Impact Factor 6.1

Journal of Cyber Security

ISSN:2096-1146

Scopus

DOI

Google Scholar

More Information
www.journalcybersecurity.com

Crossref doi Google Scholar scopus

AI and Cybersecurity in Academic Libraries: Emerging Trends and Best Practices

[1.]Dr. Gulshan Kumar Sachdeva
Librarian, Delhi School of Business, VIPS-TC, Pitampura, Delhi-110034
ORCID: 0009-0001-3079-0037

[2.]Dr. Mukesh Sachdeva
Librarian, Vivekananda Institute of Professional Studies, Delhi-110034

[3.]Dr. Anil Kumar Jharotia
University Librarian, The NorthCap University, Gurugram-122017
ORCID: 0000-0002-9720-6376

ABSTRACT

AI technology developments that largely improve the quality of user services, facilitate the automation process, and raise accessibility levels are a big step academically for the libraries of the universities. Not to Mention, these innovations bring along new threats to libraries, such as those related to intellectual property, privacy, and data that are vulnerable due to inadequate library cybersecurity measures. The present study points at the best techniques to alleviate the mentioned threats by assessing the potential and already established AI technologies for cybersecurity aimed at academic libraries. This research will investigate AI-based security technology, find important technology gaps and develop a realistic model for academic libraries to practice cybersecurity stewardship timelessly. The study will rely on expert interviews, institutional case studies, and a literature review, and the results from the research will be pointing out the need for cyber risk governance being proactive, cybersecurity talent development, and ethical artificial intelligence adoption for the purpose of protecting information systems in libraries against constant and new cyber-attacks.

Keywords: Academic Libraries, Artificial Intelligence (AI), AI-Driven Security, Cyber Security, Data Protection,

1. INTRODUCTION

Unlike previously, academic libraries have become more digital and are still being regarded as an essential ecosystem for the development of education, research, and innovation. AI, playing a key role in recommendation systems, analytics, virtual reference AI, and automated cataloging, has contributed to making the library functions and the users' interactions more refined and effective.

The digitizing and changing process in libraries, which is continuous, has been accompanied by the always-on threat of cyber-attacks. Nowadays, libraries have to face the problems of identity theft, ransomware, phishing, unauthorized access, and data breaches, that may lead, among other things, to serious consequences for the research output of the institution, user privacy, and subscription-based digital resources.

Such cyberattacks, along with the lack of privacy protection for user data and confidentiality of resources, do not leave any doubt that academic libraries need to strengthen their systems which, in turn, put AI on the side of both ethical and legal issues. This paper is an attempt to find out how academic libraries would deploy AI effectively to security measures and develop the best practices to carry out safe digital operations.

2. OBJECTIVES OF THE STUDY

The present research is focused on comprehending the correlation between AI and security in academic libraries. Essentially, the libraries' adoption of digital solutions for the storage, retrieval, and sharing of information is the main reason for the justifying the potentials and issues raised by the AI implementation. Nevertheless, the difficult side of the story is that there exist some problematic issues that have to be recognized as well. Thus, this study is centered on a main goal with numerous sub-goals that will be achieved:

1. **To investigate how AI helps in the protection of digital assets in academic libraries, and how AI strengthens library cybersecurity systems**.

This goal takes predictive analytics, machine learning, and automated threat detection into account and looks into how far these systems can be applied to enhance the cybersecurity framework of a library. The research investigates AI's capability in recognizing threats, blocking access, and managing threats in real time to secure digital collections, patron information, and institutional data.

2. **To detect and evaluate the rapid change of the digital environment, the common cybersecurity problems facing academic libraries**.

The very first authentic goal of this project is to identify the threats and challenges academic libraries are dealing with. The list of these threats is long and very scary for libraries; it mainly includes ransomware attacks, phishing, data breaches, and hacked accounts. Also, the lack of internal training, budget, and policies are among the issues that indirectly contribute to the absence of cybersecurity measures.

3. **To look into the newest trends and technologies in the field of AI-focused cybersecurity in relation to library information systems**.

Afterwards, the new possibilities for library cybersecurity that AI offers are specifically pointed out, being the detection of unauthorized access, biometric systems, blockchain technology for securing information, and automatic assessment of risky digital library services.

