Cybersecurity Awareness: Leveraging Emerging Technologies in the Security and Management of Libraries in Higher Education Institutions

Solomon Obotu Akor
https://orcid.org/0000-0001-5076-084X
Federal University of Technology Ikot Abasi, Akwa Ibom State, Nigeria
Akorsolomon11@gmail.com

Celina J. Nongo
https://orcid.org/0000-0002-7825-8111
Federal College of Education Idiep-Ibono, Akwa Ibom State, Nigeria
celinafcei23@gmail.com

Columbus O. Udofot
https://orcid.org/0009-0009-7940-537x.
Federal University of Technology Ikot Abasi, Akwa Ibom State, Nigeria
Columbusudofot@yahoo.com

Bolaji David Oladokun
https://orcid.org/0000-0002-7826-9187
Federal University of Technology Ikot Abasi, Akwa Ibom State, Nigeria
Bolaji.oladokun@yahoo.com

Abstract

This study investigates cybersecurity awareness, particularly within the realm of higher education institutions, where emerging technologies enhance library security and management. The paper adopts a qualitative research method through a scoping review of the literature to determine cybersecurity threats in libraries, establish the role of emerging technologies in cybersecurity, identify applications of these technologies in library security and management, and address challenges associated with their implementation. Findings reveal a diverse array of cybersecurity threats faced by libraries, ranging from malware infections to data breaches, highlighting the need for robust security measures. Emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain, Biometric Authentication, and Internet of Things (IoT) security are identified as crucial tools for mitigating these threats and enhancing library security. Applications of these technologies include AI-powered threat detection systems, blockchain-based digital asset management platforms, and biometric authentication systems for access control. However, challenges such as interoperability issues, data privacy concerns, and budget constraints are recognised as barriers to their effective implementation. The study concludes by emphasising the importance of addressing cybersecurity issues in libraries and

UNISA university of south africa PRESS
Southern African Journal of Security
Volume 2 | 2024 | #16671 | 14 pages
https://doi.org/10.25159/3005-4222/16671
ISSN 3005-4222 (Online)

leveraging emerging technologies to strengthen security, resilience, and innovation in library management practices.

Keywords: Cybersecurity; awareness; Higher Education Institutions; emerging technologies; Artificial Intelligence; security management.

Introduction

Libraries face myriad cybersecurity challenges that threaten the confidentiality, integrity, and availability of their digital assets. Both academic and public libraries are increasingly targeted by cyber threats ranging from phishing scams and malware attacks to data breaches and insider threats. The digitisation of library collections, the proliferation of online resources, and the adoption of cloud-based services have expanded the attack surface, making libraries vulnerable to sophisticated cyber-attacks. These threats not only jeopardise the security of library systems and networks but also compromise the privacy and confidentiality of library users' personal information and research data (Ulven and Wangen 2021). Cybersecurity is of paramount importance in higher education libraries due to their pivotal role in supporting teaching, learning, and research activities within academic institutions. Higher education libraries house valuable intellectual assets, including scholarly publications, research data, and proprietary information, making them attractive targets for cybercriminals seeking to steal sensitive data or disrupt academic operations. A cybersecurity breach in a higher education library can have far-reaching consequences, including reputational damage, financial losses, legal liabilities, and intellectual property theft, underscoring the critical need for robust cybersecurity measures to safeguard library resources and preserve academic integrity (Oladokun et al. 2024).

The adoption of emerging technologies in library management offers a promising avenue for bolstering cybersecurity defences. From advanced encryption algorithms to machine learning-powered anomaly detection systems, these technologies equip libraries with robust tools to detect, prevent, and mitigate cyber threats. Moreover, they streamline administrative processes, enhance user experiences, and fortify the overall resilience of library infrastructures. However, the landscape of cybersecurity threats in libraries is ever-evolving, necessitating continuous adaptation and innovation. Emerging technologies in cybersecurity, such as blockchain for secure data transactions and artificial intelligence for predictive threat analysis, hold immense potential but also pose implementation challenges. Integrating these technologies into library security frameworks requires meticulous planning, investment in staff training, and rigorous adherence to best practices in cybersecurity governance (Ulven and Wangen 2021).

