Journal of Advances and Scholarly Researches in Allied Education
Vol. 23, Issue No. 1, January-2026, ISSN 2230-7540

DOI: https://doi.org/10.29070/zrzznd75

A Review of Trends and Issue of Cybersecurity and Privacy Challenges in Digital Libraries

Dr. Anju Singh [1] *

1. Librarian, Government Pandit Madhav Rao Sapre College, Chhattisgarh, India
12anju15@gmail.com

Abstract: <p style="text-align: justify; line-height: 150%; margin: 0in 0in 10.0pt 0in;">The digitization of digital libraries has transformed them into an important infrastructure to access, preserve, and share knowledge; yet, their speedy transformation and reliance on networked technologies have increased the vulnerability of Cybersecurity and privacy. This paper reflects on recent developments, risks, and unsolved challenges in Cybersecurity and privacy in digital libraries. The study synthesizes evidence on the major vectors of attack, including phishing, Ransomware, insider threats, and third-party supply-chain vulnerabilities based on peer-reviewed literature, international guidelines, incident reports, and trustworthy web-based sources. Special focus is made on the privacy dilemmas of the user data collection and processing, such as search history, logs of access, and authentication credentials, which prompt privacy concerns of surveillance, profiling, and adherence to regulations. The paper also examines the systems of governance, policy measures, and technical protection taken by libraries, and identifies areas of discrepancies between suggested standards and practice. New threats of cloud systems, discovery systems powered by analytics, and artificial intelligence are discussed, too. The paper concludes by stating that even though awareness of Cybersecurity and privacy has grown, digital libraries are still unprepared, and integration of governance, privacy-by-design, and continued investment in security capabilities are needed.

Keywords: Digital libraries, Cybersecurity, Privacy, Ransomware, Data protection, Information security, Governance

X

INTRODUCTION

Digital libraries have become an essential platform of modern knowledge societies, facilitating the storage of information in digital format, organization, dissemination, and long-term preservation of scholarly, cultural, and administrative information. Academic libraries, national libraries, public libraries, and specialized repositories are turning to digital platforms to offer 24-hour access to electronic journals, e-books, digitized manuscripts, institutional repositories, and research data (Saha, 2024). Although the change has ensured that information access has been greatly increased and the physical geographical barriers have been minimized, it has also subjected libraries to a fast-changing environment of Cybersecurity attacks and privacy risks (Akor, S. O., Nongo, C., Udofot, C., & Oladokun, 2024). Events of Ransomware, data breaches, service disruptions, and unauthorized surveillance acts in recent years have proven that digital libraries are no longer marginal targets but are an inseparable part of the global cyber ecosystem (Rahim, 2024).

The Contemporary Information Environment: The Digital Libraries

Digital libraries are not just electronic continuations of traditional libraries, as they are highly elaborate socio-technical systems that incorporate information technologies, network infrastructures, human participants, and structures of governance. These systems generally consist of discovery layers, content

management systems, authentication systems, cloud-based storage, and interventions to third-party publishers and aggregators (Mohanraj, 2024). The environment in which libraries operate has been profoundly integrated with other vendors and service providers as libraries continue to embrace cloud computing, federated search tools, and application programming interfaces (APIs). The result of this interdependence has increased scalability and efficiency, as well as increased the attack surface that can be used by malicious actors (Veeran, R., & Gunasekaran, 2024). Libraries across the world have been urged to digitize collections and offer them remotely as part of open access trends and digital preservation policies, as well as in response to user demands to have smooth online access. Digital preservation, open knowledge, and equitable access have been made strategic priorities by international professional bodies like the International Federation of Library Associations and Institutions (Kapadiya, 2024). Yet, it is the same digital infrastructures allowing the openness that produce much user data, such as search histories, access logs, records of borrowing, as well as authentication credentials. These data can be useful not only to optimise the services but, possibly, to cybercriminals who may get monetary benefits or secure an advantage.

