NOVATEUR PUBLICATIONS
JournalNX- A Multidisciplinary Peer Reviewed Journal
ISSN No: 2581 - 4230
VOLUME 12, ISSUE 8, August – 2026

CYBER SECURITY CHALLENGES IN DIGITAL LIBRARIES TRANSFORMING LIBRARIES IN VIKSIT BHARAT 2047: A STUDY

Gourav Rajput
Research Scholar, Dept. of Library & Information Science,
Maharani Laxmibai Arts & Commerce College, Gwalior

Jyotsana Rajouriya
Research Scholar, Dept. of Library & Information Science,
Maharani Laxmibai Arts & Commerce College, Gwalior

Abstract
The vision of "Viksit Bharat 2047"(Developed India) aim a technologically advanced, self-reliant, and digitally empowered India, digital libraries playing a significant role in research, education, and Informative society. This paper explores the cyber security threats faced by digital libraries, It reviews existing literature on cyber security in libraries and highlights the importance of robust security measures the paper also discusses future trends in cyber security

Keyword: Viksit Bharat, Data Privacy, Digital Library, Cyber Security

1. INTRODUCTION

The objective of "Viksit Bharat 2047" (Developed India) is to build a technology-rich, self-reliant, and digitally empowered country, where digital libraries are essential for research, education, and fostering an informed citizenry. Digital libraries exemplify advancements in this idea by expanding access to information, aiding research initiatives, and enhancing educational experiences. However, the transition to a completely digital and secure setting has introduced numerous cyber security challenges, particularly for libraries that store large quantities of sensitive data such as users' names, addresses, phone numbers, and email IDs.

The advancement of the digital library has presented a set of challenges with cybersecurity concerns being one of the most Challenging issues in the modern world, libraries are highly vulnerable to phishing, malware attacks, data breaches, denial of service, insider threats, social engineering attacks, unauthorized access, and even web spying. There are many methods through which the security of a library can be breached.

Access to e-resources has make larger the potential of libraries, greatly transforming their role and how information is stored or disseminated. With convenient access to necessary information through libraries, there is a notable boost in data privacy and protection.

Digital libraries play pivotal role of India’s efforts to foster research education and economic growth. These libraries are focus to provide an information and resource and help to creations a strong knowledge drawn society

2.1 Vision and Goal of Viksit Bharat

2.1.1 Equality of Opportunity in Digital Revolution of India

In digital world can remove the gape between the rural and urban population viksit bharat play crucial to remove the digital gape

2.1.2 Digitalization

Two other global trends are especially important for India of 2050. Digitization and Green economy. Important steps taken by the Government to develop digital infrastructure, like Aadhar, UPI, ONDC, Digi Locker and financial & health stacks, need to be broadened & accelerated. (Virmani, 2024)

2.1.3 Digital Teacher (E-Achray)

AI can solve these problems for all classes of teaching and learning, from pre-school to High school. Such an expert system can be designed for a multiplicity of tasks, like providing teaching aids and materials to qualified teachers, directing local teaching assistants in rural 41 Citizens, old or young, men or women, will have Foundational Literacy and Numeracy (FLN). 43 areas to perform at teacher level, and directly help lagging students to catch up or stimulate advanced students. (Virmani, 2024)

2.1.4 Digital Skilling (E-Guru)

The former requires training in an Industrial training facility where the materials, tools, equipment and machinery that is to be used for training is available. To some extent simulators can be used to improve the quality of training, reduce material requirements, and scale up the training, by incurring higher capital cost. (Virmani, 2024)

2.1.5 Digital Economy: Expert System AI

India is on the verge of a Digital revolution. This revolution is transforming the nature of consumption, production, work and social relations. From our perspective the revolution can be used to eliminate the tyranny of geography (remote & hilly areas), gender disparity (skills, work differentials), inequality in quasi-public goods (rural-urban education-health quality) and information asymmetry (formal-informal firms, govt – citizen)0001 (Virmani, 2024)

2.1.6 Digital Regulations

The economics of digital regulations has revealed four important elements relevant for regulation of the digital economy. (1) Economies and Scale and scope are much deeper and broader than in the bricks and mortar economy. (2) Network externalities are unique to telecommunication systems and the digital economy. (3) Data is a unique natural resource, (4) 67 Algorithms can give the illusion of being neutral and more objective than human beings, but can be as much if not more biased, while being undetectable. (Virmani, 2024)

