, real-time assistance, increasing engagement and facilitating resource access (Pankaj Kumar & Jyoti, 2024). Aparna Preethi (2024) further observes that these innovative solutions can simplify complex procedures and help with data-driven decision-making in collection administration. However, several fundamental problems must be resolved for these technologies to be implemented successfully, such as guaranteeing data quality and retraining employees to interact with intelligent systems (Hassana Ibrahim & Angela Okpala, 2024).

Even if the advantages of AI in library settings are becoming more widely acknowledged, it is important to keep in mind the serious privacy, transparency, and ethical issues. According to Mallikarjuna (2024), AI could jeopardise user confidence without strong governance by permitting improper or unlawful data acquisition. According to Lo (2023), algorithmic bias is a developing problem that may impact how library resources are accessed and evaluated, perhaps marginalising authors or viewpoints. It is advised that libraries implement ethical frameworks that control the development and application of AI technologies to mitigate these hazards (Mallikarjuna, 2024). To prevent user data incidents, privacy-enhancing solutions like encryption, federated learning, and safe storage techniques have also been suggested (Ikwuanusi et al., 2023). Future studies should focus on creating inclusive, open systems that benefit users without sacrificing privacy as libraries adopt AI (Lo, 2023; Ikwuanusi et al., 2023). The way forward is to balance responsible execution, principled design, and technological advancement.

Privacy concerns in library technology

i. *Risk of algorithmic profiling and unauthorised access:* Libraries collect significant volumes of user data, including demographic information, borrowing patterns, and online interactions. While this data enhances personalised services, it exposes users to risks such as algorithmic profiling and unauthorised data breaches (Ikwuanusi et al., 2023). The potential misuse of this sensitive information highlights the need for robust privacy controls.
ii. *Mismatch between user expectations and librarian practices:* Although library users generally expect their data to be protected, not all professionals rank privacy among their highest ethical priorities. This inconsistency may lead to inadequate safeguards and variable data protection practices, undermining user confidence in digital services (Sturges et al., 2003).

iii. *Limitations of digital authentication technologies:* Digital authentication systems, especially those integrated with artificial intelligence, can compromise user confidentiality if not designed with transparency and accountability. These systems may process personal information in ways that are not fully disclosed to users, raising concerns about consent and data visibility (Dixon, 2008).

iv. *Ethical implications of AI integration:* As libraries adopt AI tools, ethical issues such as fairness, accountability, and data transparency become more prominent. Libraries must align their use of AI with national and institutional ethical standards to ensure safe integration (Al-Suqri & Fatuyi, 2012; Lo, 2023).

v. *Institutional readiness and change resistance:* Adequate privacy protection in AI-enhanced environments also depends on institutional readiness. Libraries may struggle implementing user-centric privacy safeguards without adequate staff training and proactive change management strategies. Strategic collaborations and clear policies are vital to bridge this gap (Mallikarjuna, 2024; Sturges et al., 2001).

Legal and ethical frameworks for data protection in libraries

Today's libraries must maintain free access to a wide range of information resources while maintaining strict data protection regulations. This is a tricky balancing act. According to Ayala (2018), conforming to regulations such as the General Data Protection Regulation (GDPR) improves transparency and gives users more authority over their personal information. Digital footprints, research data, and patron borrowing histories are just a few of the many types of information that libraries control, and they must be handled carefully to avoid security breaches and preserve public confidence (Lund, 2022). In response, a road map for sustainable information governance is provided by ethical guidelines issued by groups like the American Library Association (ALA) and the International Federation of Library Associations (IFLA) (Al-Suqri et al., 2020). To maintain legal adherence and cultivate respectful data interactions with users, libraries have been recommended to establish strong protocols and ethical frameworks (Lund, 2022). Any move toward digital transparency must be complemented with initiatives to protect confidentiality and adhere to changing privacy laws, as noted by Alemneh and Helge (2020).