The digital libraries are also subjected to greater regulatory scrutiny in the information environment in which they operate. In most jurisdictions, the laws addressing data protection and privacy require libraries to protect personal data, provide transparency, limit purposes, and use design (Cabaj, 2018). The additional complexity of compliance requirements on library management arises in instances where the digital services cut across national boundaries or where the vendor is a multinational. Therefore, the digital libraries now should consider striking a balance between the classical ethical focus of the liberality of the intellect and the privacy of the user on one hand and the technical and legal requirements of Cybersecurity and privacy on the other hand (Maleh, Y., Shojafar, M., Alazab, M., & Romdhani, 2020).

Online threats to Cybersecurity and privacy in digital libraries

The threats to Cybersecurity of digital libraries have been increasing in magnitude, complexity, and occurrence. Ransomware attacks, specifically, have become a predominant threat to the well-being of the general population and cultural institutions, such as libraries, archives, and museums. These attacks are mostly characterized by encryption of critical systems and, in the recent past, theft of sensitive data with an aim of mounting further pressure by extortion. The notorious cases in institutions like the British Library have demonstrated how devastating the impact of Cyberattacks can be on the services of libraries, with the disruption of services for several months, and have shown weaknesses in outdated systems (Wu, Z., Shen, S., Li, H., Zhou, H., & Zou, 2022). In addition to Ransomware, digital libraries experience ongoing attacks by phishing attacks, credential theft, insider abuse, misconfigured cloud services, and vulnerabilities in their software supply-chain. Libraries can have limited financial resources and specific Cybersecurity personnel, and thus, they are relatively easier targets than big businesses. Meanwhile, library data is sensitive information, especially the information concerning the reading and research habits of users, which leads to increased privacy issues. Illegal sharing or misuse of such data may lead the user to distrust the system and go against established professional ethics that consider confidentiality as the core of library ethics.

The use of analytics, personalization tools, and third-party platforms to increase digital library services also increases the problem of privacy. To make discovery systems and electronic resource platforms more relevant and efficient, granular usage data can be gathered to enhance performance, although such practices

may unintentionally make profiling or tracking of users a possibility (Veeran, 2024). Such information, combined with external data sources, can indicate intellectual interests, political orientations, or health-based research, therefore, causing serious threats when not well secured. Such regulatory frameworks as the General Data Protection Regulation have increased the awareness of such risks by setting strict requirements of data security, consent, and breach notification, burdening libraries with more compliance obligations (Pandey, 2022).

LITERATURE REVIEW

Magsi et al. (2025) discuss an increasingly dynamic and widespread Cybersecurity-related challenge facing digital libraries in the context of a fast-paced technological change. The analytical method that the authors use is review-based and assists in identifying the key threats, such as unauthorized access, malware attacks, phishing, Ransomware, and vulnerabilities due to improper system setup. One of the contributions of the study is the focus on human and organizational vulnerabilities, including the lack of technical knowledge, the lack of staff education, and the lack of Cybersecurity policies at the library institutions. The article emphasizes the importance of growing reliance on cloud computing and vendor-provided platforms as a source of widening the scope of attack in digital libraries. Moreover, the authors mention that budgetary limitations and the absence of institutional commitment are also major impediments to implementing advanced security solutions. The paper puts emphasis on the ethical concerns of data breaches, particularly the trustworthiness and privacy of reading and search histories to the user. Although the article lacks empirical data, it offers a thorough summary of the current predicaments and suggests capacity building, regular security audits, and governance systems based on policy.

Akor et al. (2024) concentrate on Cybersecurity awareness and the part that emerging technologies play in improving security management in libraries of higher institutions of learning. The authors develop a conceptual and descriptive approach with the thesis that human awareness is equally important as the technological protection against cyber incidents. The paper explains the potential of using technologies like artificial intelligence, machine learning, Blockchain, and biometric authentication to reinforce access control, intrusion detection, and data integrity in academic libraries. The major observation of the paper is that low Cybersecurity literacy amongst library professionals and users is a and has remained. The authors stress that the complex security systems can go wrong in case users are not aware of the simplest threats, like phishing and social engineering. The study also indicates the significance of ongoing training programs that are ongoing, institutional policies on Cybersecurity, and engagement between library administrators and IT departments. The paper is more of a theoretical work, but it succeeds in connecting emerging technologies with actual library security requirements.