The application of emerging technologies in library security and management extends beyond mere defence mechanisms. These technologies offer transformative capabilities, enabling libraries to enhance user access controls, personalise services, and curate digital collections with unprecedented precision. Whether through biometric authentication systems or augmented reality for immersive learning experiences,

emerging technologies empower libraries to reimagine their roles in the digital age. However, challenges abound in the adoption of emerging technologies for library security and management. Concerns regarding data privacy, interoperability, and resource constraints loom large, complicating the integration process and necessitating collaborative efforts between libraries, technology vendors, and cybersecurity experts.

Moreover, the rapid pace of technological advancement demands agile frameworks for risk assessment and adaptation, underscoring the need for strategic foresight and proactive governance (Orr et al. 2024). To mitigate cybersecurity risks and enhance resilience against evolving threats, higher education libraries are increasingly leveraging emerging technologies in their management practices. These technologies encompass a wide range of innovative solutions, including artificial intelligence (AI), machine learning (ML), blockchain technology, biometric authentication, and Internet of Things (IoT) security. By integrating these technologies into their systems and infrastructure, libraries can strengthen their cybersecurity posture, improve threat detection and response capabilities, and enhance the overall security and management of digital assets (Holland 2020). Therefore, cybersecurity is a pressing concern for higher education libraries, given the increasing frequency and sophistication of cyber threats targeting these institutions. Given these, the following research objectives guided the study:

1. To determine the cybersecurity threat in libraries

2. To establish the role of emerging technologies in cybersecurity

3. To determine the applications of emerging technologies in library security and management

4. Determine factors that interfere with the application of emerging technologies for library security and management.

Literature Review

The paper reviewed literature in line with the study's objectives

Cybersecurity Threat in Libraries

Libraries, as custodians of vast amounts of sensitive information and intellectual property, face myriad cybersecurity threats that pose significant risks to their operations and users. Phishing attacks represent one of the most pervasive cybersecurity threats targeting libraries and their users. Phishing involves the use of fraudulent emails, messages, or websites designed to deceive individuals into disclosing sensitive information such as login credentials, financial data, or personal details. Cybercriminals often impersonate trusted entities, such as library staff, academic institutions, or publishers, to lure unsuspecting users into clicking on malicious links or downloading

malicious attachments. Once compromised, hackers can exploit stolen credentials to gain unauthorised access to library systems, compromise user accounts, or launch further attacks (Samtani et al. 2020). Malware, including viruses, worms, and trojans, poses a significant threat to library systems and networks, compromising their integrity and availability. Malware infections can result from users inadvertently downloading infected files, visiting compromised websites, or opening malicious email attachments. Ransomware, a specific type of malware, encrypts files or locks down systems, rendering them inaccessible until a ransom is paid. Ransomware attacks have targeted libraries worldwide, disrupting operations, causing data loss, and imposing financial burdens on institutions. The proliferation of ransomware-as-a-service (RaaS) platforms has made ransomware attacks more accessible to cybercriminals, exacerbating the threat landscape for libraries (Humayun et al. 2020). Data breaches represent a critical cybersecurity concern for libraries, as they can result in the unauthorised access, disclosure, or theft of sensitive information stored within library systems. Personal data, research data, and intellectual property are among the valuable assets at risk of exposure in data breaches. Common vectors for data breaches include unsecured databases, vulnerable web applications, and compromised user accounts. Libraries must comply with data protection regulations and industry standards to safeguard user privacy and prevent data breaches. Failure to secure sensitive information can lead to reputational damage, legal liabilities, and financial repercussions for libraries and their users (Thakur 2024).

Insider threats, whether intentional or unintentional, pose a significant risk to library security and integrity. These threats may arise from disgruntled employees, negligent users, or compromised accounts with elevated privileges. Insider threats can manifest in various forms, including data theft, sabotage, or unauthorised access to confidential information. Libraries must implement robust access controls, user monitoring, and privilege management mechanisms to mitigate insider threats and prevent unauthorised activities. Educating library staff and users about cybersecurity best practices and promoting a culture of security awareness can help mitigate the risk of insider threats and foster a culture of trust and accountability (Alexei and Alexei 2021).