Incorporating digital technologies and artificial intelligence into library systems further complicates this discussion. There has been much discussion on privacy issues such as algorithmic profiling, data leaks, and illegal access (Ikwuanusi et al., 2023). Addressing these issues while defending user rights requires ethical AI methodologies, such as explainable frameworks and privacy-preserving methods (Ikwuanusi et al., 2023). According to Ayre (2017), libraries must also work with vendors, establish safe authentication procedures, and inform users of their digital rights to manage responsible data. The necessity of following Fair Information Practices is further highlighted by privacy issues related to identifiability and access control (Dixon, 2008). In the meantime, Jones and Salo (2017) have warned that new technologies such as learning analytics could oppose fundamental library ethics, especially those about patron anonymity and intellectual liberty. As Jones and Salo suggest, a proactive way ahead is to integrate ethical ideas into library technologies and governance frameworks actively. In the end, libraries must lead with accountability while striving to develop alongside digital change owing to the convergence of ethics, privacy, and innovation.

Balancing user accessibility and data security

Libraries face difficulty balancing strict data protection in their digital systems with user-friendly access. According to Luo et al. (2023), IT workers frequently must choose between protecting customer privacy from cybersecurity dangers and facilitating easy access to information. As users increasingly rely on electronic resources that require secure

authentication, it is imperative to ensure adherence to technological and ethical norms (Persadha et al., 2024). Authentication systems must reduce access obstacles and prevent breaches, especially for remote users with systemic limits (Felts et al., 2024). The transition from conventional paper-based solutions to entirely digital environments has also brought ethical conundrums about data exposure and identifiability. As Dixon (2008) noted, protecting patron confidentiality, which is legally protected in some jurisdictions, requires best practices that align with Fair Information Standards.

Libraries must create governance frameworks that include privacy and security in their operations, building on these ethical and technological challenges. The significance of adhering to legislative frameworks such as the GDPR, which direct the creation of responsible data practices, is emphasised by Besiri (2024). While minimising data exposure, a privacy-first design strategy based on data anonymisation and shorter retention durations might increase user trust (Al-Suqri et al., 2020). According to Al-Suqri and Fatuyi (2012), safeguarding critical infrastructure and upholding stringent access controls are essential elements of digital resilience. Equally important is transparency; as Allahrakha (2023) notes, libraries must explain the procedures they use to gather, store, and utilise patron data. At the same time, encouraging user education and digital literacy enables people to make knowledgeable privacy judgments (Al-Suqri et al., 2020). Ultimately, maintaining accessibility and data safety in the constantly changing information ecosystem requires an ongoing cycle of assessment, expert collaboration, and ethical response (Besiri, 2024).

Privacy risks associated with AI in digital libraries

The evolving information landscape, shaped by the rapid integration of artificial intelligence (AI) into digital libraries and smart city infrastructures, presents both opportunities and profound ethical concerns. While AI enhances innovation and operational efficiency, its deployment raises the following critical privacy risks that must be systematically addressed:

i. *Unauthorised data access and algorithmic profiling:* The collection and processing of user data without explicit consent remains a significant concern in AI-driven environments. As Ikwuanusi et al. (2023) observed, threats such as unauthorised access to personal data, opaque algorithmic profiling, and compromised security are escalating. This is especially problematic when AI systems monitor user behaviours, such as reading and browsing patterns, without informed agreement, leading to challenges in data ownership and control (Murdoch, 2021).

ii. *Privacy complications in educational and civic applications:* AI technologies used in educational platforms and civic data analysis introduce additional layers of complexity. Systems designed to personalise learning or support governance may unintentionally expose sensitive personal information, threatening student and citizen privacy (Huang, 2023; Xia et al., 2023). These scenarios underscore the importance of contextual safeguards in sensitive domains.

iii. *Lack of informed consent and transparency:* Ethical implementation of AI demands a commitment to user transparency, informed consent, and the principle of data minimisation. According to Ikwuanusi et al. (2023), the absence of these foundational elements erodes public trust in digital systems. Techniques like federated learning and differential privacy offer promising alternatives by facilitating secure, decentralised data processing while protecting individual identities:

iv. *Risks associated with behavioural analytics and biometric technologies:* Integrating behavioural analytics and biometric recognition can improve service delivery and security. However, without proper ethical oversight, these technologies may result in profiling, surveillance, or algorithmic bias (Ikwuanusi et al., 2023). Gilbert (2024)

emphasises that AI development must be grounded in human values, with transparency and accountability as guiding principles.

