



Enhancing Information Security in Digital Libraries through Real-Time Adaptive Ensemble Learning and Continual Analysis of User Access Streams: A Conceptual Analysis

Bello Ahmad Muhammad¹, Abba Ahmad Muazu^{2,*}

¹ College of International Communication Cooperative, Sichuan University Culture and Arts, Mianyang City, Sichuan Province, China

² University Library, Bayero University, Kano, Nigeria

* Corresponding author: aamuazu.lib@buk.edu.ng

ARTICLE HISTORY

Received: 31 July 2026

Accepted: 19 September 2026

Published: October 2026

ARTICLE INFO



Vol. 1, No. 2 (2026), pp. 362–372

ISSN: 3141-6268 (Print)

3156-5077 (Online)

DOI: 10.67523/aujmss.v1i2.008

License: CC BY 4.0

HOW TO CITE

Muhammad, B. A., & Muazu, A. A. (2026). Enhancing information security in digital libraries through real-time adaptive ensemble learning and continual analysis of user access streams: A conceptual analysis. *Azman Univ. Int. J. Manag. Soc. Sci.*, 1(2), 362–372. <https://doi.org/10.67523/aujmss.v1i2.008>

ABSTRACT

The rapid expansion of digital libraries has transformed access to scholarly information, enabling users to retrieve digital resources remotely and continuously. However, increasing dependence on networked and cloud-based systems has also exposed digital libraries to evolving cybersecurity threats, including unauthorized access, malware, data breaches, credential compromise, and insider attacks. Traditional security mechanisms that rely primarily on predefined rules and signatures may be insufficient for detecting emerging and constantly changing threats. This conceptual paper examines how Real-Time Adaptive Ensemble Learning and continual analysis of user access streams can strengthen information security in digital library environments. Drawing on existing literature on digital library security, machine learning, intrusion detection, and cybersecurity, the paper proposes a six-component conceptual framework comprising User Behaviour and System Activity, Data Pre-processing and Feature Extraction, Adaptive Ensemble Learning Engine, Threat Detection and Classification, Response and Mitigation Layer, and Continuous Feedback. The framework enables continuous monitoring of user and system activities, transformation of access data into behavioural features, adaptive classification of activities through multiple machine learning models, identification of anomalous and evolving cyber threats, appropriate response and mitigation, and continuous feedback for updating detection capabilities. The feedback mechanism connects threat detection and response with continual model adaptation, allowing the proposed system to evolve in response to changing user behaviours, attack patterns, and security conditions. The paper contributes a conceptual foundation for integrating adaptive artificial intelligence into digital library security and provides a basis for future empirical research and implementation.

Keywords: Digital Libraries; Information Security; Cyber-security; Ensemble Learning; Continual Learning; User Access Streams; Machine Learning; Intrusion Detection

1. Introduction

Digital libraries have become essential components of the present-day information ecosystem, providing efficient systems for accessing, professionally enterprising, storing, renewing, retrieving, and disseminating digital information resources. Unlike traditional libraries, virtual libraries give users access to scholarly materials, institutional repositories, electronic books, electronic journals; allow access to multimedia resources, and study information remotely without geographic or time constraints. As higher education institutions, learning organizations, and public libraries maintain to embody digital change, virtual libraries continue to evolve into critical infrastructures that aid teaching, identification, research, and expertise sharing. There is strong enough scholarly communication to provide seamless access to information, and the opportunities for collaboration between researchers all over the world are manifold. Information and Communication Technologies (ICTs), cloud computing, cellular technology, and web-based services have expanded international adoption of digital libraries, and many academic institutions now use cloud-based, fully virtual library systems to manipulate and distribute information sources to numerous consumer communities. These technologies, which rely heavily on institutional repositories and on-line databases, have advanced the accessibility, efficiency and scalability of library offerings and allowed libraries to facilitate remote learning, virtual research and virtual scholarship.

As digital libraries become increasingly central to information access and knowledge dissemination, ensuring information security has become a critical concern. Imamverdiyev (2017) argues that digital libraries are complex information systems that require comprehensive security mechanisms to protect personal data, digital resources, and intellectual property. The author further proposes the IDEA4SP model as a framework for analysing information security challenges in digital library environments.