3. Cybercrime

Cybercrime refers to illegal activities that involve computers or networks. It can take many forms, affecting individuals, organizations, and governments and libraries

Cybercrime may be defined as "Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of a crime". (Saroha, 2014)
Professor S.T. Viswanathan has proposed three potential definitions of cybercrimes, any unlawful action where a computer serves as the tool or object of the crime. In other Words, any crime that aims to affect the operation of a computer. Any incident involving computer technology that causes or could potentially cause harm to a victim, resulting in a perpetrator gaining or potentially gaining something of value Intentionally. Computer abuse refers to any illegal, unethical, or unauthorized behavior related to the automatic processing and transmission of data (Bhavsar, 2017)

3.1 Types of cyber-crimes on libraries

3.1.1 Phishing – Phishing attacks use phony emails and messages to obtain private information, including personal information. Phishing attempts to get access to the library repository may target digital libraries

3.1.2 Data Breaches –When unauthorized access to sensitive information stored in library system. These breaches can affect both physical and digital records**;** jeopardize user privacy and the overall trust in organization. Libraries are huge amount of personal data including, name addresses borrowing histories

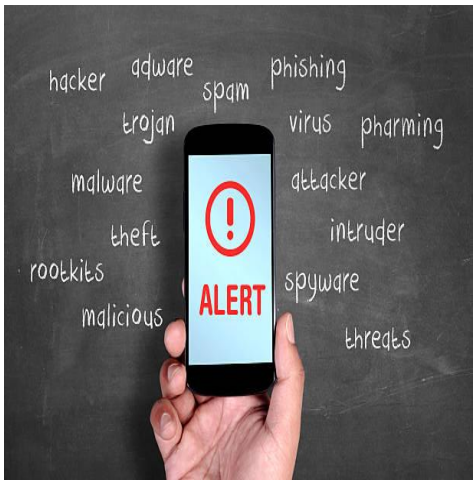

Figure 1 Type of Cyber Crime in Libraries

3.1.3 Malware –Malicious software can affect the library network , can damage or help to enter the unauthorized access to sensitive information , such as user records , patron information some malware are virus , worm , Trojan , spyware, ransom ware
3.1.4 Denial of service (DoS)-A denial of service (DoS) attack a malicious attempt to sack down the targeted server Library became the target of a distributed denial of service (DDoS) network attack that resulted in the disruption of Library services and websites, including the U.S. Copyright Office, the BARD service from the National Library Service for the Blind and Physically Handicapped, our many databases, and both incoming and outgoing email

3.1.5 Insider Threats-An insider threat can happen when someone close to an organization with authorized access misuses that access to negatively impact the organization's critical information or systems. This person does not necessarily need to be an employee—third-party vendors, contractors, and partners could also pose a threat.

3.1.6 Social Engineering –Social engineering is referring to use to non technical individual to gain an unauthorized access to information, resource or system. This method has real threat to computer industry but in recent time libraries face this type of threat because they have amount of data and personal records of user Example vishing,smishing, baiting

4. Cyber Security Challenges for Libraries

Digital libraries can significantly face their cyber security challenges . These are a few significant aspects that can pose challenges to digital libraries.

4.1 Lack of Infrastructure

One major problem that might jeopardize the security of digital assets, user data, and the library's overall integrity is the absence of cybersecurity infrastructure in digital libraries. Vulnerability to Data Breaches, Inadequate Authentication & Authorization, Inadequate Backup and Disaster Recovery.

4.2 Use Insecure Public Wifi

for cyberattacks cybersecurity risk for digital libraries is the use of public Wi-Fi that is insecure and can allow multiple potential attacks on both the user and the library through the infrastructure. Wired networks in public spaces.

4.3 Lack of IT professionals

If these libraries lack trained cybersecurity specialists to keep their systems secure and up-to-date, they expose themselves to cyberattacks, data Digital libraries.

4.4 Use Outdated Software and Systems

Outdated software in digital libraries poses a cybersecurity major threat and exposes libraries to diverse cyber threats when these systems are running outdated or unsupported software, vulnerabilities that have been patched in newer versions persist, exposing the entire system to cyberattacks, data leaks and other forms of exploitation.

5. Current Cyber Security Measures in Digital Libraries

Digital libraries take some safety measure in cyber threat to ensuring the protection of sensitive and important information, prevention in unauthorized access, so various libraries taken some preventive measure to ensure the integrity and privacy of the resource. Some current cyber security measure is as

5.1 Data Encryption – Information is kept in formats that cannot be easily understood, including e-books, academic papers, and encrypted personal data, which serve to safeguard against unauthorized access.

