Academic Libraries and Their Patrons' Digital Data Privacy: a systematic literature review

Shivangi Singh

Junior Research Fellow, Department of Library and Information Science, Panjab University, Chandigarh

Dr. Khushpreet Singh Brar

Assistant Professor, Department of Library and Information Science, Panjab University, Chandigarh

Abstract

This systematic literature review is performed to analyse the current state and gaps in knowledge of user data security in libraries. It explores the critical issue of digital data privacy for patrons in academic libraries, examining the evolving landscape of information technology and its impact on data security. The data were collected from well-known databases, that as, Library Information Science and Technology Abstracts (LISTA), Library and Information Science Abstracts (LISA), Emerald Insight, Scopus, and Web of Science. It followed the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to choose relevant articles with keyword searching. It was identified from the review that this digital expansion raises concerns about the privacy and security of patrons' personal information. Various threats and vulnerabilities are identified, encompassing hardware and software security, network security settings, data security, third-party applications, RFID systems, and the IoT environment. Challenges such as the lack of regulatory policies, limited access to resources, inadequate training and awareness, connectivity issues, and technical challenges are also highlighted. To mitigate these challenges, potential strategies are proposed, including implementing artificial intelligence and block chain technologies, pseudonym and obfuscation techniques, and leveraging authentication systems like Shibboleth, etc. This research addresses a critical and evolving concern in the modern library environment, where the security of user digital data is paramount. The research provides practical recommendations for enhancing digital data security in library settings and has the potential to influence the way libraries approach information security and user privacy.

Keywords: Data and information security policy, Digital data security, Library data security, Patron digital data privacy, Systematic literature review

1. Introduction

Information and communication are the core needs of a society. Thus, to add value to the information it is necessary to provide early and easy access to it. Evolving technologies are dictating over every aspect of human necessity and academic communities. Advanced data analytics and artificial intelligence are propelling us into a realm of predictive and prescriptive analytics (Biswas, 2023), fostering disruptive advancements. These innovations have the potential to revolutionise society, paving the way for a promising future. Such development has compelled and urged us to accept the deluge

of information communication technologies (ICTs).Libraries are no such exceptions to it. The underlying consequence of the prominence of ICT is the threat to users' data.

Modern day libraries have transformed into digital and virtual libraries that serve information and resources mostly in electronic and digital forms and are also not restricted by time or space. Such ongoing expansion in digital libraries around the world brings to attention the shortcomings in addressing privacy and security related issues.

Additionally, the introduction of IoT gadgets in the library suggests a conjunction between various equipment that use the internet as their communication medium which holds great potential to strengthen the concept of "smart" libraries but also poses some threats to the library's administration and patrons (Igbinovia & Okuonghae, 2021). Among the top 10 security issues with IoT devices, according to the OWASP Internet of Things Top Ten Project, HP Security Research discovered an average of 25 vulnerabilities per device. Attackers were able to identify legitimate user accounts through enumeration on seven out of ten of the devices when used in conjunction with their cloud and mobile applications (Chickowski, 2014). This necessitates heightened vigilance and awareness of the security risks inherent in the situation.

In light of the introduction of big data into libraries, it can also jeopardise the privacy of library patrons' personal information such are readers' reading behaviour, personal preferences, social relations, etc., as it can be collected, integrated, analysed, and mined to forecast reader demand and track desired services (Fangjing, 2021).

Incorporating a cloud network into resource sharing between academic institutions and institutional libraries can foster information sharing and offer robust technical support for the specialised services offered by university libraries. Since the services are offered over the Internet thus, it becomes very difficult to assess the physical location of servers and software and scrutinising the security is hard to undertake. Due to these wide range of services and users that a library caters to, it is vulnerable to data security threats.

2. Background of the study

The excessive use and collection of data has resulted in increasing privacy implications within the library and information services, their users and society. According to (IFLA Statement on Privacy in the Library, 2015) commercial internet services, especially those that provide library and information services, gather a lot of information about users and their behaviour. Privacy as described by Universal Declaration of Human Rights under article 12 states that:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation"(United Nations: Peace, dignity, equality on a healthy planet, 2018).