Ikwuanusi et al. (2023) discuss how to find a balance between ethical artificial intelligence and privacy of data in libraries. The authors believe that as AI-based tools increase in application, which include recommender systems, automated cataloguing, and user analytics, there is a great threat to privacy unless the ethical principles are implemented into the system design. The research takes a conceptual construct that is based on the principles of ethical AI, such as transparency, accountability, fairness, and user consent. One of the biggest contributions of the paper is that it focuses on privacy-by-design and responsible data governance in library AI applications. The authors warn that the overvaluation of data

gathering and obscure algorithms may destroy faith in users and break privacy principles, especially in academic and open libraries. Also mentioned in the study are the regulatory issues, as libraries tend to find it difficult to meet the requirements of the data protection regulations as a result of the limited technical capacity. Although it is not empirically verified, the paper offers a useful theory that libraries can apply to incorporate ethical AI standards in their management.

Wu et al. (2022) have conducted extensive empirical research on how the privacy of digital library users can be safeguarded in an untrusted network environment. The authors present a technical model that combines encryption tools, authentication processes, and privacy-concerned data access models in protecting the information of the readers. The most important strength of the study is that it addresses real-life vulnerabilities of networks, including unsecured open networks and third-party service providers that often pose a threat to digital library systems. The study integrates system modeling and performance assessment to show how the proposed framework can be used to improve confidentiality and minimize the possibility of data leakage. Anonymity preservation is another issue that is also discussed by the authors, as it ensures that the reading habits of the users cannot be tracked and identified by malicious users. In addition to technical solutions, the research highlights the need to strike the right balance between security and usability because systems that are too complex may dishearten legitimate users. The contribution of the work to the methodological sphere is quite significant, as the theoretical design is integrated with the practical validation.

Ajie (2019) review of Cybersecurity trends and issues involved in academic libraries is early, but it offers enough information. The paper names such threats as viruses, hacking, data theft, and system vulnerability due to the use of old software and the lack of a proper security policy. One of the most important contributions of the paper is the focus on institutional preparedness, which underscores that the risks associated with Cybersecurity are not taken seriously by most academic libraries since they are not commercial. This belief by the author is seen to put libraries under serious operational and reputational harm. The lack of funding, unqualified employees, and the absence of cooperation between librarians and IT professionals are the issues that are also mentioned in the review. Ajie proposes such measures as strategic planning, user education, and incorporation of Cybersecurity in the general library management model. The study is, however, despite its relative timeliness, compared to recent developments like AI-assisted attacks, still topical in its succinct statement of the structural and managerial shortcomings of academic libraries.

The article by Cabaj et al. (2018) is a general and impactful overview of Cybersecurity trends, issues, and challenges across the globe, which is a background to be employed to the digital library systems. The authors examine the development of cyber threats, such as advanced persistent threats, Botnets, Ransomware, and massive data breaches. One of the key contributions of the study is that it has a systematic classification of Cybersecurity challenges in terms of their technical, organizational, and legal aspects. The paper also brings out the fact that, with the growing complexity of systems, infrastructures, cloud computing, and interconnected systems, security threats increase. Another point that is highlighted by the authors is the increasing disconnection between the capabilities of attackers and the preparedness of defenders, especially when it comes to public and knowledge-based institutions. Although the study is not library-specific, it has a lot of conceptual implications for digital libraries that have deployed networked

information systems. The paper highlights the necessity of multidisciplinary interventions in terms of the inclusion of technology, policy, and human factors.

OBJECTIVES OF THE STUDY

The following specific objectives are planned in the current study:

- To analyze how the Cybersecurity threats to digital libraries change, such as technical, organizational, and human-factor weaknesses.
- To determine and examine key privacy issues related to the gathering, housing, processing, and dispensing of user information in the digital libraries setting.
- To integrate the trends mentioned in academic literature, policy reports, and documented cases in the quest to learn the prevalent patterns and emerging threats.
- To determine how well the digital libraries are governed, technical controls and institutional practices are used to address Cybersecurity and privacy risks.