v. *Legal and ethical concerns in digital authentication:* Digital authentication systems in libraries must comply with existing legal frameworks that protect patron anonymity. In many jurisdictions, these protections are enshrined in law, reinforcing the need for ethical safeguards (Dixon, 2008). One viable solution lies in privacy-first AI models, such as federated learning, that ensure localised and secure data handling (Scripa, 2017).

vi. *Need for robust governance and security protocols:* Finally, responsible AI adoption in digital libraries requires the implementation of comprehensive data governance mechanisms, end-to-end encryption protocols, and clear regulatory frameworks. These measures support a balanced and user-centred approach to AI integration (Ikwuanusi et al., 2023; Gilbert, 2024), ensuring that innovation does not come at the cost of individual privacy.

AI-driven security measures in library systems

In contemporary library settings, where sensitive patron data is frequently stored and accessed, artificial intelligence (AI) has become critical to strengthening cybersecurity. When deployed responsibly, AI technologies enhance the resilience of digital infrastructures and ensure user privacy and institutional integrity. In order to strengthen cybersecurity, ensure user and institutional integrity, the following AI-driven security measures in the library systems are necessary:

i. *Real-time threat detection through intelligent monitoring:* AI algorithms are increasingly utilised to monitor network traffic and detect real-time anomalies. Suparman et al. (2024) highlight that these systems enable the rapid identification of potential cyberattacks by analysing irregular activity patterns, thereby enhancing the responsiveness and accuracy of security protocols in libraries and similar information environments.

ii. *Proactive defense using deep learning architectures:* Deep learning models, particularly recurrent neural networks (RNNS) and convolutional neural networks (CNNS), have increased the reliability and adaptability of AI security frameworks. These models allow systems to learn from historical data and evolve to detect new threat patterns, offering libraries a proactive defence mechanism (Suparman et al., 2024).

iii. *Reduction of human error through automation:* AI reduces the risk of human error by automating threat detection, response coordination, and dynamic behavioural analysis. Rangaraju (2023) notes that automated incident response mechanisms enabled by AI can initiate countermeasures without requiring manual oversight, significantly decreasing response time and improving overall system robustness.

iv. *Predictive analytics for future threat assessment:* Predictive analytics powered by AI enables institutions to anticipate potential threats by recognising trends from historical cyber incidents. According to Kashyap (2024), this approach facilitates pre-emptive adjustments in security protocols, essential for institutions like libraries that manage evolving digital collections and access services.

v. *Integration of privacy-preserving techniques:* Security must not compromise user privacy. Privacy-preserving AI models such as federated learning and differential privacy offer secure alternatives by decentralising data processing. These models allow local analysis of user data while safeguarding anonymity, reducing the risk of breaches due to centralised storage (Ikwuanusi et al., 2023).

vi. *Ethical governance and user-centric deployment:* Ethical deployment of AI in library systems requires strict adherence to principles of informed consent, transparency, and fairness. Ikwuanusi et al. (2023) argue that successfully integrating AI into library cybersecurity strategies must account for algorithmic bias, user autonomy, and data ownership, ensuring that technological benefits do not undermine fundamental rights.