Despite their huge benefits, virtual libraries face a huge variety of cyber-security threats due to their increasing reliance on digital technologies. As digital collections expand and more services grow to be online, the attack surface for cybercriminals has increased exponentially. Unauthorized access, malware infections, ransomware attacks, phishing campaigns, denial of service attacks, identity robbery, insider threats, and data breaches have become the main security concerns affecting virtual library infrastructure. These cyber threats not only threaten the privacy of digital information sources, undermining integrity and availability, but also undermine acceptance and self-assurance as trust with users in digital library services. Ngwum et al. (2020) examine that cyber-security threats continue to pose a serious risk to protect virtual library collections, institutional repositories, and public information. Traditional cyber-security mechanisms, including firewalls, antivirus software, password authentication, and intrusion detection systems, remain largely on the defensive. Virtual libraries play an important role in infrastructure, but the increasing sophistication and dynamics of cyber-attacks have highlighted significant limitations in those traditional protection processes. Modern cyber-threats are often characterized by their ability to evade signature-based, fully-identity structures, exploit 0-day vulnerabilities, and constantly adapt their attack strategy.

In response to these increasingly demanding situations, artificial intelligence (AI) and machine learning (ML) have gained full attention as a transformative technology for strengthening cyber-security in virtual libraries. Machine learning technologies are capable of analyzing vast amounts of network traffic and individual behavior data, identifying unusual activity, detecting previously unknown attack styles, and predicting capacity security incidents with minimal human intervention (Zhu et al., 2025). Unlike traditional rule-based systems, machine learning algorithms can analyze large volumes of data, recognize hidden patterns, and identify abnormal behaviors. Beena and Kabir (2019) argue that machine learning techniques have expanded the capabilities of digital libraries by improving information retrieval, automation, and security management. In cyber-security contexts, machine learning models are widely used for anomaly detection, malware identification, intrusion detection, and threat intelligence.

Furthermore, the integration of machine learning into digital library security supports proactive rather than reactive cyber-security management. Intelligent security systems can monitor user activities in real time, detect anomalous behaviour, generate automated alerts, and initiate immediate responses before cyber-attacks cause significant damage. These capabilities are particularly important for digital libraries that manage large volumes of sensitive

institutional data, scholarly publications, research datasets, and users' personal information. By improving the speed and accuracy of threat detection, machine learning enhances the resilience of digital library systems while ensuring uninterrupted access to information resources. Given the rapidly evolving cyber threat landscape, there is a growing need for intelligent and adaptive cyber-security frameworks capable of constantly learning from consumer interactions, identifying emerging attack patterns, and effectively responding to sophisticated cyber threats. Digital library services have the ability to protect digital assets, protect users' privacy, and help in long-term sustainability. Consequently, this paper examines cybersecurity enhancement in virtual libraries, with particular emphasis on detecting current cyber threats, assessing existing security challenges, and identifying appropriate strategies and practical applications for strengthening the security of virtual library systems. It also considers the current status of threat identification and the measures required to ensure the security, reliability, and sustainability of digital library services. This paper examines how Real-Time Adaptive Ensemble Learning combined with Continual Analysis of User Access Streams can enhance information security in digital libraries.

2. Literature Review

2.1 Privacy and Surveillance in Digital Libraries

Privacy has long been regarded as a fundamental professional value within librarianship. Libraries have an ethical responsibility to protect users' intellectual freedom and maintain the confidentiality of their information-seeking behaviour, collecting only the personal information necessary for service delivery and safeguarding users' records against unauthorized disclosure. In this context, Jones and Salo (2018) argue that the increasing use of learning analytics and behavioural monitoring in academic libraries introduces significant ethical concerns relating to user consent, transparency, surveillance, and data governance. The proposed framework relies on continuous behavioural monitoring to detect anomalous activities and identify potential cyber threats. Although such monitoring enhances cyber-security, it may also create privacy concerns if users are unaware of how their behavioural data are collected, analysed, and stored. Excessive monitoring could undermine users' trust and discourage free access to information. Therefore, any intelligent cyber-security framework should incorporate privacy-preserving mechanisms, transparent data governance policies, and compliance with relevant data protection regulations to balance effective threat detection with users' privacy rights.