Cybersecurity breaches can have far-reaching consequences for library operations and users. Disruption of library services, loss of critical data, and compromised user privacy are among the immediate impacts of such breaches. Libraries may experience downtime, service interruptions, or loss of access to digital resources, affecting user productivity and research activities. Moreover, the loss of user trust and confidence in library services can have long-term repercussions, undermining the institution's reputation and credibility. Library users may suffer financial losses, identity theft, or reputational harm due to compromised personal information, highlighting the need for proactive cybersecurity measures to protect user data and preserve trust (Alferidah and Jhanjhi 2020).

Cybersecurity threats pose significant risks to libraries and their users, necessitating proactive measures to mitigate vulnerabilities and safeguard digital assets. By addressing common threats such as phishing attacks, malware and ransomware, data breaches, and insider threats, libraries can enhance their cybersecurity posture and protect the confidentiality, integrity, and availability of information resources. Moreover, libraries must educate staff and users about cybersecurity best practices, promote a culture of security awareness, and invest in robust security controls and technologies to effectively combat cyber threats and preserve the trust and confidence of their stakeholders.

Role of Emerging Technologies in Cybersecurity

In the ever-evolving landscape of cybersecurity, emerging technologies play a pivotal role in empowering organisations to defend against increasingly sophisticated cyber threats. Libraries, as custodians of valuable information and intellectual property, can leverage these technologies to bolster their security posture and protect digital assets from malicious actors.

Artificial Intelligence (AI) and Machine Learning (ML)

AI and ML technologies have revolutionised cybersecurity by enabling automated threat detection, predictive analysis, and adaptive response mechanisms. AI-driven algorithms can analyse vast amounts of data in real-time to identify anomalous patterns, detect emerging threats, and proactively mitigate security incidents. For instance, AI can analyse network traffic patterns and user behaviour to identify sophisticated cyber threats such as zero-day attacks or insider threats. By learning from historical data, AI-powered content analysis tools can automatically categorise, tag, and enrich metadata for digital resources in library collections. This facilitates efficient search and retrieval processes for users while enabling librarians to curate and organise content more effectively.

Moreover, AI-driven simulations and interactive modules can be used to educate library staff and patrons about cybersecurity best practices, raising awareness about common threats such as phishing scams and social engineering attacks. ML algorithms can analyse user preferences, borrowing histories, and search patterns to generate personalised recommendations for relevant resources, thereby enhancing user engagement and satisfaction. These algorithms can also detect deviations from normal patterns and alert security personnel to potential breaches in real-time. By learning from historical data and user behaviour, ML models continuously improve the accuracy and effectiveness of threat detection. AI-powered security solutions can augment human capabilities, streamline security operations, and improve overall resilience against cyber-attacks (Zewdie and Girma 2020). Through these advanced technologies, libraries can not only safeguard their digital assets but also enhance user experiences and operational efficiency.

Blockchain Technology

Blockchain technology offers a decentralised and tamper-resistant platform for secure data storage, transaction processing, and identity management. Utilising cryptographic techniques and distributed consensus mechanisms, blockchain ensures data integrity, immutability, and transparency. In the context of cybersecurity, blockchain can create secure digital ledgers for recording access logs, audit trails, and authentication records. By leveraging blockchain-based solutions, libraries can enhance data privacy, establish trust among stakeholders, and prevent unauthorised modifications to critical information assets. Blockchain-based smart contracts can automate the management of copyright licenses and permissions for digital content, ensuring that authors and publishers receive fair compensation for their works while enabling seamless access for authorised users. Blockchain's immutable ledger provides a tamper-proof record of transactions, allowing libraries to verify the authenticity and provenance of rare or valuable artefacts in their collections. This is particularly relevant for special collections and archival materials with historical significance.