User perceptions and concerns regarding data security

Both exciting opportunities and important responsibilities come with integrating AI into library services, especially when protecting user privacy and data security (Ikwuanusi et al., 2023; Chakala, 2024). Although users appreciate the effectiveness and ease of use of AI-powered applications, worries about data breaches, unauthorised access, and possible misuse of private data remain; these concerns should not be disregarded (Ikwuanusi et al., 2023). Ikwuanusi et al. stress the significance of incorporating ethical principles into AI design, emphasising the functions of data ownership, user consent, and privacy-preserving techniques like federated learning and differential privacy. Dixon (2008) asserts that these methods preserve analytical skills while lowering the dangers connected to centralised data storage. To strengthen user confidence, libraries are encouraged to openly discuss their data practices and adhere to accepted ethical frameworks (Sutlieff & Chelin, 2010). It has been noted that even while most libraries currently follow good privacy practices, increased technological complexity and surveillance require even more attention to detail and flexibility (Sutlieff & Chelin, 2010). Chakala (2024) emphasises that to guarantee that AI improves rather than detracts from the library experience, significant AI adoption must coexist with staff training, interdisciplinary collaboration, and a user-first approach.

Challenges in balancing security with accessibility

The evolution of digital libraries has significantly expanded access to information, yet it has also introduced complex security and ethical challenges. Balancing open, equitable access with robust cybersecurity protections remains a persistent issue for library systems globally. The following challenges highlight critical areas of concern:

i. *Balancing accessibility and privacy protection:* A central tension in digital libraries is safeguarding user privacy while ensuring equitable access to information. As Al-Suqri and Fatuyi (2012) argue, this balance becomes increasingly complex as library platforms scale, requiring nuanced strategies to protect sensitive user data without undermining access. Overemphasis on security can inadvertently create barriers for legitimate users, particularly those in remote or underserved communities.

ii. *Usability limitations of authentication systems:* Authentication protocols are essential for digital security but may pose usability issues. Felts et al. (2024) note that multi-step or technologically demanding authentication systems can discourage use by individuals with limited digital literacy or unreliable internet access, effectively excluding them from library resources.

iii. *Ethical concerns in user data management:* Maintaining ethical standards in the management of user data is another ongoing challenge. Dixon (2008) underscores the importance of fair information practices, including transparency, informed consent, and limited data retention. Failure to meet these ethical standards risks eroding public trust and violating legal protections surrounding patron anonymity and data rights.

iv. *Structural vulnerabilities in decentralised systems:* Digital library infrastructures often employ decentralised or agent-based architectures to enhance scalability and autonomy. However, this design also introduces unique vulnerabilities. Vemulapalli et al. (2002) caution that such systems require security measures that extend beyond

traditional protocols, incorporating performance guarantees to protect against evolving cyber threats.

v. *Lack of adaptive and user-centric security frameworks:* To keep pace with emerging risks, digital libraries must implement flexible, adaptive security models that can evolve alongside technological advancements. Felts et al. (2024) advocate for dynamic frameworks that combine technical safeguards with user education and collaboration with cybersecurity experts. This holistic approach strengthens resilience while maintaining digital libraries' accessibility and educational mission.

Comparative analysis of best practices in AI-enhanced library systems

AI-enhanced library systems evolve as institutions adapt technologies to improve services, security, and user access. While strategies may differ across regions and institutions, emerging best practices are shaping how libraries responsibly deploy AI. The following practices represent key approaches that balance innovation with ethical and operational concerns.

i. *Adoption of user-centric AI interfaces:* Libraries are increasingly implementing AI technologies that enhance user experience and accessibility. Chakala (2024) highlights that AI tools such as voice-activated search, automated metadata tagging, and personalised recommendations empower diverse user groups, including those with disabilities, to engage with digital resources more effectively. These tools facilitate inclusive access and optimise information discovery across demographics.

ii. *Implementation of AI-driven security mechanisms:* Libraries are integrating AI-enabled security features to protect intellectual property and sensitive user data. Mallikarjuna (2024) notes that AI-assisted copyright monitoring, behavioural anomaly detection, and digital rights management systems help libraries mitigate cyber risks and ensure regulatory compliance. These tools serve as critical safeguards in the protection of digital assets.

iii. *Use of scalable, context-sensitive AI solutions:* Institutional context heavily influences the type of AI solutions adopted. Adewojo and Dunmade (2024) explain that while technologically advanced institutions employ deep learning models for automated decision-making and resource forecasting, libraries in resource-constrained environments benefit from scalable, cloud-based AI platforms that offer cost-effective access to advanced features without extensive infrastructure.