5.2 Strong Password – Libraries recommend that users implement robust measures to secure their accounts and mitigate insider threats.

5.3 Bio-Metrics – A biometric authentication system has been installed to prevent unauthorized access to the library's server room.

5.4 Used Next Generation firewall – Organization install firewall system to regulate and monitors all incoming outgoing traffic and based on define set of security rule . Next gen firewall consist deep packet inspection system , it insure that malicious file are not affect the data of organization

Figure 2 Next Generation Firewall (Sheldon, 2021)

5.6 Intrusion Detection System (IDS*)*

An intrusion detection system (IDS) can help accelerate and automate network threat detection by alerting security administrators to known or potential threats, or by sending alerts to a centralized security tool. (IBM, 2023)

5.7 Proxy Server

A proxy server is a gate that separates your computer and the Internet. Meaning, when you type a URL, instead of searching for it on the Internet, Your request will first go through a proxy server and then, to the Internet (Yogendra, 2022)

5.8 Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs) allow organizations to provide secure connectivity between devices in physically separate locations Providing a second layer of defense against misconfigured, unlatched, or poorly designed internal services (Device Security Guidance, 2021)

6. Future Trends

6.1 Harnessing the Power of Artificial Intelligence in Cyber security

Artificial intelligence has emerged as a fundamental component in improving cyber security in multiple industries. By leveraging machine learning algorithms, AI has facilitated the creation of automated solutions that can perform tasks such as natural language understanding, facial recognition, and

detecting threats. Conversely, cybercriminals are also using this technology to devise intricate tactics aimed at overcoming security measures.

6.2 Block Chain Technology

Blockchain technology is a framework that maintains transactional records, commonly referred to as blocks, which are interconnected through nodes. Its primary characteristics include decentralization, transparency, and immutability. Blockchain has the capability to safeguard sensitive information, defend intellectual property rights, and thwart unauthorized access.

6.3 Cloud-Based Data Security

Cloud-based data security in digital libraries encompasses the methods, technologies, and practices used to protect digital content, user information, and other sensitive data stored and managed in a cloud environment. Some notable cloud service providers include AWS, Amazon, Microsoft Azure, Google Cloud Platform, and IBM Cloud.

6.4 Emergence of Quantum Computing: A New Horizon

Quantum computing signifies a groundbreaking development in cybersecurity that could considerably affect businesses, governments, and libraries.. A quantum-ready cyber security framework requires a workforce skilled in quantum mechanics and quantum computing. (FORTINET)

6.5 AI Predicting Attack Scenarios

By analyzing vast datasets of past attacks and security incidents, generative AI can identify patterns and trends, enabling it to predict potential future attack scenarios. This predictive capability allows organizations to stay one step ahead of cybercriminals and proactively implement countermeasures

7. Notable Cyber Security Breaks

7.1 On October 28, 2023, **Toronto Public Library** suffered a ransom ware attack that took key technical systems offline, including the library's internal network, website and public computers. As Library Journal reported, "Although TPL managed to keep all of its 100 branches open and host programs throughout the ordeal, patrons were unable to access their library accounts online or use the library's computers for more than two months. (Enis, 2024)

7.2 On the very same day, the **British Library** began to experience technical issues, including an outage of its Wi-Fi network and online catalog. As it turned out, the United Kingdom's largest library had been targeted in a ransom ware attack by a hacker group called Rhysida. When the library refused to pay the ransom, the hackers leaked some 600GB of data onto the dark web, including personal details of library users and staff members. The British Library has estimated it will use about 40% of its financial reserves — around £6–7 million, to recover from the attack. (British Library , 2023)

7.3 Seattle Public Library, Meanwhile, is still dealing with the fallout of a May 25, 2024, ransom ware attack. According to a June 18 article from The Stranger, users can still check out physical and digital media through the Libby app and the Seattle Public Library Overdrive site, and all 27 branch buildings remain open. Many vital services, however, are still missing: "Borrowers cannot return physical media or place holds on anything, Interlibrary Loans are down, in-building Wi-Fi is down, public computers

are down, mobile hotspots are virtually impossible to checkout, the catalog won't update, and no one can use the printers." (Lahud-Zahner, 2024)