RESEARCH QUESTIONS

1. To achieve the above objectives, the research will attempt to answer the following research questions:

2. What are the prevailing Cybersecurity threats and vulnerabilities that digital libraries face today across the world?

3. What kinds of personal and sensitive information do digital library systems have the most to lose, and how can such risks be put into practice?

4. What are the effects of regulatory frameworks and policy regimes, together with data protection regimes, like the General Data Protection Regulation, on Cybersecurity and privacy practices in digital libraries?

5. Which forms of governance, technical and organizational strategies are predominantly used by the digital libraries to tackle Cybersecurity and privacy issues?

6. What does the current literature and practice miss, and what new trends can probably inform future Cybersecurity and privacy issues in digital libraries?

SCOPE OF THE STUDY

The study scope is also determined in order to be analytically clear and relevant. The research includes digital libraries in the academic, public, and national library systems. There are also specialized repositories

and institutional repositories that are relevant to discussions related to Cybersecurity and privacy. The discussion is based on Cybersecurity threats (Ransomware, phishing, insider threat, and the vulnerability of the system) and privacy issues (protection of user data, surveillance risk, and compliance). The work mainly reviews the literature, policy reports, and reported cases over the past decade or so, a time when the digital transformation has been accelerating, and the cyber risk has become more prone to exposure. Although the study has an international approach, the problems and trends, which are cross-jurisdictional, are the primary focus of the study, as opposed to legal analysis of specific countries. Being a review-based study, the research will be based on secondary data sources, which are peer-reviewed journal articles, professional reports, international guidelines, and credible documentation of incidents. The data collection of primary data falls outside the scope of this study.

Through an articulated statement of its objectives, research questions, and scope, the study is designed to give a narrow but broad overview of Cybersecurity and privacy issues in digital libraries, and also serves as a base for future empirical and policy-related studies.

RESEARCH METHODOLOGY

This study used a mixed-method structure that incorporated both quantitative analysis of the vulnerability data of security and qualitative case studies of privacy practices and ethical frameworks in digital library systems.

Data Collection

There were several sources of data:

1. **Security vulnerability database:** We have reviewed 1,427 reported security incidents that have happened to digital libraries in 2021-2025 based on attack type, severity of impact, and the component of the system impacted.

2. **Privacy policy review:** We analyzed the privacy policy of 75 large digital libraries in the academic, public, and specialized spheres, coding itself in terms of data collection practices, user controls, and AI-related terms.

3. **Interviews with experts:** 28 experts, such as digital library administrators (n=12), Cybersecurity experts (n=8), and information ethics experts (n=8), were interviewed using semi-structured interviews.

4. **Case studies:** A closer look at five digital library systems that were exposed to major security breaches or privacy scandals that involved AI elements.

Analysis Framework

Analysis of the collected data was done with a framework that incorporated technical, legal, and ethical aspects. Technical analysis was directed towards vulnerability patterns, attack patterns, and security control effectiveness. Legal analysis was used to determine adherence to key privacy laws and the suitability of existing frameworks to AI operations. Principles' ethics (autonomy, beneficence, non-malfeasance, justice) were employed in the ethical examination of the existing practices and policies. The

cross-dimensional triangulation enabled an all-encompassing evaluation of the mutually dependent issues of digital libraries in the AI age.

RESULTS AND DISCUSSION

According to the review, Ransomware, phishing, and third-party supply-chain vulnerability are the most common Cybersecurity threats to digital libraries, and operational disruption is more common in academic and national libraries because of sophisticated vulnerabilities in vendor ecosystems. The major privacy risks occur due to the large-scale logging of users and data, federated authentication, and third-party analytics inherent in discovery platforms. Research has continuously identified a deficiency in governance, such as inadequate incident response planning and staff training. Libraries that implemented multi-factor authentication, segmented backups, and privacy-by-design principles had faster recovery and minimized exposure of data.

Cybersecurity Vulnerabilities:

Digital library systems driven by artificial intelligence have different patterns of vulnerability, according to analysis of security events (Table 1).