The dogma of Information Security (IS) seeks confidentiality, integrity and availability (Whitman & Mattord, 2021) and thus every element of a security system in an organisation must serve and implement such principles. A library environment is exposed to both external and internal threats, thus the professionals must possess sufficient knowledge of various cyber-security issues to combat cyber threats (Ibinovia & Ishola, 2023). Furthermore, Sun and Ma (2014) discussed the features of libraries in the Big Data era and their influence on information security of libraries.

In addition to instructional technologies, organisations can and frequently do collect information about user interactions with virtual assistants, smart phones, tablets, wearable gear, computers, sensors, and ID card readers (Kyle et. al, 2020). As pointed out by Megan Oakleaf (2015), to assess and research the relationships between student library interactions and student learning and success measures, librarians may adopt such Library Analytics (LA) practices. Moreover, worms, viruses, plagiarism, flaming, hacking, and misinformation are the threats as a result of dysfunctional human behaviour as identified by Ikolo (2019).

Thus, to address such challenges, a library environment dealing with information and data handling must be holistically secured. Ayofe and Irwin (2010) people and professionals who use the internet for personal and professional tasks should receive training on how to protect their systems from harmful attacks and maintain the security and integrity of their data. Therefore, it is necessary to train and retrain library professionals on cyber security issues to guard against un-authorised access to their patron's data and secure their e-resources.

3. Research objectives

User data security threat is a major problem in all its forms and manifestations. This paper answers the following research questions to:

RQ1. What are the data and information security measures that have been proposed in the existing literature?

RQ2. What gaps and open issues emerge from the analysis of existing literature?

4. Methodology

The systematic review technique promotes thorough and organised ways of reviewing the literature and systematic analysis of published research, which can also be considered as a component of qualitative research (Bearman et. al, 2012). This paper included the utilisation of the Preferred Reporting Items for Systematic Reviews and Meta Analysis (PRISMA) for the review of current literature (Moher et al, 2015).

4.1 *Sources of information*

The search was performed on 5 different well-known databases namely LISTA (Library, Information Science and Technology Abstracts | EBSCO), LISA (LISA: Library and Information Science Abstracts (proquest.com)), Emerald Insights (Discover Journals, Books & Case Studies | Emerald Insight), Scopus (Scopus - Document search) and Web of Science database (https://www.webofscience.com/wos/woscc/basic-search).

To perform the systematic review of literature, different sets of keywords have been applied to carry out the results with the required objectives:

- 'Information security in libraries'
- 'Data privacy'
- 'User data privacy'
- 'Digital information security'
- 'Patron anonymity'
- 'Library security policy'
- 'Information security management policies in Libraries'
- 'Data security measures in libraries'

The publication year was restricted from 2013-2023 and only English language studies were included in the review.

4.2 *Criteria for inclusion*

Only those studies that presented academic libraries were selected for systematic review.

- Book chapters were not included
- Articles without abstract were not included
- Documents or studies with fewer than 4 pages were excluded
- The medium of document included is strictly English
- Only journal articles have been included in the review
- Titles dating back to 2013 have been taken

Other types of libraries, such as those devoted to computer programming languages, are not included in this study.The majority of data security dedicated studies in the fields of IT, business, health, education, and cloud computing were disregarded.