2.2 Evaluation of Ensemble Learning

Ensemble learning has consistently demonstrated superior predictive performance compared with individual machine learning classifiers because it combines the strengths of multiple models while reducing prediction errors (Dietterich, 2000; Zhou, 2012). Techniques such as Random Forest, boosting algorithms, and stacking have achieved high detection accuracy across numerous cybersecurity applications (Breiman, 2001). Despite these advantages, ensemble learning is not without limitations. Compared with single classifiers, ensemble models typically require greater computational power, larger memory capacity, and longer training times because multiple learning algorithms must be trained simultaneously. Furthermore, many ensemble models function as "black-box" systems whose predictions are difficult to interpret, thereby reducing transparency and limiting administrators' understanding of how security decisions are reached. These limitations may significantly affect implementation within smaller academic libraries, particularly in developing countries where ICT infrastructure, technical expertise, and financial resources remain constrained. Consequently, while ensemble learning offers substantial improvements in threat detection accuracy, its practical deployment should be carefully balanced against institutional capacity, computational costs, and explainability requirements.

2.3 Cyber-security Frameworks for Digital Libraries

The increasing digitization of academic libraries has introduced significant cybersecurity concerns regarding the protection of digital collections. Aregbesola and Nwaolise (2023) argue that while digital technologies have expanded access to scholarly information, they have simultaneously increased exposure to cyber threats. The authors emphasize that implementing comprehensive cybersecurity practices is essential for safeguarding digital collections, maintaining user confidence, promoting institutional collaboration, and supporting secure research environments. Their findings highlight the importance of integrating both organizational security measures and advanced technological solutions into digital library infrastructures. The increasing volume of digital resources, cloud-based infrastructures, and remote access services has expanded the attack surface available to cybercriminals. Security threats such as unauthorized access, malware infections, ransomware attacks, phishing attempts, and data breaches threaten the confidentiality and integrity of digital library collections and user information (Ngwum et al., 2020).

Several internationally recognized cyber-security frameworks provide guidance for protecting information systems, including digital libraries. The National Institute of Standards and Technology (NIST) Cyber-security Framework (CSF 2.0) provides a risk-based approach organized around six core functions: Govern, Identify, Protect, Detect, Respond, and Recover (NIST, 2024). These functions assist organizations in managing cyber-security risks through governance, asset identification, continuous monitoring, incident response, and recovery planning. Likewise, ISO/IEC 27001:2022 establishes requirements for implementing an Information Security Management System (ISMS), emphasizing risk assessment, access control, asset management, continuous improvement, and organizational security governance (ISO, 2022). While these frameworks provide comprehensive guidance for managing information security risks, they primarily focus on governance, policy development, and organizational controls rather than intelligent threat detection. They do not prescribe adaptive machine learning techniques capable of learning from users' behavioural patterns or automatically detecting emerging cyber threats. Consequently, while NIST and ISO/IEC 27001 provide an essential governance foundation, they require complementary intelligent technologies to improve real-time detection of sophisticated cyber-attacks in digital library environments. The proposed adaptive ensemble learning framework seeks to complement rather than replace these established security frameworks by introducing predictive and adaptive threat detection capabilities.

2.4 Digital Libraries and Information Security Challenges

The increasing dependence on digital libraries has intensified concerns regarding cybersecurity and the protection of digital information resources. Idris et al. (2025) examined librarians' perspectives on the impact of cyber threats in the management of digital libraries in Kwara State, Nigeria. Their study identified data breaches, ransomware, and phishing attacks as major threats to digital library systems. Furthermore, the authors found that cybersecurity priorities differed across library types, with public libraries emphasizing data encryption and academic libraries focusing on access control and regular software updates. Using a Random Forest model, the study achieved a prediction accuracy of 95%, demonstrating the potential of machine learning techniques for assessing cyber threat exposure in digital library environments.