iv. *Promotion of transparent and ethical AI use:* Ensuring fairness and accountability in AI operations is vital. Gajbhiye (2024) emphasises the role of transparent AI practices in eliminating algorithmic bias and ensuring equitable information access. This includes adopting explainable AI models and ethical auditing practices that help foster user trust and institutional credibility.

v. *Continuous user feedback for adaptive AI refinement:* Libraries that actively gather and incorporate user feedback into AI system design achieve better alignment with real-world needs. Chakala (2024) and Adewojo & Dunmade (2024) argue that iterative feedback loops improve service responsiveness, identify accessibility gaps, and enable AI tools to evolve alongside user expectations and technological trends.

Conclusion

There are many chances to improve resource management, boost security, and improve user experience by integrating AI into digital library systems. AI-powered solutions like predictive analytics, tailored recommendations, and automated cataloguing have completely changed how libraries function and improved the effectiveness and usability of information access. However, these developments also bring new difficulties, especially in data privacy, moral AI

applications, and striking a balance between security and usability. To preserve ethical norms, guarantee transparency, and safeguard user data while preserving easy access to knowledge, libraries must properly apply AI technologies.

Institutions should implement best practices that prioritise user-centered methods, strong security measures, and responsible AI deployment to create a long-lasting and successful AI-enhanced library system. the order to fill the current research gaps and improve AI applications for the changing requirements of digital libraries, cooperation between libraries, legislators, and technology developers is essential. Future studies should concentrate on reducing the hazards associated with AI, guaranteeing inclusivity, and regularly evaluating how AI affects library services. Libraries can fully utilise AI while preserving data security, user confidence, and academic integrity by balancing innovation and ethical responsibility.

The following are recommended in the light of what has been presented in the paper:

1. *Strengthen data security with encryption and access controls***:** A multi-layered security approach, incorporating cutting-edge access control and encryption techniques, is advised to improve the security of digital libraries. By allocating user permissions according to predetermined roles, Zhou et al. (2013) contend that Role-Based Access Control (RBAC) is a flexible and successful methodology for managing data access that streamlines administrative duties and guarantees users access only to what they need. This is corroborated by Pritam et al. (2016) and Zhou et al. (2013), who stress that integrating RBAC with strong encryption techniques greatly improves data security, especially in cloud-based settings. Furthermore, Abduhari et al. (2024) stress the significance of putting Multi-Factor Authentication (MFA) into practice, pointing out that it offers the best level of security against unwanted access, outperforming more conventional techniques like strong passwords and even RBAC alone. To protect the confidentiality and integrity of digital resources while promoting user confidence and institutional legitimacy, the best security framework for digital libraries is a thorough, tiered approach incorporating MFA, RBAC, and encryption techniques.
2. *Adopt privacy-focused ai and data minimisation strategies:* Federated Learning (FL), a crucial tactic for safeguarding user privacy while utilising artificial intelligence, is recommended for libraries. According to Yang (2021) and Kosaraju (2024), FL is a promising privacy-preserving AI technology that enables decentralised model training, significantly lowering the possibility of data exposure by keeping data on local devices or servers and sharing only model updates. Libraries that frequently handle sensitive user data will benefit from this. According to Ikwuanusi et al. (2023), FL helps libraries safeguard user data from breaches and illegal access, particularly as AI-driven applications proliferate. Libraries must incorporate additional privacy-enhancing technologies, including encryption and differential privacy, to improve data security. These technologies can work with FL to create a stronger privacy framework. Furthermore, Ikwuanusi et al. (2023) emphasise the significance of putting ethical AI techniques into reality, such as getting user consent and using data minimisation principles, which promote user trust and guarantee adherence to privacy laws like the FCCPA and GDPR. Libraries may create safe, user-centered environments that protect privacy and make the most of AI using these all-encompassing strategies.
3. *Enhance transparency and user control over data:* To increase openness and foster user trust, libraries should place a high priority on creating privacy policies that are understandable, accessible, and easy to use. To ensure that users can understand how their data is gathered, stored, and utilised, privacy policies must be stated in clear