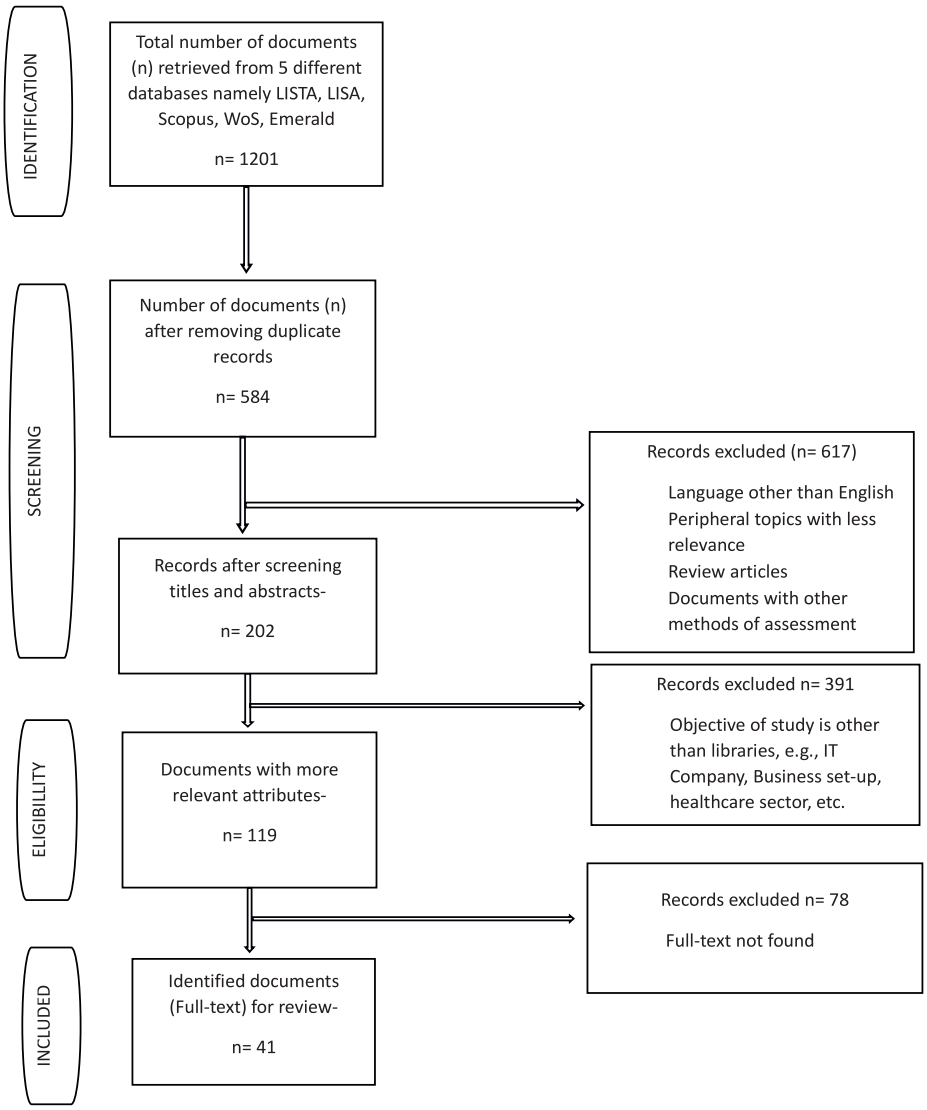

Figure 1: PRISMA chart on data and information security in academic libraries

Figure 1 (PRISMA diagram) shows a flow chart outlining the scanning process as well as the criteria used to exclude research and choose those that qualify. Data scanning included title, abstract, and full-text papers in two stages. 41 studies were chosen for inclusion based on the evaluation of the selection criteria. For each qualified study, a material extraction framework was used to compile information on the Data and Information Security in libraries. For each qualifying study, a data extraction table was created to gather data on the title, author(s), publication year, nation, population, participants, outcomes, difficulties, and conclusions.

5. Result and discussions

Overview of the studies undertaken

A search in five different databases and search engines was conducted, yielding 1201 studies on data and information security in libraries from well-known databases i.e., LISTA, LISA, Scopus, Web of Science and Emerald.

After the removal of duplicates, the number of the remaining studies stood at 584, after initial scanning and exclusion of records based on various reasons, 617 studies were excluded. Criteria were further narrowed down, and only 119 studies were found relevant to the overall data and information security in the libraries. However, 41 studies were ultimately chosen to meet the research objectives and inclusion criteria based on the topic in academic libraries. The selected studies were from 2013 to 2023, and most of the studies were published in Library and Information Science, Information Communication and IT journals, International Conference Proceedings, with some in business and e-commerce industries.

Preferred study designs of selected studies

Of the selected 41 articles under review, USA posed 15 documents that scrutinised user data and information privacy in libraries, followed by China, India and Nigeria. In this review (Figure 2), 12 studies were quantitative in method with survey design and data was collected through a structured questionnaire and most of the respondents were academic librarians and library heads. Qualitative method has only been adopted in 2 studies. Conceptual papers have been provided by 9 studies wherein a conclusion has been drawn after defining and mapping the objectives. Moreover, exploratory, mixed methods, case studies have also been adopted.