Digital libraries operate in highly interconnected environments that facilitate resource sharing, remote access, and collaborative data trading. While these features improve accessibility, they also introduce several security weaknesses. According to Abdelrahman (2026), virtual libraries face huge privacy and security challenges related to consumer data protection, unauthorized access, and cyber-attacks, and Hazarika and Konch (2025) similarly note that migration of library systems to cloud-based infrastructures has elevated concerns about information security, privacy and system flexibility. Evidence from the Nigerian context also suggests that many academic libraries continue to experience significant information security challenges. Musa and Yelwa (2025) investigated data privacy and security challenges in digital libraries of tertiary institutions in Zamfara State using a qualitative approach involving library personnel from two institutions. The study found that inadequate ICT infrastructure, insufficient staff training, limited financial resources, and weak institutional policies significantly constrained the protection of digital library resources. The authors recommended regular cyber-security awareness programmes, improved technological infrastructure, increased funding, and the development of institutional data privacy policies.

aligned with international standards. These findings demonstrate that cyber-security challenges in digital libraries extend beyond technological vulnerabilities to include organizational and human factors that influence the effectiveness of security management. Digital libraries increasingly face cyber-security threats that compromise the confidentiality, integrity, and availability of digital information resources. In a mixed-methods study, Magsi et al. (2025) examined cyber-security challenges in digital libraries and identified data breaches, unauthorized system access, malware attacks, and cyber intrusions as major threats affecting digital repositories. The authors further emphasized the importance of robust authentication mechanisms, data encryption, and proactive security strategies to strengthen the protection of digital collections. Their findings highlight that effective cyber-security requires a combination of technical safeguards and organizational preparedness to mitigate evolving cyber risks.

The primary security challenges confronting digital libraries include: unauthorized access to digital collections; identity theft and credential compromise; data leakage and privacy violations; malware and ransomware attacks; insider threats; distributed denial-of-service (DDoS) attacks; and exploitation of software vulnerabilities.

These challenges necessitate proactive security approaches capable of identifying threats before substantial damage occurs.

2.5 Machine Learning and Cyber-security in Digital Libraries

Machine learning technology has demonstrated significant potential in cyber-security programs. Unlike conventional rule-based systems, machine learning algorithms can examine vast amounts of data, detect hidden patterns, and detect atypical behavior. Beena and Kabir (2019) note that machine learning techniques have accelerated the capabilities of digital libraries by improving information retrieval, automation, and security management. In cyber-security contexts, machine learning models are widely used for anomaly detection, malware identification, intrusion detection, and threat intelligence. The increasing complexity of cyber threats has urged researchers to develop smart detection structures capable of reading historical and real-time data.

Similarly, Nissim et al. (2019) proposed an active machine learning framework (Sec-Lib) designed to protect scholarly digital libraries from malicious or infected documents, demonstrating that intelligent learning models can significantly strengthen digital library security by detecting threats that conventional approaches may overlook. Schmitt (2023) argues that AI-powered security systems offer great benefits in detecting state-of-the-art attacks that regularly bypass conventional protection controls. As a result, machine learning has become a fundamental component of digital library security frameworks of the current era.

2.6 Understanding Real-Time Adaptive Ensemble Learning

The effectiveness of ensemble learning has been demonstrated across various cyber-security domains. Uppal et al. (2025) found that combining multiple supervised learning algorithms substantially improved intrusion detection performance compared with individual classifiers. Their proposed ensemble framework achieved an overall detection accuracy of 99.82%, indicating that ensemble approaches are highly suitable for real-time intrusion detection applications. These findings provide empirical support for incorporating ensemble learning into digital library security architectures.

The Real-Time Adaptive Ensemble Learning combines three concepts:

Real-Time Learning: Real-time learning allows security systems to analyze incoming information immediately as soon as it is generated. In digital libraries, user activities consisting of logins, searches, downloads, and database queries can be monitored continuously to be immediately notified of suspicious behavior.

Adaptive Learning: Adaptive learning allows security systems to adjust their detection mechanisms based on evolving user behaviors and emerging threats. Unlike static models that require periodic retraining, adaptive systems continuously update their knowledge base as new information becomes available.

Ensemble Learning: Ensemble learning integrates multiple machine learning models to enhance predictive performance. Rather than relying on a single classifier, the ensemble system combines outputs from several algorithms, including random forests, decision trees, support vector machines, and neural networks, to achieve

better recognition accuracy. The integration of these three capabilities creates a robust framework capable of identifying both known and previously unseen cyber threats.

2.7 Continual Analysis of User Access Streams

User access streams refer to the continuous flow of data generated through user interactions within digital library environments. These interactions include: authentication requests; search activities; resource downloads; database access; navigation patterns; and session durations. Continuous analysis involves tracking those activities in real time to detect deviations from everyday behavior patterns. For example, an individual who downloads hundreds of files at once within a short period of time may exhibit behavior that is inconsistent with established usage patterns. Such anomalies may also hint at compromised credentials, automated scraping, or malicious intent. Continuous analysis structures use these observations to refine their detection capabilities, thereby improving long-term protection performance.