7.4 Cyber attack on AIIMS: December 2022 In December 2022, the All-India Institute of Medical Sciences (AIIMS) suffered a significant cyber attack, leading to the encryption of about 1.3 terabytes of data across five servers. The incident was attributed to unauthorized network access, exacerbated by inadequate network segmentation. While no ransom was demanded, the attack underscored vulnerabilities in critical healthcare infrastructure. Fortunately, e-Hospital data was restored from an unaffected backup, and application functionalities were reinstated within two weeks. (sattrix, 2024)

7.5 Telangana Police's Hawk Eye App Data Breach: 2023 The Telangana police's Hawk Eye app experienced a data breach, exposing sensitive information of approximately 200,000 citizens. The breach, attributed to hacker "Adm1nFr1end" involved personal data such as phone numbers and addresses. The police were able to track the hacker and make an arrest, highlight the importance of proactive cyber security measures. (sattrix, 2024)

8. Preventive Measures in Cyber Security Threats

8.1 Use of Updated System: Ensure that the system and software of library are updated. Install the most recent security updates to fix bugs, intrusions and security challenges software update regularly

8.2 Firewall and Antivirus Software: Use of firewall to restrict the unauthorized access to a system, use a reputable antivirus and anti malware software to detect and remove malicious software

8.3 Employee Training: If you run a business, train your employees about the risks of cyber threats and how to prevent them. This includes safe internet usage, recognizing phishing attempts, and reporting any suspicious activities.

8.4 Regular Backups: Regularly back up your important data to an external drive or cloud storage. This ensures that you have a copy of your data in case of a cyber attack like ransom ware**.**

8.5 Use Secure Network: The library must ensure that users utilize a secure network, avoiding public Wi-Fi, and accessing the secure network system instead**.**

9. Conclusion

As digital libraries continue to grow, they will aid India's transition into a developed country by 2047. However, an area that needs immediate focus is cyber security. If cutting-edge technologies are adopted and a culture of cyber security is instilled, then digital libraries can protect resources, user data, and contribute to a digitally empowered Viksit Bharat cyber threat is biggest challenge to the digital libraries .To address these challenges, digital libraries need to implement strong cyber security measures, including data encryption, strict password policies, biometric authentication, and advanced firewalls. Furthermore, new technologies like Artificial Intelligence (AI) and block chain present valuable opportunities for improving threat detection, safeguarding sensitive information, and blocking unauthorized access. Additionally, cloud-based data protection offers scalable and effective security solutions for handling digital content and user data. . The future of maintaining the credibility of digital libraries as reputable sources of knowledge rests on how they manage the shifting borders of cyber security

References

1. (n.d.). Retrieved from FORTINET: https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity
2. (2023, 10). Retrieved from British Library : https://www.bl.uk/cyber-incident/
3. (2023, 4 19). Retrieved from IBM: https://www.ibm.com/think/topics/intrusion-detection-system
4. (2024, 12 27). Retrieved from sattrix: https://www.sattrix.com/blog/biggest-cyber-attacks-in-india/
5. (2024, 12 27). Retrieved from sattrix: https://www.sattrix.com/blog/biggest-cyber-attacks-in-india/
6. Bhavsar, S. B. (2017). Cyber Crime and Measures to Prevent in Libraries. *An International Peer Reviewed Bilingual E-Journal of Library* , 3(5), 38-47.
7. *Device Security Guidance*. (2021, 6 29). Retrieved from National Cyber Security Centre : https://www.ncsc.gov.uk/collection/device-security-guidance/infrastructure/virtual-private-networks
8. Enis, M. (2024 , 1 7). Retrieved from Library jouranl: https://www.libraryjournal.com/story/toronto-public-library-recovers-from-ransomware-attack
9. Lahud-Zahner, C. (2024, 6 18). Retrieved from The Stranger : https://www.thestranger.com/news/2024/06/18/79563956/were-making-it-work
10. Saroha, R. (2014). Profilling a Cyber Criminal. *International Jouranl of Information and Computation Technology* , 253-258.
11. Sheldon. (2021, 10 21). *FS.* Retrieved from https://www.fs.com/blog/what-is-a-nextgeneration-firewall-14097.html
12. Virmani, A. (2024). *NITI WORKING PAPER VIKSIT BHARAT: UNSHACKLING JOB CREATORS , EMPOWERING GROWTH DRIVERS.* New Delhi.
13. Yogendra, P. (2022, 6 23). *NEXGEN*. Retrieved from What is a Proxy Server and how does it work: https://www.nexgi.com/digital-library/proxy-server/