Additionally, blockchain-based access control mechanisms can decentralise authentication processes, reducing reliance on centralised authentication servers and mitigating the risk of single points of failure or unauthorised access. Blockchain can also be used to create cryptographic hashes of digital artefacts and timestamp them on the blockchain, providing verifiable proof of their existence and integrity over time. This enhances the trustworthiness of digital archives and ensures their long-term preservation (Mahmood et al. 2022). Through these applications, blockchain technology can significantly strengthen the security and integrity of library systems and their valuable information resources.

Biometric Authentication

Biometric authentication technologies enable user identity verification based on unique physiological or behavioural characteristics, such as fingerprints, facial features, or iris patterns. This method offers a higher level of security compared to traditional password-based authentication, as biometric identifiers are inherently more difficult to spoof or replicate. Libraries can implement biometric authentication systems to secure access to sensitive resources, restrict unauthorised entry, and protect user privacy. Biometric authentication enhances user convenience and reduces the risk of credential theft or misuse. It can complement traditional authentication methods such as passwords or PINs, providing an additional layer of security for accessing sensitive library systems or resources.

Additionally, biometric authentication systems can enhance accessibility for users with disabilities by offering alternative biometric modalities, such as voice recognition or iris scanning, accommodating a diverse range of physical abilities and preferences. Given the sensitivity of biometric data, robust privacy protections are essential. Libraries must implement secure storage and encryption mechanisms to safeguard biometric templates

and comply with regulations such as the General Data Protection Regulation (GDPR). Biometric authentication solutions can seamlessly integrate with existing library management systems, enabling smooth authentication workflows for users while enhancing security and accountability (Alghamdi and Ragab 2022). Through these measures, libraries can significantly bolster their security infrastructure and improve user experience.

Internet of Things (IoTs)

The proliferation of IoT devices in library environments, such as smart sensors, RFID tags, and connected appliances, introduces new security challenges related to device vulnerabilities, data privacy, and network security (Thakur 2024). IoT security measures encompass device authentication, data encryption, network segmentation, and threat monitoring to mitigate the risk of unauthorised access and data breaches. Libraries can deploy IoT security solutions to safeguard IoT endpoints, detect anomalous activities, and enforce security policies across interconnected devices. By adopting IoT security best practices, libraries can minimise the risk of IoT-related cyber threats and maintain the integrity of their digital infrastructure. Additionally, IoT sensors and actuators can optimise energy usage, lighting, and environmental controls within library facilities, reducing operational costs and enhancing user comfort without compromising security or privacy. IoT devices can remotely monitor the health and status of critical infrastructure components such as servers, network switches, and HVAC systems, enabling proactive maintenance and minimising downtime due to unexpected failures or malfunctions. Security protocols such as TLS (Transport Layer Security) and DTLS (Datagram Transport Layer Security) ensure secure communication between IoT devices and backend systems, protecting sensitive data from interception or tampering during transit.

Moreover, IoT security platforms can aggregate and analyse telemetry data from diverse IoT devices to identify potential security threats or anomalies in real time. This enables prompt incident response and remediation actions to mitigate risks and minimise impact (Zewdie and Girma 2020). Through these comprehensive security measures, libraries can effectively manage and secure their IoT environments, ensuring a safe and efficient operational framework.

Applications of Emerging Technologies in Library Security and Management

Libraries can leverage AI-powered threat detection platforms to monitor network traffic, analyse security logs, and identify suspicious activities indicative of cyber-attacks. AI algorithms can detect malware infections, phishing attempts, and insider threats in real-time, enabling proactive incident response and remediation actions. AI-driven threat intelligence platforms can provide libraries with actionable insights into emerging threats, vulnerabilities, and attack trends, allowing them to strengthen their defence mechanisms and prevent security breaches. By employing these advanced technologies, libraries can enhance their cybersecurity posture, ensuring the safety and integrity of

their digital assets and maintaining the trust of their users. AI-powered tools not only help detect threats but also understand the evolving landscape of cyber threats, enabling libraries to stay ahead of potential attacks and continuously improve their security strategies.