language rather than legalese, as stressed by Lobato et al. (2009). Libraries must empower patrons by providing privacy settings that give them control over their data and clear policies. Furthermore, according to Lobato et al. (2009), features that allow users to request the deletion of stored data, anonymise search history, or opt out of data collecting are essential for upholding user autonomy and safeguarding their digital footprints. The usefulness of web extensions that graphically describe privacy policies makes them easier to understand. It empowers users to make knowledgeable decisions regarding their data, as Brunotte et al. (2022) demonstrated. By combining these tactics, libraries may make their digital systems more transparent and user-friendly.

4. *Conduct regular privacy audits and staff training:* Libraries must conduct regular privacy assessments and third-party audits to proactively uncover potential vulnerabilities in their systems and guarantee compliance with data protection laws like the FCCPA and GDPR. Regular audits are essential for upholding accountability and transparency since they enable libraries to identify security flaws before they can be exploited, according to Ikwuanusi et al. (2023). Furthermore, it should be prioritised as continuing cybersecurity training is crucial for library employees to stay current with new threats and data protection best practices. According to Ikwuanusi et al. (2023), knowledgeable employees are essential to protecting sensitive user data and maintaining the organisation's privacy requirements. By incorporating these safeguards, libraries may guarantee that their systems stay safe and adaptable to changing privacy issues.
5. *Leverage ai for security monitoring and collaborative protection:* Libraries must implement AI-powered security technologies to bolster their defences against changing cyberthreats. According to Kashyap (2024), these systems can scan vast amounts of data, identify odd trends like illegal access or questionable activities, and react quickly to reduce risks. Palthya (2021) further underlines that AI-driven security technologies provide improved speed and accuracy in threat identification compared to traditional techniques. In addition to putting AI technology into practice, libraries should actively collaborate with cybersecurity specialists, data protection organisations, and legislators to develop strong privacy frameworks that consider new and existing dangers. Libraries can promote safer digital spaces for patrons and strengthen public trust by exchanging best practices and remaining updated through these collaborations.

References

Abduhari, E. S., Shaik, T. C., Adidul, A. B., Ladja, J. H., Saliddin, E. S., Adin, A. J., Rumbahali, F. A., Sali, A. B., Jemser, J. M., & Tahil, S. K. (2024). Access control mechanisms and their role in preventing unauthorised data access: A comparative analysis of RBAC, MFA, and strong passwords. *Natural Sciences, Engineering and Technology Journal*. https://doi.org/10.37275/nasetjournal.v5i1.62

Adewojo, A. A., & Dunmade, A. O. (2024). From big data to intelligent libraries: Leveraging analytics for enhanced user experiences. *Business Information Review*. *41*(3). https://doi.org/10.1177/0266382124126470

Akor, S. O., Nongo, C., Udofot, C., & Oladokun, B. D. (2024). Cybersecurity awareness: Leveraging emerging technologies in the security and management of libraries in higher education institutions. *Southern African Journal of Security 2* (July):14 pages. https://doi.org/10.25159/3005-4222/16671.

Al-Suqri, M. N., & Fatuyi, E. O. (2012). Security and privacy in digital libraries: Challenges, opportunities and prospects. *International Journal of Digital Library Systems, 3*, 54–61.

Al-Suqri, M. N., AlKindi, S. S., & Saleem, N. E. (2020). User privacy and security online: The role of information professionals, ABC-CLIO.

Alemneh, D. G., & Helge, K. (2020). Providing open access to heterogeneous information resources without compromising privacy and data confidentiality, pp.131-152 DOI:10.1201/9781003042235-7

Allahrakha, N. (2023). Balancing cyber-security and privacy: Legal and ethical considerations in the digital age. *Legal Issues in the Digital Age*. *Legal Issues in the Digital Age*, *4*(2), 78-121. https://doi.org/10.17323/10.17323/2713-2749.2023.2.78.

Ayala, D. (2018). Shore to shore: How Europe's new data privacy laws help global libraries and patrons. *International Information & Library Review, 50*, 212–218.