3. Theoretical Framework

This study is grounded in three complementary theoretical perspectives: the Confidentiality, Integrity, and Availability (CIA) Triad, Denning's Intrusion Detection Model, and Machine Learning Theory. These theories collectively provide the conceptual and technical foundation for the proposed adaptive ensemble learning framework. The CIA Triad defines the fundamental objectives of information security, Denning's model explains anomaly-based intrusion detection, and Machine Learning Theory justifies the use of ensemble learning techniques for intelligent threat detection in digital library environments.

3.1 Confidentiality, Integrity, and Availability (CIA) Triad

The CIA Triad is one of the most widely accepted models in information security and provides the foundation for protecting digital information systems (NIST, 2024; ISO, 2022). It consists of three core principles: confidentiality, integrity, and availability.

Confidentiality ensures that information is accessible only to authorized users. In digital libraries, this involves protecting users' personal information, institutional repositories, and subscription-based electronic resources through appropriate authentication, access control, and encryption mechanisms. Integrity refers to maintaining the accuracy, consistency, and reliability of digital information by preventing unauthorized modification or destruction. This is particularly important in digital libraries, where cyber-attacks such as malware, ransomware, or unauthorized alterations can compromise the authenticity of scholarly resources. Availability ensures that authorized users can access digital library resources whenever needed. Maintaining service availability is essential because teaching, learning, and research increasingly depend on uninterrupted access to electronic information resources.

The CIA Triad therefore provides the security objectives that guide the proposed framework. The adaptive ensemble learning model is designed to strengthen these three principles by improving the detection and prevention of cyber-security threats in digital library systems.

3.2 Denning's Intrusion Detection Model

Denning's Intrusion Detection Model (1987) provides the theoretical basis for behavioural monitoring within the proposed framework. The model suggests that computer systems can detect cyberattacks by continuously monitoring users' activities and identifying behaviours that deviate from established patterns. Unlike traditional signature-based detection methods, anomaly-based detection can identify previously unknown attacks by recognizing unusual system activities.

This approach is particularly relevant to digital libraries because legitimate users generally exhibit predictable patterns when accessing electronic resources, while malicious users often display abnormal behaviours. By continuously analysing user activities, adaptive security systems can detect suspicious actions before significant damage occurs. The proposed framework builds on Denning's model by incorporating adaptive machine learning techniques that continuously update behavioural profiles as user activities change over time.

3.3 Machine Learning Theory

Machine Learning Theory provides the computational foundation for the proposed framework. Machine learning enables computer systems to learn from historical data and identify patterns that support intelligent decision-making. In cyber-security, machine learning algorithms are widely used to detect malicious activities and classify normal and abnormal user behaviour.

Among the various machine learning approaches, ensemble learning has demonstrated superior performance because it combines the predictions of multiple classifiers to improve detection accuracy and reduce classification errors (Dietterich, 2000; Breiman, 2001; Zhou, 2012). Techniques such as Random Forest, Boosting, and Stacking have been successfully applied in cyber-security due to their ability to improve predictive performance compared with single classifiers.

However, ensemble learning also has limitations. Training multiple models requires greater computational resources, increased processing time, and more technical expertise than using individual classifiers. In addition, ensemble models are often difficult to interpret, making it challenging for administrators to understand how classification decisions are made. These limitations may affect the implementation of ensemble learning in smaller academic libraries with limited financial and technological resources. Nevertheless, the improved accuracy and adaptability of ensemble methods make them suitable for detecting evolving cyber threats in digital library environments.