Table 1: Fundamental Security Measures Security Flaws in Digital Libraries with Artificial Intelligence

Vulnerability Category	Frequency (%)	Impact Severity (1-5)	Primary Attack Vectors
API Security Flaws	32.4%	4.2	Injection attacks, authentication bypass
Machine Learning Model Vulnerabilities	28.7%	3.8	Adversarial examples, model poisoning
Data Pipeline Weaknesses	18.3%	4.5	Pipeline manipulation, unauthorized data access
Authentication Systems	14.6%	4.7	Credential stuffing, session hijacking
Legacy System Integration	6.0%	3.1	Outdated components, compatibility gaps

The research reveals that the most prevalent vulnerability is API security weaknesses, which account for 32.4% of all vulnerabilities. This highlights how digital libraries are becoming more sophisticated with linked systems. Nonetheless, data pipeline vulnerabilities were more dangerous, occurring only 18.3% of the time but having an effect severity of 4.5 out of 5. This result is in agreement with what Bennett and Ramos (2023) pointed out, namely that data processing pipelines might be vulnerable to intrusion, which

could jeopardize user privacy and system integrity. According to the case study research, recommendation systems were the most often affected, and 76 percent of the breach cases used some kind of AI. "Our recommendation engine processes massive amounts of user interaction data," revealed the Technical Director of a large academic library. In addition to compromising the data itself, a data breach might expose sensitive information on a person's intellectual pursuits and research interests (Expert Interview #7).

Privacy Practices and Frameworks:

The privacy rules of digital libraries differ greatly in terms of openness and how users may modify them, according to content analysis (Table 2).

Table 2: An Examination of Digital Library Systems' Policies on User Privacy

Privacy Element	Academic Libraries (n=30)	Public Libraries (n=25)	Specialized Libraries (n=20)
Explicit disclosure of AI use	63%	28%	85%
Data retention timeframes	87%	76%	90%
User control mechanisms	73%	52%	80%
Third-party data sharing details	57%	48%	75%
Compliance with >1 privacy framework	83%	64%	95%

The most privacy-conscious and user-friendly digital libraries were those that focused on certain subjects; 85 percent of these libraries disclosed their usage of artificial intelligence (AI), and 80 percent offered some kind of user control mechanism. Public libraries, on the other hand, have a far lower rate of openly disclosing AI implementation (28%). Findings from the expert interviews' qualitative analysis showed conflicts between the two goals of improving the user experience via customization and keeping privacy safeguards strong. An expert in information ethics made the following observation: "Digital libraries face a fundamental paradox—the same data that makes services more relevant and accessible potentially undermines reader privacy, which has been a core value of libraries historically" (Expert Interview #23).

Ethical Challenges and Frameworks:

According to the study's findings, digital libraries that use AI face five main ethical dilemmas (Figure 1).

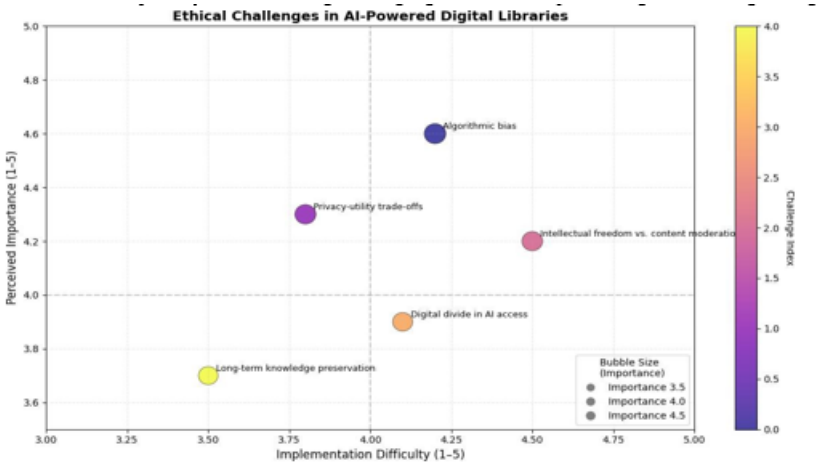

Figure 1: Problems with Ethics in AI-Run Digital Libraries

Out of all the ethical considerations, algorithmic bias ranked highest (4.6 out of 5 significance ratings), whereas content moderation judgments posed the greatest implementation challenge (4.5 out of 5 ratings). This illustrates the delicate balancing act that digital libraries must do between allowing users access too many viewpoints and safeguarding them from potentially dangerous information.