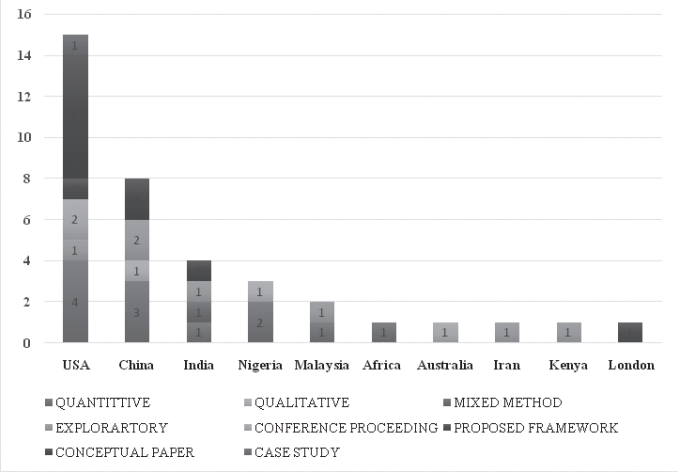

Figure 2: Types of studies published globally, identifying threats to user data and information privacy methodologically

5.1 *Core threats identified in present scenario*

Library in particular deals with two types of patron data which is PII- Personally Identifiable Information and Non PII- Non-Personally Identifiable Document. Security of electronic, physical and users' assets is not strictly a technological requirement but is a foundational element for almost all academic libraries.

Gressel (2014) emphasised that libraries must create and put into place rules for the security of user and staff data. Different countries have adopted different policies on information systems and abide by rules for protecting their user's data under national schemes. These policies may cover information systems, data security, data privacy, user registration ID and passwords, data backups and software that steal users' personal information. Hess (2014) in his work pointed out that libraries must follow federal, state, and institutional regulations regarding student privacy and information security in addition to the Library Bill of Rights and related documents.

Patron data anonymity is a growing concern for the library set-up. However, in India no or very few schemes have been implemented to look after the security of the library and its users' data. India in the current scenario is lying back from the other countries as it does not have any dedicated policy to abide by, thus making it exposed to various security threats.

The core threats identified after reviewing the existing literature are mentioned below in table 1.

Table 1: Core threats and sub-threats identified for library and its patron's data privacy-complied by author

Core Threats	Sub-threats
Hardware Security	• Natural calamity that can jeopardise the hardware security, • Accidents such as stealing or vandalism, • Bugs or errors generated from routers or firewall, leading to the defect of hardware, • Malicious intrusion or destruction, • Cases of theft or vandalism, • Faulty equipment • Failure of power supply or communication equipment or services, • It also accounts for lack of maintenance, theft, physical sabotage etc.
Software Security	• Threats to operating systems • Application related threats such as copying software infected from malware (i.e., Computer viruses, ransom ware, worms and Trojan horses) (Shen, 1999) • Abuse of computer access control • Computers installed with spyware and adware • Failure of system software or system corruption • Installation or use of unauthorised programmes or software • Weak authentication mechanism • Use of pirated or unauthorised software • Unauthorised changes to software settings that can compromise the integrity of a computer system (Ibrahim & Umar, 2020)

Core Threats	Sub-threats
Network Security Settings	• Cracking of passwords • Damage to equipment due to uneven power supply • Internet based attacks on internal network resources • Transmission errors (Ajie, 2019) • Website Defacement- which is an attack usually initiated by a system cracker who breaks into a web server and changes the visual appearance of the website.
Data Security Threats	• Interruption of services • Exposure of patron's sensitive data due to web attack • Masquerading of user identity • Social engineering threats such as 1. Phishing, 2. Tailgating, 3. Impersonation, 4. Sniffing, 5. Baiting, 6. Dumpster diving, etc., • Unauthorised access and transfer of data
Third Party Applications on library websites	• Tracking cookies that may beutilised for 1. Advertising 2. Analytics 3. General and Invasive Fingerprinting (Marino, 2021)
RFID Systems	• Privacy of the borrower 1. Tracking 2. Hot-listing 3. Profiling (Butters, 2007) • Threats to the library 1. Digital vandalism 2. Tag-based viruses
IoT Environment	• Lack of updated process or mechanism • Unsecured network services and ecosystem interfaces • Outdated IoT app components

IoT devices are becoming more prevalent in our daily lives and libraries pose no exceptions to the use of such devices. As stated by Ram (2023) privacy-by-design principles should be used in IoT applications for libraries to guarantee data privacy. Strong security mechanisms, user-centric privacy frameworks, and user and stakeholder awareness are all necessary, said by Kumar and Mittal (2016). Moreover, according to HPE Cyber Risk Report 2016, attackers now concentrate majorly on applications rather than servers and operating systems thus, making the third-party library applications on library websites a threat to user data security. Privacy of item-level tagging has also been a concern when using RFID systems in libraries. The COVID-19 pandemic's effects on patronage of academic libraries were the subject of an OCLC survey in 2021. It was revealed that in university libraries, the use of digital resources has significantly increased, with e-books and online journals being the most frequently accessed publications, according to the survey. There is a risk that people's reading preferences could be utilised for purposes that violate their privacy and human rights due to the possibility of data profiling and tracking as stated by Arora (2023).