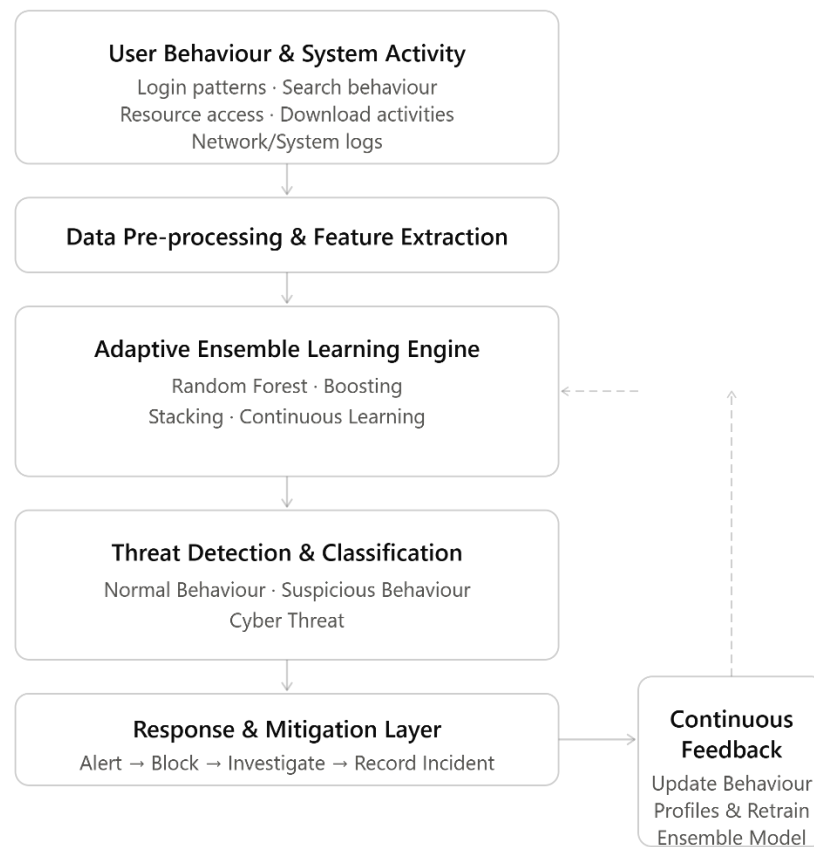
3.4 Theoretical Basis of the Proposed Framework

The proposed adaptive ensemble learning framework integrates these three theoretical perspectives. The CIA Triad defines the security objectives of protecting confidentiality, integrity, and availability. Denning's Intrusion Detection Model provides the foundation for detecting anomalous user behaviour, while Machine Learning Theory supports the use of adaptive ensemble learning to improve threat detection accuracy. Together, these theories provide a comprehensive foundation for developing an intelligent cyber-security framework capable of responding to evolving security threats in digital libraries.

Conceptual Framework: Security in Digital Libraries through Real-Time Adaptive Ensemble Learning and Continual Analysis of User Access Streams

Figure 1: Proposed Conceptual Framework for Security in Digital Libraries

**Conceptual Framework: Security in Digital Libraries through
Real-Time Adaptive Ensemble Learning and Continual Analysis of User Access Streams**



Source: Developed by the authors

This paper proposes a conceptual framework consisting of six interconnected components:

- 1. User Behaviour and System Activity:** This component collects information about users' interactions with the digital library, such as login attempts, search activities, resource access, downloads, and system logs. These activities provide the data needed to distinguish normal behaviour from suspicious activities.
- 2. Data Pre-processing and Feature Extraction:** The collected data are cleaned, organized, and transformed into meaningful features before analysis. This process removes irrelevant information and improves the efficiency and accuracy of the machine learning model.
- 3. Adaptive Ensemble Learning Engine:** This is the core of the framework. It combines multiple machine learning algorithms, such as Random Forest and Boosting, to analyse user behaviour and detect cyber threats more accurately than a single algorithm. The model continuously learns from new data, enabling it to adapt to changing attack patterns.
- 4. Threat Detection and Classification:** The ensemble model analyses processed data and classifies activities as either normal, suspicious, or malicious. This enables the framework to identify potential cyber threats while minimizing false alarms.
- 5. Response and Mitigation Layer:** Once a threat is detected, the framework initiates appropriate security actions. It generates an alert to notify administrators, blocks suspicious activities or unauthorized users, investigates the incident to determine its cause and impact, and records the incident for future analysis and security improvement.

6. Continuous Feedback: The framework continuously learns from detected incidents and user behaviour. Information from previous attacks is used to update the ensemble learning model, improving its ability to detect new and emerging cyber threats while adapting to changes in user behaviour over time.