Ayre, L. B. (2017). Protecting patron privacy: Vendors, libraries, and patrons each have a role to play. *Collaborative Librarianship, Vol. 9: Iss. 1, Article 2*.https://digitalcommons.du.edu/collaborativelibrarianship/vol9/iss1/2

Besiri, D. (2024). Information governance in the age of data privacy: Balancing security and accessibility. *Human Computer Interaction*. 8(1):159 DOI:10.62802/8awbd485

Brunotte, W., Chazette, L., Kohler, L., Klünder, J. A., & Schneider, K. (2022). What about my privacy? Helping users understand online privacy policies. In *Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering*.

C, M. (2024). Integrating artificial intelligence in academic libraries. *DESIDOC Journal of Library & Information Technology*. 44(2):124–129. DOI:10.14429/djlit.44.2.18958

Carter, J., Podpadec, T., Pillay, P., Babayiğit, S., & Gazu, K. A. (2024). A systematic review of the effectiveness of reading comprehension interventions in the South African multilingual context. *Educational Research and Evaluation, 29*(1–2), 69–103. https://doi.org/10.1080/13803611.2024.2314522

Corrado, E. M. (2024). Cybersecurity and libraries. *Technical Services Quarterly, 41*, 82–95.

Dahlian Persadha, P., Judijanto, L., Susanti, M., & Kreshna Reza, H. (2024). Data privacy and security protection strategies in library electronic resources management. *Holistik Analisis Nexus* 1(7):115-122. DOI:10.62504/nexus742

Dixon, P. (2008). Ethical issues implicit in library authentication and access management: Risks and best practices. *Journal of Library Administration, 47*, 141–162.

Felts, J., Green, D. W., Ragucci, M., & Enoch, T. (2024). Open the gate! Ensuring easy authentication while mitigating cybersecurity risks. *NASIG Proceedings*.

Gajbhiye, C. K. (2024). Impact of artificial intelligence (AI) in library services. *International Journal for Multidisciplinary Research*. 2582-2160, www.ijfmr.com.

Gilbert, C. (2024). The convergence of artificial intelligence and privacy: Navigating innovation with ethical considerations. *International Journal of Scientific Research and Modern Technology (IJSRMT)*. 3(9):9-17, DOI:10.38124/ijsrmt. v3i9.45

Hongchang, W., Qian, W., & Xuefang, W. (2012). The security design of digital library. In *2012 International Conference on Computer Science and Service System* (pp. 339–342).

Ibrahim, H., & Okpala, A. (2024). Exploring the integration of artificial intelligence in Nigerian library services. *International Journal of Knowledge Dissemination*. *5*(1), 55–65. Retrieved from https://ijkd.uniabuja.edu.ng/index.php/ijkd/article/view/98

Ikwuanusi, U. F., Adepoju, P. A., & Odionu, C. S. (2023). Developing predictive analytics frameworks to optimise collection development in modern libraries. *International Journal of Multidisciplinary Research Updates.* International Journal of Scientific

Research Updates, 2023, 05(02), 116–128 DOI: https://doi.org/10.53430/ijsru.2023.5.2.0038

Jones, K. M., & Salo, D. (2017). Learning analytics and the academic library: Professional ethics commitments at a crossroads. *College & Research Libraries, 79*, 304–323.

Jyoti, K. P. (2024). Reshaping the library landscape: Exploring the integration of artificial intelligence in libraries. *IP Indian Journal of Library Science and Information Technology, 9*(1), 29–36.

Kashyap, S. (2024). The influence of artificial intelligence on cybersecurity. *International Journal of Innovative Research in Computer and Communication Engineering*. Volume 12, Special Issue 1.

Kuzma, J. (2010). European digital libraries: Web security vulnerabilities. *Library Hi Tech, 28*, 402–413.