Blockchain technology can be used to create immutable records of library transactions, access permissions, and digital assets, ensuring data integrity and transparency. Libraries can implement blockchain-based solutions for secure data storage, archival preservation, and intellectual property management. Blockchain-based access control mechanisms enable libraries to enforce granular permissions, authenticate users securely, and track data access and usage in a decentralised manner. By leveraging blockchain, libraries can enhance data security, streamline audit processes, and build trust with stakeholders (Tella et al. 2022). Biometric authentication systems can enhance library security by verifying the identity of users based on unique physiological or behavioural traits. Libraries can deploy biometric authentication solutions for access control, user authentication, and identity verification purposes. Biometric identifiers, such as fingerprints, facial scans, or iris patterns, provide a high level of security and accuracy, reducing the risk of unauthorised access or identity theft. Biometric authentication enhances user experience and strengthens security measures, ensuring that only authorised individuals have access to library resources and services (Okubanjo et al. 2021).

As libraries embrace IoT technologies to enhance service delivery and user experiences, it is crucial to implement robust IoT security measures to safeguard interconnected devices and data streams. Libraries can employ IoT security solutions to secure IoT endpoints, monitor device behaviour, and detect potential security vulnerabilities or anomalies. IoT platforms can provide libraries with visibility into their IoT ecosystems, automate security policy enforcement, and respond to emerging threats in real-time. By prioritising IoT, libraries can minimise the risk of IoT-related cyberattacks, protect user privacy, and maintain the integrity of their digital infrastructure (Yugha and Chithra 2020).

Emerging technologies offer libraries powerful tools to strengthen their cybersecurity defences, protect digital assets, and safeguard user privacy. By leveraging AI and ML for threat detection, blockchain for secure data storage, biometric authentication for user identity verification, and IoT security measures for network protection, libraries can enhance their security posture and mitigate the risk of cyber-attacks. As libraries continue to evolve in the digital age, investing in innovative cybersecurity solutions is essential to ensure the confidentiality, integrity, and availability of information resources and services.

Factors that Interfere with Application of Emerging Technologies for Library Security and Management

In the digital age, libraries are tasked not only with preserving and disseminating knowledge but also with safeguarding their collections and ensuring secure access to information. Emerging technologies offer promising solutions to enhance library security and management, but their implementation presents a myriad of challenges. One of the foremost challenges in adopting emerging technologies for library security and management is the rapid pace of technological evolution. Innovations emerge at an exponential rate, making it challenging for libraries to keep pace with the latest developments and select the most suitable solutions for their needs (Zewdie and Girma 2020). Moreover, the dynamic nature of emerging technologies requires libraries to continually update their infrastructure, invest in staff training, and adapt to changing security threats and management practices. Another significant challenge is the complexity of integrating diverse technologies into existing library systems and workflows. Libraries often operate legacy systems that may lack compatibility with newer technologies, leading to interoperability issues and integration challenges. Moreover, implementing emerging technologies requires careful planning, resource allocation, and stakeholder buy-in, which can be hindered by budget constraints, organisational inertia, and resistance to change (Haque et al. 2022).

Data privacy and security concerns pose additional challenges in the application of emerging technologies for library security and management. Libraries are entrusted with sensitive patron information and intellectual property, necessitating robust measures to protect against unauthorised access, data breaches, and privacy violations (Oladokun et al. 2024). However, the adoption of emerging technologies introduces new vulnerabilities and attack vectors, raising concerns about data sovereignty, compliance with regulations such as GDPR, and liability in the event of security incidents. Furthermore, the complexity and sophistication of emerging cybersecurity threats pose formidable challenges for libraries. Cyber attackers are constantly devising new tactics, techniques, and procedures to exploit vulnerabilities in library systems and networks. Libraries must deploy advanced cybersecurity solutions, such as intrusion detection systems, threat intelligence platforms, and security analytics tools, to detect and mitigate these evolving threats effectively. However, such solutions require significant expertise, investment, and ongoing maintenance, which may exceed the capabilities of resource-constrained libraries (Javed et al. 2022). Ethical and societal considerations also complicate the application of emerging technologies for library security and management. Biometric authentication systems, for example, raise concerns about consent, surveillance, and the potential for discriminatory practices. Similarly, AI-driven algorithms for content analysis and recommendation may perpetuate biases or infringe on intellectual freedom if not carefully designed and implemented. Libraries must navigate these ethical dilemmas and ensure that emerging technologies are deployed in a manner that upholds their core values of access, equity, and privacy.