4. Methodology

This study adopted a conceptual analysis approach to develop an adaptive ensemble learning framework for enhancing cybersecurity in digital libraries. The approach was considered appropriate because it enables the integration of existing theories, concepts, and empirical evidence to address a research problem and propose a theoretically grounded framework (Jaakkola, 2020).

The framework was developed through a comprehensive review of peer-reviewed literature on digital library cyber-security, intrusion detection, ensemble learning, adaptive learning, and established cybersecurity frameworks, including the NIST Cyber-security Framework (CSF 2.0) and ISO/IEC 27001. Relevant studies were identified from reputable academic databases such as Scopus, IEEE Xplore, SpringerLink, ScienceDirect, and Google Scholar. The selected literature was critically analysed and synthesized to identify key concepts and relationships, which informed the development of the proposed framework. The framework is theoretically grounded in the CIA Triad, Denning's Intrusion Detection Model, and Machine Learning Theory. As a conceptual study, the framework has not been empirically validated and is intended to provide a foundation for future implementation and evaluation in digital library environments.

5. Implications for Library and Information Science

The proposed adaptive ensemble learning framework has important implications for Library and Information Science (LIS), particularly in Nigeria and other developing countries where digital libraries are expanding. As cyber-security becomes an essential aspect of digital library management, library professionals need skills in cyber-security, artificial intelligence, and data governance. The framework complements existing security standards, such as the NIST Cyber-security Framework and ISO/IEC 27001, by improving real-time threat detection and response. The adoption of artificial intelligence for digital library security also changes the responsibilities of librarians and information professionals. Beyond managing information resources, professionals are increasingly expected to participate in cyber-security governance, risk assessment, and user education. Pasipamire (2024) emphasizes that fostering a culture of cyber-security awareness within libraries is essential for reducing human-related vulnerabilities and ensuring the sustainable protection of digital information assets.

However, implementing the framework may be challenging due to limited funding, inadequate ICT infrastructure, and shortages of skilled personnel in many Nigerian and African academic libraries. A phased implementation approach, beginning with basic cyber-security controls before introducing advanced machine learning techniques, would be more practical for resource-constrained institutions. Additionally, libraries must ensure that behavioural monitoring is conducted ethically, with due regard for user privacy, transparency, and data protection. Such an approach can strengthen the security and sustainability of digital library services while remaining feasible for developing-country contexts.

6. Conclusion

The increasing sophistication of cyber threats requires digital libraries to adopt intelligent and adaptive cyber-security solutions beyond traditional security mechanisms. This paper proposed an Adaptive Ensemble Learning Framework that integrates the CIA Triad, Denning's Intrusion Detection Model, and Machine Learning Theory to enhance real-time threat detection, behavioural analysis, and incident response in digital library environments. By combining these theoretical perspectives with adaptive ensemble learning, the framework contributes to the existing literature by providing a conceptually grounded approach to improving the confidentiality, integrity, and availability of digital library resources.

Nevertheless, the proposed framework is conceptual and has not yet been empirically validated. Its implementation may also be constrained by limited ICT infrastructure, financial resources, and technical expertise, particularly in

many Nigerian and African academic libraries. Future research should therefore focus on implementing and evaluating the framework in real-world digital library settings, comparing its performance with existing cyber-security approaches, and assessing its scalability, cost-effectiveness, and impact on user privacy. Such studies will provide empirical evidence to refine the framework and support its practical adoption in digital library environments.

7. AI Use Declaration

The authors declare that artificial intelligence (AI) tools were used solely to support language editing and manuscript refinement during the preparation of this article. Specifically, QuillBot was used for paraphrasing, summarization and improving sentence clarity and readability. No AI-based tools were used for data collection, statistical analysis, interpretation of findings, or formulation of conclusions. All intellectual contributions are entirely the responsibility of the authors. The authors further confirm that the manuscript has been critically reviewed and validated to ensure academic integrity and originality.