Kosaraju, D. (2024). Securing AI: Federated learning as a tool for privacy preservation. *Galore International Journal of Applied Sciences and Humanities*. Vol. 7; Issue: 1; DOI: https://doi.org/10.52403/gijash.20230109

Lo, L. S. (2023). AI policies across the globe: Implications and recommendations for libraries. *IFLA Journal, 49*, 645–649.

Luo, A. F., Warford, N., Dooley, S., Greenstadt, R., Mazurek, M. L., & McDonald, N. (2023). How library IT staff navigate privacy and security challenges and responsibilities. *USENIX Security Symposium*.

Lobato, L. L., Fernández, E. B., & Zorzo, S. D. (2009). Patterns to support the development of privacy policies. In *2009 International Conference on Availability, Reliability and Security* (pp. 744–749).

Lund, B. D. (2022). Libraries in a world of data. *Advances in Library and Information Science*. pp.182–196 DOI:10.4018/978-1-7998-8942-7.ch011

Mala, J. M. (2024). From Dewey to deep learning: Exploring the intellectual renaissance of libraries through artificial intelligence. *Journal of Information and Knowledge, 61*(1), 29–38. https://doi.org/10.17821/srels/2024/v61i1/171001

Mallikarjuna, C., An Analysis of Integrating Artificial Intelligence in Academic Libraries (April 04, 2024). Available at SSRN: https://ssrn.com/abstract=4898532 or http://dx.doi.org/10.2139/ssrn.4898532

Navandar, P. (2022). Enhancing cybersecurity in the digital age: Challenges and strategies. *Journal of Artificial Intelligence & Cloud Computing*. SRC/JAICC-313. DOI: doi.org/10.47363/JAICC/2022(1)294

Palthya, R. (2021). AI-based systems enhance cybersecurity defences and identify and mitigate cyber threats in real time. *International Journal of Science and Research (IJSR)*. Vol 10 Issue 6, pp. 1859-1864 DOI: https://dx.doi.org/10.21275/SR24827013755

Pritam, D., Student, M. E., & Professor, M. C. (2016). Enforce role-based access control for secure data storage in the cloud using authentication and encryption techniques—Journal *of Network Communications and Emerging Technologies (JNCET)*, *6*(4).

Preethi, M. A. (2024). Transforming libraries: The impact of artificial intelligence. *International Journal of Scientific Research in Engineering and Management*. 08(10):1-6 DOI:10.55041/IJSREM38103

Rangaraju, S. (2023). Secure by intelligence: Enhancing products with AI-driven security measures. *EPH - International Journal of Science and Engineering*. 9(3):36-41DOI:10.53555/ephijse. v9i3.212

Saha, R. (2024). Data privacy and cyber security in digital library perspective: Safeguarding user information. *International Journal of Scientific Research in Engineering and Management*. 08(04) DOI:10.55041/IJSREM30761

Scripa, Andrea, Artificial Intelligence as a Digital Privacy Protector (December 14, 2017). 31 Harv. J.L. & Tech. 217 (2018), Available at SSRN: https://ssrn.com/abstract=3088118

Suparman, A., Akhmad, E. P., & Dinata, B. M. (2024). Leveraging artificial intelligence for enhancing cybersecurity: A deep learning approach to real-time threat detection. *The Journal of Academic Science*. 1(7):835-842 DOI:10.59613/0yv79c49

Tanwar, P. R. (2025). Cybersecurity challenges. *International Journal for Research in Applied Science and Engineering Technology*. 13(1):564-566DOI:10.22214/ijraset.2025.66263

Vemulapalli, S., Halappanavar, M. M., & Mukkamala, R. (2002). Security in distributed digital libraries: Issues and challenges. In *Proceedings. International Conference on Parallel Processing Workshop* (pp. 480– 486).

Yang, Q. (2021). Toward responsible AI: An overview of federated learning for user-centred privacy-preserving computing. *ACM Transactions on Interactive Intelligent Systems, 11*, 32:1–32:22.

Zhou, L., Varadharajan, V., & Hitchens, M. (2013). Achieving secure role-based access control on encrypted data in cloud storage. *IEEE Transactions on Information Forensics and Security, 8*, 1947–1960.