5.2 *Challenges indentified*

The "Privacy: An Interpretation of the Library Bill of Rights" document, created by the ALA, addresses the challenges of data protection in the digital age stating that:

"Confidentiality extends to, 'information sought or received and resources consulted, borrowed, acquired or transmitted,' including but not limited to: database search records, reference questions, and interview, circulation records, interlibrary loan records, information about materials downloaded or placed on 'hold' or 'reserve,' and other personally identifiable information about uses of library materials, programmes, facilities, or services" (American Library Association, 2006).

This view demonstrates the profession's dedication to upholding strict standards for client privacy, in spite of the challenges brought on by the digital age (Palmer, 2020).

Table 2: Challenges identified in implementing secure environment in library

Themes	Sub-themes
Lack of regulating policy	• For the protection of materials and user information and data, libraries lack a technological and organisational data and information security written policy and do not apply one (Aregbesola & Nwaolise, 2023). • No defined legal framework for regulations • Libraries do not have copyright policies for digital content in modern areas (Hess et. al, 2015)
Limited access to resources	• Developing nations frequently lack the financial and technological resources necessary to implement cyber security safeguards (Ajie, 2019).
Lack of training and awareness in professionals and owner of privacy data (Users)	• Lack of necessary training of the most recent cyber security dangers, safeguards and best practices • Users' un-explicit awareness of malpractices of sites before enclosing their personal data
Connectivity and Infrastructure Limitations	• Inadequate internet access and insecure infrastructure • Lower diffusion of information and communication technologies (Khan et. al, 2021)
Technical Challenges	• Challenges in libraries such as technical measures, data storage, operating and control system, server and password (Farid et. al, 2023)

According to Akporido (2011), a lack of cogent policy can lead to the creation (or continuation of) inefficient infrastructure and resource waste. One of the key findings of Khan (2021) suggested thatLIS practitioners, policymakers, and the government should realise the relevance and importance of data and information security measures within university libraries. Also, in the view of technical challenges, Ali and Soomro (2014) expressed that although ITIL (Information Technology Infrastructure Library) is a comprehensive IT framework but lacks information security management which needs to be catered for effective IT service management.

When it comes to breaches, carelessness is frequently a major issue. All personnel should receive frequent training from their employers on how to spot attacks and weaknesses and what to do next as pointed out

by Sarkar (2018).To ensure data privacy and security, it's crucial to foster awareness and understanding of Data Information Security Management (DISM) and its associated policies within libraries (Farid et. al, 2023). Library staff, administrators, and stake-holders play an active role in advocating for and putting into action DISM policies within their libraries and organisational settings.

5.3 *Possible theories of mitigation*

Enforcing optimal cyber security practices for digital collections can present significant challenges for libraries in developing nations. Since, academic libraries deal with sensitive user information, research data, and academic records. Libraries should implement strong measures to safeguard data privacy, such as ensuring secure transmission of data, obtaining user consent and granting them control, anonymising information, and integrating privacy-focused design principles. However, there is promise in various upcoming technologies and future strategies that can potentially bolster cyber security efforts within academic libraries. Artificial intelligence and Machine learning can automate threat detection and response. Simultaneously, block chain is a structured data arrangement where blocks of information link sequentially to form a chain. Each block is closely linked to its adjacent one, and the data within it is protected using cryptographic methods. When one block remains unchanged, altering other blocks becomes challenging, enhancing the security and dependability of storing library data (Zhao et. al, 2022).Thus, can enable secure and transparent transactions, protect intellectual property rights, and prevent un-authorised access or modifications to critical data (Zhang, 2019).