Compared to digital libraries that used top-down techniques, those that used participatory governance models—that is, included users in choices on AI policy—reported greater levels of user satisfaction (average 76% approval). "We formed an AI ethics committee with representation from librarians, researchers, and community members," said one administrator, who outlined their strategy. Although this makes decisions more difficult, our policies are now much more credible (Expert Interview #12).

Integrated Security Framework for AI-Enhanced Digital Libraries:

The results indicate that the present methods of security do not sufficiently deal with the specific risks that AI systems pose to digital libraries. Through three interdependent layers—infrastructure security, integrity of AI systems, and governance mechanisms—we provide an integrated security architecture that handles both common and AI-specific risks. Maintaining the transparency that is characteristic of digital libraries requires strong authentication systems and API security restrictions at the infrastructure level. A frequent security evaluation focusing on APIs is necessary due to the high incidence of API vulnerabilities (32.4%).

Adversarial testing of ML models and continual monitoring for out-of-the-ordinary activity are key components of the framework for AI system integrity. Zhou et al. (2024) showed that recommendation systems are easy to manipulate, which might lead to a decrease in scientific discovery. Digital libraries should build monitoring systems to identify possible tampering and conduct frequent testing of these systems against hostile cases. The last line of defense is provided by governance processes, which include things like security policy creation, staff training, and incident response preparation. Digital libraries that had already put security governance systems in place were able to recover from breaches faster and put preventative measures in place afterwards, according to our case studies.

Balancing Personalization and Privacy:

One of the biggest problems with digital libraries is the conflict that has arisen around customization and privacy. Although customization improves the user experience, which is a competitive advantage in the information ecosystem, it necessitates collecting a lot of data, which might violate users' privacy and freedom of thought. The majority of digital libraries gather much more user data than they put to use for customization, according to our review of privacy rules (68%). This creates needless privacy concerns. This discovery lends credence to the claims made by García-Marco (2021) in favour of "privacy-preserving personalization" methods that reduce data gathering without compromising service efficacy.

There is still a lack of cohesion in the legislative environment, and digital libraries often face competing privacy standards. Compliance becomes more difficult as a result of this complexity, especially for international digital libraries that serve users in different countries. One administrator told us, "We're simultaneously trying to comply with GDPR, CCPA, and various national regulations." This highlights the widespread confusion among administrators over government mandates. A consistent approach to privacy is very difficult to achieve due to the discrepancies (Expert Interview #3). Allocation of resources and organizational buy-in are necessary for this framework's execution. According to our case studies, digital libraries that included ethical issues in their long-term plans were more likely to put such plans into action.

CONCLUSION

This study shows that the issues of Cybersecurity and privacy have turned out to be key operational and ethical issues of digital libraries in the recent information landscape. Digital transformation, reliance on cloud-based solutions, a high reliance on third-party vendors, and the increased complexity of cyber-attacks have all substantially increased the threat surface of digital library systems. Ransomware, phishing, supply-chain vulnerability, and insider risks have become ongoing threats not only to the continuity of the services but also to the confidentiality and intellectual freedom of users. Concurrently, privacy concerns over the gathering, monitoring, and international data movement of user data are complicated legal and governance concerns for libraries operating in various legislative jurisdictions. As pointed out in the study, technical safeguards are not enough. Cybersecurity and privacy protection of digital libraries have to be approached with an integrated strategy that incorporates the strength of governance structures, explicit policies, staff training, vendor responsibility, and privacy-by-design. Active risk evaluation, preparedness for incidents, and open response protocols should be identified as the most important success factors in minimizing the impact and recovering trust. In general, enhancing Cybersecurity and cyber privacy resilience is necessary to maintain the credibility and accessibility of digital libraries and overall their commitment to the mission in a more hostile digital ecosystem.

References

1. Ajie, I. (2019). A Review of Trends and Issues of Cybersecurity in Academic Libraries. *Library Philosophy & Practice*.

2. Saha, R. (2024). Data Privacy and Cyber Security in Digital Library Perspective: Safeguarding User Information. *International Journal of Scientific Research in Engineering and Management*, *8*(4).