4. **To provide safe, AI-assisted methods and well-thought-out strategies that ensure data security while respecting the privacy of users and the authority of institutions**.

Essentially, our objective is to formulate the rules and regulations that are feasible for the morally correct use of AI in libraries. The approach used here not only highlights the importance of ethics, observance of data protection laws, training of staff, but also the establishment of uniform cybersecurity standards that could significantly enhance the digital resilience of academic institutions.

3. LITERATURE REVIEW

3.1 Cybersecurity in Academic Libraries

Academic libraries must protect their online materials, library systems and user data. As more patrons access library databases and e-journals remotely, libraries face greater risk of cyberattacks. As Gupta (2022) noted, libraries store important academic information as well as sensitive user data, so the data must be kept safe. Because of this, libraries are more vulnerable to cybercriminals.

To protect their patrons' data, libraries must adopt protective cyber security practices that are commensurate with their level of risk. As the IFLA-International Federation of Library Associations has advised, this means implementing appropriate, secure, accessible and reliable digital systems and library services.

3.2 Role of Artificial Intelligence

AI influences nearly every function of contemporary libraries. As Kumar and Sharma (2021) noted, AI powers more intelligent searching and customized recommendation systems. More broadly, AI streamlines the processes of cataloging, indexing and analyzing user behavior to anticipate their future needs.

In the war against cybercrime, AI can be a step ahead in spotting the danger and taking measures to lessen it. By analyzing the traffic in the network, AI algorithms can detect the patterns of behavior that have deviated from the norm thus allowing the organizations to help the possible cyber threats on their own terms before the damage goes to a considerable level.

3.3 Cyber Threat Landscape

The University Libraries are equally open to cyber-attacks as any other digital institution. Some of their face dangers are listed below**:**

- Phishing attacks, when the hackers deceive library personnel or users into giving away confidential information.
- Ransomware that seizes the electronic archives or educational data and demands a release fee.
- Data stealing that causes a leak of secret user details or institutional information.
- Unauthorized accessing of online databases and payment services, frequently via faked IP addresses and stolen login credentials.

If these threats are not managed properly, they can lead to libraries' shutting down, security breaches, and their negative reputation affecting the organization's reputation.

3.4 AI for Cyber Defense

To maintain the safety of the cyber space in which they operate, libraries have no option but to invest in cybersecurity approaches that integrate AI. For instance, Intrusion Detection Systems, (IDS) and analytical tools are capable of using AI for the continuous monitoring of activities, detection of abnormal behaviors that are different from the usual computer operations, and the notification of the users about possible cyber threats. On the other hand, Deep Learning algorithms are set up to study the previous threats and in so doing indirectly aid the unveiling

of new attack methods, among which the most challenging one's technically referred to as zero-day vulnerabilities are the ones that have never been encountered before (Raj and Bhardwaj, 2023).

AI is a mixed blessing that has a lot of popularity but also a lot of drawbacks. Neglecting to use AI responsibly can lead to ethical and privacy issues stemming from data monitoring and algorithm bias. In this regard, human intervention is necessary to supervise and control AI when it is used in the field of cybersecurity.

3.5 Research Gaps

Several studies have been done on the application of the AI in library management and the use of AI in cybersecurity in general, however, a very small number of such studies have been done on the use of AI to enhance the security of information systems in university libraries.

Such a gap in the research is very prominent in India where libraries are making a transition to digital. This study is intent on bridging this gap. It studies concepts and implements them in the school library security framework with the use of AI.

4. RESEARCH METHODOLOGY

4.1 Research Design

The purpose is to provide a panoramic view that blends tech, law, and morals. We employed a mixed-methods approach involving both quantitative and qualitative aspects in this study. Such a combination enabled us to obtain a more comprehensive and equitable view of the influence of AI on cybersecurity in college and university libraries.

We focused on academic libraries located in the Delhi/NCR area of India, where the majority of schools are beginning to implement digital technology and AI tools. Through the examination of these libraries, we intended to figure out the exact influence of technology on security solutions in academic libraries all over the globe at present.