Despite these challenges, there are strategies that libraries can employ to overcome barriers to the application of emerging technologies for security and management. Collaboration and knowledge-sharing within the library community can facilitate the exchange of best practices, lessons learned, and practical solutions for implementing emerging technologies. Partnerships with technology vendors, research institutions, and cybersecurity experts can provide libraries with access to specialised expertise, funding opportunities, and collaborative resources to address their unique challenges. Moreover, investing in staff development and training is essential to build internal capacity and expertise in emerging technologies and cybersecurity. Libraries can offer professional development opportunities, workshops, and certifications to empower staff with the knowledge and skills needed to leverage new technologies effectively and mitigate security risks. Cultivating a culture of innovation, experimentation, and continuous improvement is crucial to fostering a dynamic and adaptive environment conducive to the successful application of emerging technologies for library security and management. While the application of emerging technologies holds great promise for enhancing library security and management, it is not without its challenges. Libraries must navigate the complexities of technological innovation, interoperability, data privacy, cybersecurity threats, ethical considerations, and resource constraints to realise the full potential of these technologies. By embracing collaboration, investing in staff development, and prioritising ethical principles, libraries can overcome these challenges and harness the transformative power of emerging technologies to safeguard knowledge and empower communities in the digital age (Tella et al. 2022).

Methodology

The study employed a qualitative research design. This study aims to conduct a scoping review of the literature to explore cybersecurity issues in libraries within the timeframe of 2019 to 2024. The review seeks to identify key themes, trends, and gaps in the existing literature on library security and management within higher education institutions. The researchers conducted a comprehensive search of academic databases, including ResearchGate, Google Scholar, Scopus, and Web of Science. Keywords and search terms relevant to cybersecurity issues in libraries were employed, such as "library security," "cyber threats," "information security," "emerging technologies," and "higher education libraries." Filters were applied to include only articles published between 2019 and 2024, ensuring the relevance and currency of the literature reviewed. Duplicate articles were removed to maintain the integrity of the review process. Articles were included if they focused on cybersecurity issues in libraries, particularly within the context of higher education institutions. Only peer-reviewed journal articles, conference proceedings, and scholarly publications were considered for inclusion. Articles published in languages other than English were excluded due to language limitations. Articles published before 2019 were excluded to ensure the currency and relevance of the literature reviewed. Relevant articles were screened based on their titles and abstracts to determine their eligibility for inclusion in the review. Full-text articles meeting the inclusion criteria were retrieved and critically evaluated to extract key

findings, methodologies, and theoretical frameworks. Data extraction was conducted using a standardised form to record key information such as author(s), publication year, research objectives, methodology, main findings, and implications. Thematic analysis was employed to identify recurring themes, concepts, and patterns across the included articles, allowing for the synthesis of findings and the identification of gaps and areas for further research. The researchers adhered to ethical guidelines and principles throughout the review process, ensuring the ethical conduct of research and the protection of participants' rights and confidentiality. All data sources were adequately cited and credited to the original authors to uphold academic integrity and intellectual property rights.

Discussion

The study revealed that libraries face a wide range of cybersecurity threats, including malware infections, phishing attacks, data breaches, and ransomware incidents. These threats pose significant risks to the confidentiality, integrity, and availability of library resources and patron information, compromising the trust and reputation of libraries. These findings validate the study of Oladokun et al. (2024) and Zewdie and Girma (2020). Factors contributing to cybersecurity threats in libraries include the increasing digitisation of library collections, reliance on networked systems, and the proliferation of personal devices accessing library resources. Emerging technologies play a crucial role in enhancing cybersecurity defences and mitigating threats in library environments. Artificial Intelligence (AI) and Machine Learning (ML) algorithms are utilised for anomaly detection, predictive analytics, and content analysis to identify and respond to cybersecurity threats more effectively. The study of Jimmy (2024) agrees with this study. Blockchain technology offers decentralised and tamper-proof mechanisms for securing transactions, verifying digital assets, and ensuring data integrity in library systems. Biometric authentication solutions provide secure and user-friendly access controls, reducing reliance on vulnerable password-based authentication methods. Internet of Things (IoT) security protocols protect interconnected devices and infrastructure from unauthorised access, manipulation, and exploitation.