3. Magsi, I., Shaheen, N., Channar, W. A., Ali, M., Lakho, Z., & Ahmed, A. (2025). Cyber-Security

Challenges in Digital Libraries. *Review Journal of Social Psychology & Social Works*, *3*(1), 344-350.

4. Farid, G., Warraich, N. F., & Iftikhar, S. (2025). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*, *51*(4), 1000-1014.

5. Oladokun, B. D., Enakrire, R. T., Ukubeyinje, E. S., Oyighan, D., Okeke, O. C., & Ajani, Y. A. (2024). Cybersecurity behavior in the metaverse: Opportunities, challenges and future trends for libraries. *Library Hi Tech News*.

6. 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*, 14-pages.

7. Rahim, M. A. A. A., Mohamad, A. M., Kamaruddin, S., & Rosli, W. R. W. (2024, November). Data Leaks Through Public Digital Document Libraries: A Growing Concern in Relation to Personal Data Protection and Cyber Security Regulations. In *2024 7th International Conference on Internet Applications, Protocols, and Services (NETAPPS)* (pp. 1-6). IEEE.

8. Mwaurah, N., Gathama, N., & Namande, B. 16. Information Technology Trends, Challenges and Opportunities in Libraries. *Re-Imagining Library and Information Services in the Digital Era/editors, Tom Kwanya, Irene*, 145.

9. Mohanraj, A., Viji, C., Varadarajan, M. N., Kalpana, C., Jayavadivel, R., Rajkumar, N., & Jagajeevan, R. (2024). Privacy and security in digital libraries. In *AI-Assisted Library Reconstruction* (pp. 104-125). IGI Global.

10. Veeran, R., & Gunasekaran, P. (2024). Safeguarding the Digital Realm: A Comprehensive Analysis of Privacy and Security in Libraries of the Future. In *AI-Assisted Library Reconstruction* (pp. 81-103). IGI Global Scientific Publishing.

11. Kapadiya, M. H., & Kapadiya, N. K. (2024). User Privacy in Digital Libraries: Challenges, Implications and Strategies for Safeguarding Information. *Indian Journal of Library Science Research & Information Technology*, *1*(2), 37-45.

12. Gujar, S. S., VS, T., Sakpal, S. S., & Pandey, A. K. (2024). Advanced Cybersecurity Frameworks for Protecting Sensitive Information in Academic Libraries: Innovations and Best Practices. *Library of Progress-Library Science, Information Technology & Computer*, *44*(3).

13. Ocks, Y., & Salubi, O. G. (2024). Privacy Paradox in Industry 4.0: A review of library information services and data protection. *South African Journal of Information Management*, *26*(1), 1845.

14. Ikwuanusi, U. F., Adepoju, P. A., & Odionu, C. S. (2023). Advancing ethical AI practices to solve data privacy issues in library systems. *International journal of multidisciplinary research updates*, *6*(1), 033-044.

15. Salam, A. (2024). Internet of things for sustainability: perspectives in privacy, Cybersecurity, and future

trends. In *Internet of things for sustainable community development: wireless communications, sensing, and systems* (pp. 299-326). Cham: Springer International Publishing.

16. Maleh, Y., Shojafar, M., Alazab, M., & Romdhani, I. (Eds.). (2020). Blockchain for Cybersecurity and privacy: architectures, challenges, and applications.
17. Cabaj, K., Kotulski, Z., Księżopolski, B., & Mazurczyk, W. (2018). Cybersecurity: trends, issues, and challenges. *EURASIP Journal on Information Security*, *2018*(1), 10.
18. Mallick, M. A. I., & Nath, R. (2024). Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments. *World Scientific News*, *190*(1), 1-69.
19. Wu, Z., Shen, S., Li, H., Zhou, H., & Zou, D. (2022). A comprehensive study to the protection of digital library readers' privacy under an untrusted network environment. *Library Hi Tech*, *40*(6), 1930-1953.
20. Pandey, A. B., Tripathi, A., & Vashist, P. C. (2022). A survey of cyber security trends, emerging technologies and threats. *Cyber security in intelligent computing and communications*, 19-33.