4.2 Data Collection

For this research, we employed various data sources, including primary and secondary data, to obtain the necessary information:

- Primary Data: We used predetermined questions with 60 people, including librarians and IT workers, from 10 schools to get direct information about the use of AI tools, cyber safety issues, and how much librarians are aware of these things. Besides that, we interviewed 10 experts - senior librarians and cyber safety pros - to know more insights and get their expert views on what works best and how to put these ideas into action.
- Secondary Data: We have collected secondary data by reviewing various already existing sources. Some of these sources include research journals, books, policy reports, and officially recognized cybersecurity guidelines such as NIST (National Institute of Standards and Technology) and CERT-IN (Computer Emergency Response Team – India). These materials gave us the necessary context and information regarding GBS AI and the intricacies of cybersecurity management in educational institutions globally.

4.3 Data Analysis

We started our analysis after collecting the data by

- As for the survey data, we performed the statistics at a very basic level. This enabled us to summarise the info in percentages, charts, and tables. It facilitated the data presentation as well as pointing out general trends in a visually way.
- As for the narrative data, we examined the interviews looking for common themes. We identified the repeated concepts that people mentioned most combining these approaches allowed the research to uncover fresh trends, practical problems, and effective methods of using AI-driven tools for cybersecurity in school libraries.

5. Findings and Analysis

In this part, we will discuss the main outcomes which are based on data gathered via surveys and interviews. I have pointed out the level of AI usage, the cyber threats to academic libraries, the trends in AI for security, and the necessity for training and awareness among staff members.

5.1 Level of AI Adoption

The research indicates that a large number of libraries located in the Delhi/NCR area are actively taking up Adobe (AI) tools as a way to improve their virtual services. Close to 70 percent of these libraries stated that they were applying some type of AI technology, mostly for analytics of users, discovery of resources, or assistance via chatbots.

Of those libraries, only 35 percent are applying AI technology for security functions like anomaly detection, threat prediction, or controlling access. This could mean that a lot of libraries are incorporating AI into their systems with the aim to provide a better user experience, however, the security aspect of AI is still underutilized in library services and there is still room for improvement in that area through technology.

AI Application Area	**Percentage of Libraries Using AI**
User Analytics and Discovery Tools	70%
Chatbots and Virtual Assistants	60%
AI in Cybersecurity (Threat Detection, Access Control)	35%
Predictive Maintenance and Automation	25%

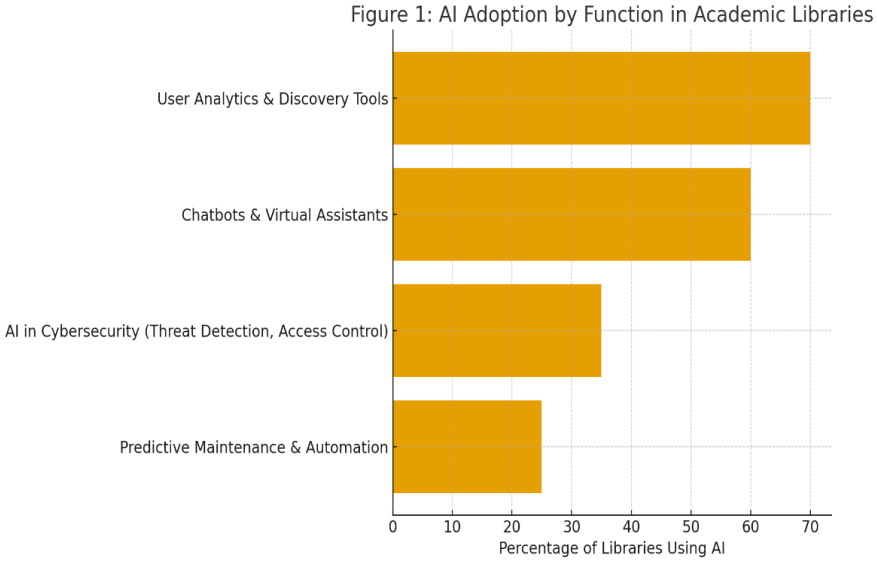

Figure 1 presents the findings in the form of a bar chart, which indicates how different functions in academic libraries adopt AI. The data suggests that the most widespread use of AI is in the area of user analytics and chatbots, while the application of AI to security is still at its infancy stage.