Emerging technologies are applied in various aspects of library security and management to strengthen defences, improve operational efficiency, and enhance user experiences. AI and ML algorithms are used for threat detection, resource allocation, and personalised services, enhancing the effectiveness of security measures and user engagement. Blockchain technology facilitates secure digital asset management, copyright enforcement, and archival preservation, ensuring the authenticity and integrity of library collections. This study validates the findings of Tella et al. (2022). Biometric authentication systems enable seamless access controls, identity verification, and transaction security, enhancing user convenience and privacy. IoT devices monitor environmental conditions, track inventory, and automate maintenance tasks, optimising library operations while maintaining security standards.

Despite their potential benefits, the adoption of emerging technologies in library security and management poses several challenges. Interoperability issues and integration complexities hinder the seamless integration of diverse technologies into existing library systems and workflows. Data privacy and security concerns raise ethical and legal considerations regarding the collection, storage, and use of sensitive patron information. Budget constraints, resource limitations, and organisational inertia may impede the adoption and implementation of emerging technologies in libraries. This corroborates the findings of Igbinovia and Ishola (2023). Cybersecurity risks, including evolving threats, skill shortages, and compliance requirements, demand continuous investment in training, expertise, and risk management strategies. Overall, the study highlights the critical importance of addressing cybersecurity issues in libraries and leveraging emerging technologies to enhance security, resilience, and innovation in library management practices. By understanding the nature of cybersecurity threats, harnessing the capabilities of emerging technologies, and addressing associated challenges, libraries can strengthen their defences and better serve their communities in the digital age.

Conclusion

The paper explored the critical intersection of cybersecurity issues and emerging technologies in libraries, particularly within the context of higher education institutions. Given these, the study has generated valuable insights into the current state of library security and management, as well as the role of emerging technologies in mitigating cybersecurity threats. Libraries face a multitude of cybersecurity threats, including malware infections, phishing attacks, data breaches, and ransomware incidents. These threats pose significant risks to the confidentiality, integrity, and availability of library resources and patron information. Emerging technologies such as Artificial Intelligence (AI), Machine Learning (ML), Blockchain, Biometric authentication, and Internet of Things (IoTs) security play pivotal roles in enhancing cybersecurity defences and mitigating threats in library environments. These technologies offer innovative solutions for threat detection, access control, data integrity, and operational efficiency.

Emerging technologies are applied across various facets of library security and management to strengthen defences, improve operational efficiency, and enhance user experiences. From AI-powered threat detection systems to blockchain-based digital asset management platforms, these technologies offer transformative capabilities for safeguarding library collections and services. Despite their potential benefits, the adoption of emerging technologies in library security and management poses several challenges. These include interoperability issues, data privacy concerns, budget constraints, and cybersecurity risks. Addressing these challenges requires concerted efforts from library administrators, IT professionals, cybersecurity experts, and stakeholders.

References

Alexei, L. A., and A. Alexei. 2021. “Cyber Security Threat Analysis in Higher Education Institutions as a Result of Distance Learning.” *International Journal of Scientific and Technology Research* (3): 128–133.

Alferidah, D. K., and N. Z. Jhanjhi. 2020. “Cybersecurity Impact over Bigdata and IoT Growth.” *2020 International Conference on Computational Intelligence (ICCI)*, October: 103–108. https://doi.org/10.1109/ICCI51257.2020.9247722

Alghamdi, A. S. A. M., and M. Ragab. 2022. “Artificial Intelligence Techniques Based Learner Authentication in Cybersecurity Higher Education Institutions.” *Computers, Materials and Continua* 72 (2): 3131–3144. https://doi.org/10.32604/cmc.2022.026457