References

- Abdelrahman, O. H. (2026). Privacy and security challenges to user data in digital libraries: A literature review. *Cybrarians Journal*, 78. <https://doi.org/10.70000/cj.2026.78.670>
- Aregbesola, A., & Nwaolise, E. L. (2023). Securing digital collections: Cyber security best practices for academic libraries in developing countries. *Library Philosophy and Practice (e-journal)*, Article 7822. <https://digitalcommons.unl.edu/libphilprac/7822>
- Beena, A. L., & Kabir, H. S. (2019). Machine learning and security applications in digital library. *International Journal of Innovative Technology and Exploring Engineering*, 9(1), 2165–2168. <https://doi.org/10.35940/IJITEE.AL4718.11>
- Breiman, L. (2001). Random forests. *Machine Learning*, 45(1), 5–32. <https://doi.org/10.1023/A:1010933404324>
- Denning, D. E. (1987). An intrusion-detection model. *IEEE Transactions on Software Engineering*, 13(2), 222–232. <https://doi.org/10.1109/TSE.1987.232894>
- Dietterich, T. G. (2000). Ensemble methods in machine learning. In *Multiple classifier systems* (pp. 1–15). Springer. https://doi.org/10.1007/3-540-45014-9_1
- Hazarika, H. J., & Konch, P. K. (2025). Securing knowledge in the cloud: Implementing a library software package with enhanced security measures. *Program: Electronic Library and Information Systems*. <https://doi.org/10.1177/09557490251340819>
- Idris, O. I., Yusuf, A. A., Bolakale, L. A., & Muhammad, T. J. (2025). Perspectives of librarians on the impact of cyber threats in the management of digital libraries in Kwara State, Nigeria. *FUDMA Journal of Sciences*, 9(12), 9–19. <https://doi.org/10.33003/fjs-2025-0912-3990>
- Imamverdiyev, Y. N. (2017). IDEA4SP: An information security model for digital libraries. *Problems of Information Society*, 8(2), 65–72. <https://doi.org/10.25045/jpis.v08.i2.08>
- International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.
- Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, 10(1–2), 18–26. <https://doi.org/10.1007/s13162-020-00161-0>
- Jones, B., & Salo, D. (2018). Learning analytics and the academic library: Professional ethics commitments at a crossroads. *College & Research Libraries*, 79(3), 304–323.
- 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. <https://doi.org/10.71145/rjsp.v3i1.102>
- Musa, H., & Yelwa, A. S. (2025). Data privacy and security challenges in digital libraries of tertiary institutions in Zamfara State. *FUGUS International Journal of Library and Information Science*, 2(2). <https://doi.org/10.57233/fijlis.v2i2.08>
- National Institute of Standards and Technology. (2024). *Cybersecurity Framework (CSF) 2.0*. U.S. Department of Commerce. <https://www.nist.gov/cyberframework>

- Ngwum, N., Raina, S., Aguon, S., Taylor, B., & Kaza, S. (2020). A model for security evaluation of digital libraries: A case study on a cybersecurity curriculum library. *Journal of the Colloquium for Information Systems Security Education*, 7(1). <https://doi.org/10.53735/cisse.v7i1.115>
- Nissim, N., Cohen, A., Wu, J., Lanzi, A., Rokach, L., Elovici, Y., & Giles, L. (2019). Sec-Lib: Protecting scholarly digital libraries from infected papers using active machine learning framework. *IEEE Access*, 7, 110050–110073. <https://doi.org/10.1109/ACCESS.2019.2933197>
- Pasipamire, E. (2024). Building a culture of cybersecurity awareness in libraries: A systematic review of best practices and frameworks. Paper presented at the 23rd European Conference on Cyber Warfare and Security. ProQuest. <https://www.proquest.com/openview/1e8c55a3195b7105a8b77f608ea0175a/1>
- Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with AI-enabled malware and intrusion detection. *Journal of Industrial Information Integration*, 36. <https://doi.org/10.1016/j.jii.2023.100520>
- Uppal, M., Gulzar, Y., Gupta, D., Uppal, J., Kumar, M., & Saini, S. (2025). Enhancing accuracy through ensemble-based machine learning for intrusion detection and privacy preservation over the network of smart cities. *Discover Internet of Things*, 5(11). <https://doi.org/10.1007/s43926-025-00101-z>
- Zhu, D., Wei, Y., Cai, J., Wang, J., & Chen, Z. (2025). A security data detection and management method in digital library network based on deep learning. *Frontiers in Physics*, 12. <https://doi.org/10.3389/fphy.2024.1492114>
- Zhou, Z.-H. (2012). Ensemble methods: Foundations and algorithms. *Machine Learning & Pattern Recognition Series*. Chapman & Hall/CRC. <https://tjzhifei.github.io/links/EMFA.pdf>