5.2 Common Cybersecurity Challenges

Additionally, the research brought forward a number of shared challenges that hinder the establishment of effective cybersecurity in academic libraries. Among the factors mentioned by the interviewees were:

- A significant portion of library personnel is not adequately trained in cybersecurity, hence they are prone to making mistakes and being ignorant of the risks.
- Often the IT security budget is too small, which results in libraries lacking to invest in good security software or people with expertise.
- Many libraries find themselves using obsolete firewalls and antivirus programs which are unable to counter new threats.
- Libraries have become an increasing number who are unhelpful in terms of cybersecurity since they are with no support.

The research highlights that there is a lack of institutional backing and provision of training for academic libraries to develop a robust cybersecurity culture which is a vital one**.**

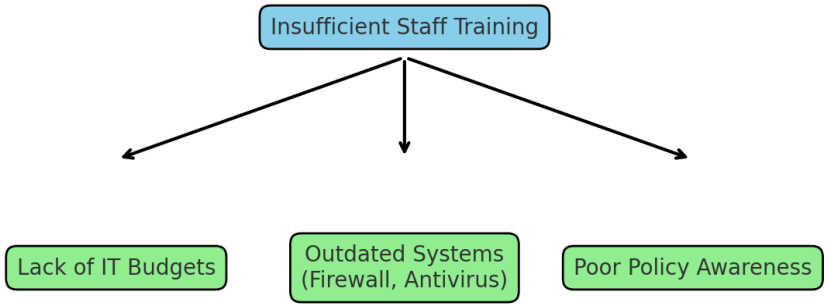

Figure 2: a graph showing the recurring cybersecurity difficulties that the library takes are they also record that lack of staff training is strongly linked to issues such as tight IT budgets, outdated systems, and a general lack of awareness of policies.

5.3 Emerging AI Trends in Library Cybersecurity

The research has also revealed that few futuristic trends AI being used to secure libraries are:

1. **Predictive Threat Detection:** Libraries are increasingly turning to machine learning models that evaluate system behavior to locate potential cyberattacks before they occur.
2. **Demonstrative Security Monitoring:** AI-powered dashboard has been enged to user activity monitoring, login attempts tracking, and automatically flagling of suspicious activity of all types continuosly and proactivly thus they are able to notify the aid requests even before they have arrived.
3. **Data Encryption and Blockchain:** A few libraries are experimenting with blockchain technology to establish unchangeable and transparent records for digital resource management.
4. **AI-Powered Access Control:** AI-powered authentication mechanisms utilize AI-based risk scoring to grant or refuse user access depending on login behavior, device type, or other features.

These developments point to the emergence of intelligent, self-learning systems capable of lessening human mistakes and handling cyber incidents much faster.

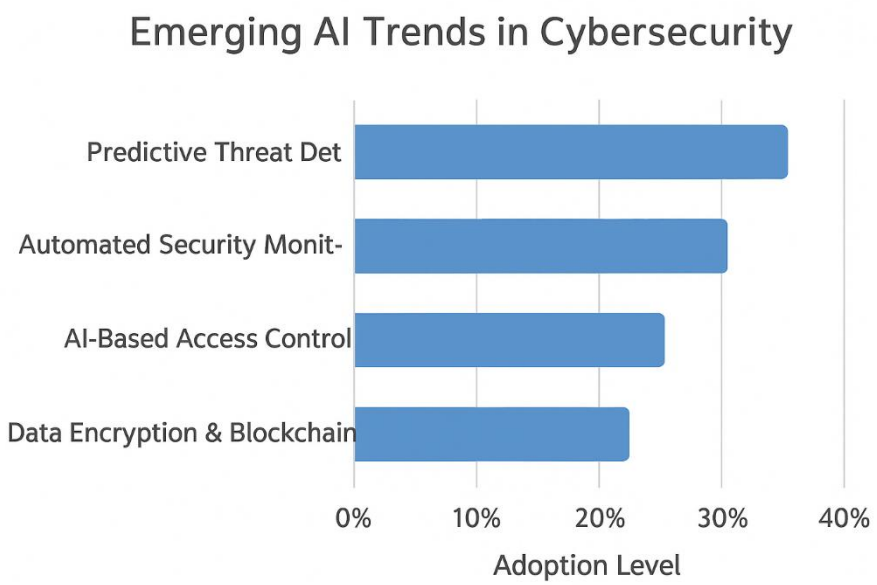

Figure 3: AI Trends in Library Cybersecurity (Delhi/NCR Academic Institutions) would contain:

- It is a horizontal bar chart, describing the extent of adoption of various AI applications in cyber security in academic libraries.
- On the X-axis, the Adoption Level (%) is indicated, while the Y-axis shows the trends.