Haque, A. B., B. Bhushan, and G. Dhiman. 2022. “Conceptualizing Smart City Applications: Requirements, Architecture, Security Issues, and Emerging Trends.” *Expert Systems* 39 (5): e12753. https://doi.org/10.1111/exsy.12753

Holland, B. 2020. “Emerging Technology and Today's Libraries.” *Emerging Trends and Impacts of the Internet of Things in Libraries*, 1–33. https://doi.org/10.4018/978-1-7998-4742-7.ch001

Humayun, M., M. Niazi, N. Z. Jhanjhi, M. Alshayeb, and S. Mahmood. 2020. “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study.” *Arabian Journal for Science and Engineering* 45: 3171–3189. https://doi.org/10.1007/s13369-019-04319-2

Igbinovia, M. O., and B. C. Ishola. 2023. “Cyber Security in University Libraries and Implication for Library and Information Science Education in Nigeria.” *Digital Library Perspectives* 39 (3): 248–266. https://doi.org/10.1108/DLP-11-2022-0089

Javed, A. R., F. Shahzad, S. ur Rehman, Y. B. Zikria, I. Razzak, Z. Jalil, and G. Xu. 2022. “Future Smart Cities: Requirements, Emerging Technologies, Applications, Challenges, and Future Aspects.” *Cities* 129: 103794. https://doi.org/10.1016/j.cities.2022.103794

Jimmy, F. 2024. “Emerging Threats: The Latest Cybersecurity Risks and the Role of Artificial Intelligence in Enhancing Cybersecurity Defenses.” *Valley International Journal Digital Library*, 564–574. https://doi.org/10.18535/ijsrm/v9i2.ec01

Mahmood, S., M. Chadhar, and S. Firmin. 2022. “Cybersecurity Challenges in Blockchain Technology: A Scoping Review.” *Human Behavior and Emerging Technologies* 2022: 1–11. https://doi.org/10.1155/2022/7384000

Okubanjo, A., A. Okandeji, O. Osifeko, A. Onasote, and M. Olayemi. 2021. “Development of a Hybrid Radio Frequency Identification (RFID) and Biometric Based Library Management System.” *Gazi University Journal of Science*, 1. https://doi.org/10.35378/gujs.834087

Oladokun, B., E. Oloniruha, D. Mazah, and O. Okechukwu. 2024. “Cybersecurity Risks: A Sine Qua Non for University Libraries in Africa.” *Southern African Journal of Security* (2024): 1–14.

Orr, S. G., C. J. Bonyadi, E. Golaszewski, A. T. Sherman, P. A. Peterson, R. Forno, S. Johns, and J. Rodriguez. 2024. “Shadow IT in Higher Education: Survey and Case Study for Cybersecurity.” *Cryptologia* 48 (1): 26–90. https://doi.org/10.1080/01611194.2022.2103754

Samtani, S., M. Abate, V. Benjamin, and W. Li. 2020. “Cybersecurity as an Industry: A Cyber Threat Intelligence Perspective.” *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 135–154. https://doi.org/10.1007/978-3-319-78440-3_8

Tella, A., H. O. Amuda, and Y. A. Ajani. 2022. “Relevance of Blockchain Technology and the Management of Libraries and Archives in the 4IR.” *Digital Library Perspectives* 38 (4): 460–475. https://doi.org/10.1108/DLP-08-2021-0065

Thakur, M. 2024. “Cyber Security Threats and Countermeasures in Digital Age.” *Journal of Applied Science and Education (JASE)*, 1–20.

Ulven, J. B., and G. Wangen. 2021. “A Systematic Review of Cybersecurity Risks in Higher Education.” *Future Internet* 13 (2): 39. https://doi.org/10.3390/fi13020039

Yugha, R., and S. Chithra. 2020. “A Survey on Technologies and Security Protocols: Reference for Future Generation IoT.” *Journal of Network and Computer Applications* 169: 102763. https://doi.org/10.1016/j.jnca.2020.102763

Zewdie, T. G., and A. Girma. 2020. “IoT Security and the Role of AI/Ml to Combat Emerging Cyber Threats in Cloud Computing Environment.” *Issues in Information Systems* 21 (4).