AI Trend	**Adoption Level (Approx.)**	**Potential Impact**
Predictive Threat Detection	45%	High
Automated Security Monitoring	40%	High
Data Encryption & Blockchain	25%	Moderate
AI-Based Access Control	30%	High

5.4 Staff Awareness and Training

A major issue revealed by this study is the inconsistency of training and awareness among library personnel. Only 42% of library employees indicated that they had received formal training for cyber security.

Many places of employment characterized their training as scheduled and often reactive, meaning that it takes place after a cyber-event. Respondents, interviewees, and librarians agreed that continual professional growth is fundamental to managing cyber security costs.

Most also believe further inclusion between librarians and IT departments should occur to create a sense of shared responsibility for digital safety.

Training Type	Percentage of Respondents
Formally Trained	42%
Untrained / Minimal Training	58%

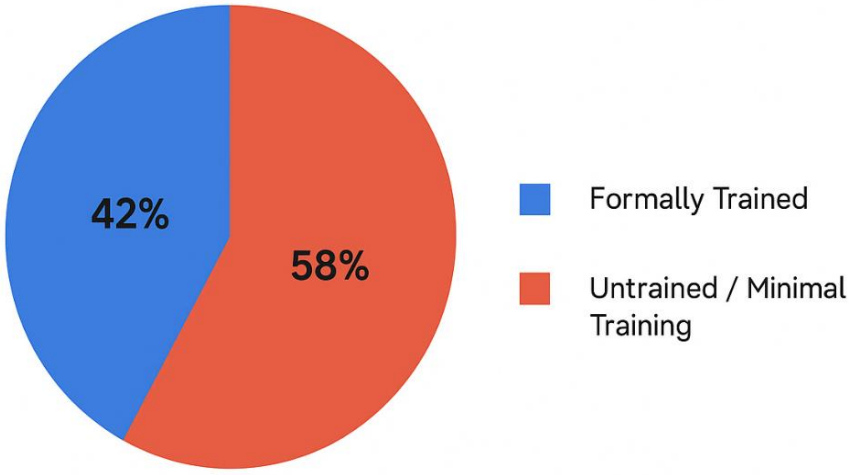

Figure 4 - Pie Chart- Cyber Security Training Status of Library Staff, or in other words, the pie chart will be a two-part simple pie chart reflecting the training or lack thereof of staff:

- Formally Trained: 42%
- Untrained/Minimal Training: 58%

Summary of Key Insights

- The adoption rate of AI is high for user services, but low for cybersecurity operation.
- Cybersecurity problems arise primarily as learning/awareness, funding or systems are all outdated.
- AI initiatives like predictive & threat detection and blockchain have all performed positively. Staff awareness level is low which speaks to the need to build institutional capacity.

6. DISCUSSION

6.1 The Dual Role of AI

The AI technology used in libraries can be seen as a double-edged sword. It can improve the security of libraries through analytics and automation and at the same time, cause issues if not managed properly. For example, AI may inadvertently collect personal information clumsily, thus causing privacy and surveillance issues to arise.

6.2 Integration Challenges

The use of AI tools in library management systems requires not only a solid technical support but also a hefty financial investment. A good number of libraries depend on outsourced IT support and the data protection experts will not always match with library operations.

6.3 Ethical and Policy Implications

There are ethical obligations that involve the need for a transparency in AI algorithms, the requirement of the user consent, and the establishment of the data governance policies that are sound. It is up to each institution to establish the data collection guidelines that are clear and to make sure that there is a compliance with the regulations such as the Digital Personal Data Protection Act, 2023 (India) and the GDPR when one is in a collaboration with another institution**.**

6.4 Best Practices Identified

This study has pinpointed best practices in these areas:

1. **Adopt AI-Enhanced Security Tools:** Implement machine learning-based intrusion detection and threat monitoring.
2. **Develop Cybersecurity Policy Frameworks:** Align library policies with institutional IT governance.
3. **Regular Training and Awareness:** Conduct periodic cybersecurity drills and awareness workshops.
4. **Data Privacy and Ethical AI Use:** Implement data minimization, anonymization, and transparent algorithms.
5. **Collaborative Security Networks:** Engage in knowledge-sharing with other libraries and cybersecurity agencies.
6. **Backup and Recovery Plans:** Ensure regular data backups and implement disaster recovery protocols.

7. CONCLUSION

As academic libraries transform into digital learning centres, the implementation of AI is accompanied with immense advantages and complicated cyber risks. The research emphasis on the urgency of the setting of strong rules and moral standards when developing AI-based security solutions. Academic libraries, instead of perfecting the new technology, should accept it, and also kindle the staff and user’s awareness of cybersecurity.

By itself, the incorporation of AI in a vigilant and ethical way can help libraries to keep their digital records safe, protect the privacy of users, and safeguard the trust of academic information systems. It is recommended that further research be carried out to create quantitative risk models and to assess the impact of AI-driven security measures on library services over time, particularly concerning the quality of services provided.

8. REFERENCES

- Almeida, F., & Silva, M. (2021). AI-enabled risk assessment frameworks for information security management. Information Systems Frontiers, 23(2), 345–358.
- Choudhary, D. (2023). Awareness and implementation of cybersecurity policies in university libraries: A case study from India. Journal of Library Administration, 63(4), 289–305.
- Computer Emergency Response Team – India (CERT-IN). (2022). Guidelines for information security practices in academic and research institutions. Ministry of Electronics and Information Technology, Government of India.
- Gupta, R. (2022). Cybersecurity Practices in Indian Academic Libraries: Challenges and Opportunities. Journal of Library and Information Technology, 39(2), 67–75.
- International Federation of Library Associations (IFLA). (2022). Guidelines for Library Information Security.
- Jain, P., & Tiwari, K. (2023). Staff training and cybersecurity literacy in Indian university libraries. Annals of Library and Information Studies, 70(2), 145–152.
- Johnson, T., & Becker, L. (2022). Machine learning for data protection in higher education environments. Computers & Security, 115, 102598. https://doi.org/10.1016/j.cose.2022.102598
- Jharotia, A.K. (2024). Cybercrime and Prevention: An Awareness Overview, Manupatra (E-Database of Law) 13 Sept. 2024, Copyright © Manupatra http://artapp.manupatra.com/UserArticles/ViewSingleArticleDetails?iarticleguId=372d61d1-f125-4ff4-b2f7-468dae4ee1d7
- Kumar, A., & Sharma, D. (2021). Artificial Intelligence Applications in Academic Libraries. Library Hi-Tech, 39(4), 1120–1135.
- National Institute of Standards and Technology (NIST). (2020). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce. Retrieved from https://www.nist.gov/cyberframework
- Nguyen, H., & Lee, D. (2022). Blockchain technology for academic record management and cybersecurity. Journal of Information Technology Education, 21, 115–132.
- O'Connor, M. (2024). Ethical implications of AI in data privacy and cybersecurity in higher education. AI & Society, 39(1), 59–73. https://doi.org/10.1007/s00146-023-01655-2
- Pandey, M., & Mehta, R. (2020). Digital transformation and cybersecurity in academic libraries: Opportunities and challenges. DESIDOC Journal of Library & Information Technology, 40(6), 423–430. https://doi.org/10.14429/djlit.40.06.15700
- Patel, S., & George, E. (2021). Emerging trends in AI-based intrusion detection systems for educational institutions. International Journal of Computer Applications, 183(10), 22–28.
- Raj, A., & Bhardwaj, R. (2023). AI-driven cybersecurity frameworks for higher education institutions. Journal of Information Security Research, 12(2), 87–99. https://doi.org/10.1016/j.jisr.2023.04.003.
- Singh, N., & Verma, A. (2024). Integrating AI with cybersecurity in Indian academic libraries: A strategic approach. Asian Journal of Library and Information Science, 16(1), 21–34.