Besides the conventional technical security strategies like identity verification, access control, and data encryption employed for protecting data in digital libraries, additional measures such as pseudonym techniques (Gao et. al, 2013), obfuscation techniques (Duckham & Kulik, 2005), confusion techniques that provide location privacy, and encryption techniques can also be utilised to ensure the privacy of patrons' behavioural data. Shibboleth which provides a single-sign-on (SSO) service authentication system. This architecture was been defined by Scavo and Cantar (2005) as SAML (Security Assertion Markup Language).Libraries frequently utilise Shibboleth to ensure a smooth and secure user experience when accessing digital materials, databases, and online content. Shibboleth ensures the best data security and privacy protection to the users with the software based on SAML. Remote library services pose a serious challenge and burden beyond those already posed in regular library services. When it comes to safeguarding the privacy of patrons within the library setting, it is essential to give careful thought to consent and defined purposes for data usage, minimising the data collected, as well as employing techniques like anonymisation and pseudonymisation.

6. Conclusion

The review of the literature identified that libraries may be facing challenges without the Data and Information Security Policy as they do not adopt technical measures to secure the hardware, software, tools and networking (Han et. al, 2016). It has also been found that libraries faced issues with technical tools, hardware development, workstations, the Internet, data and network security. Further, in the view of Zongda Wu et. al (2022), as of now, the domain of library sciences still faces a notable gap in conducting thorough and organised research regarding the safeguarding of the privacy of readers' actions within the libraries. When financial resources permit, libraries should incorporate contemporary data breach detection tools to

achieve the highest possible level of security.

References

Ajie, I. (2019). A review of trends and issues of cybersecurity in academic libraries. *Library philosophy and practice.* (2015). Akamai's State of the Internet Security Report Q2. Retrieved from https://www.akamai.com/site/en/documents/state-of-the-internet/akamai-state-of-the-internet-report-q2-2015.pdf

Akporido, C. E., & Achugbue, E. (2011). National information and communication technology policy process. *Frameworks for ICT Policy: Government, Social and Legal Issues.*

Ali, S. M., & Soomro, T. R. (2014). Integration of information security essential controls into information technology infrastructure library: a proposed framework. *International Journal of Applied Science and Technology, American Library Association.* (2006, July 7). Retrieved from privacy: an interpretation of the library bill of rights: https://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy

Aregbesola, A., & Nwaolise, E. L. (2023). Securing digital collections: cyber security best practices for academic libraries in developing countries. *Library Philosophy and Practice.*

Arora, T. (2023, June 13). *Digital libraries: a boom amid privacy ceoncerns.* Retrieved from Deccan Herald: https://www.deccanherald.com/education/digital-libraries-a-boon-amid-privacy-concerns-1227237.html

Ayofe, A., & Irwin, B. (2010). Cyber security challanges and the way forward. GESJ: *Computer Science and Telecommunications,* 56-69.

Bearman, M., Smith, C., Carbone, A., & al., e. (2012). Systematic review methodology in higher education. *High Educ Res Dev* 31 (5), 625-640.

Biswas, A. (2023). Application of data analytics for mapping of library system and services of Oxford University Library. In *Technology Integration in Higher Education: opportunities and challenges.* New Delhi: NLUD Press. Retrieved from https://www.researchgate.net/publication/375447227_Application_of_Data_Analytics_for_Mapping_of_Library_System_and_Services_of_Oxford_University_Library

Butters, A. (2007). RFID systems, standards and privacy within libraries. *The electronic library,* 430-439.

Chickowski, E. (2014, July 29). *Internet of Things Contains Average of 25 Vulnerabilities Per Device.* Retrieved from Dark Reading: https://www.darkreading.com/vulnerabilities-threats/internet-of-things-contains-average-of-25-vulnerabilities-per-device

Duckham, M., & Kulik, L. (2005). A formal model of obfuscation and negotitation for location privacy. *Proc. 3rd Int. Conf. Pervasive Computing (PERVASIVE' 05).*

Fangjing, Y. (2021). Study on library individualized information security under the background of big data. *IEEE 6th International Conference on Big Data Analytics.* doi:10.1109/ICBDA51983.2021.9402989

Farid, G., Warraich, N., & Iftikhar, S. (2023). Digital information security management policy in academic libraries: a systematic review. *Journal of Information Science.*

Gao, S., Ma, J., & Shi, W. (2013). TrPF: a trajectory- privacy preserving framework for participatory sensing. *IEEE transactions on Information Forensics and Security.*

Gressel, M. (2014). Are libraries doing enough to safeguard their patrons' digital privacy? *The Serials Librarian.* doi:10.1080/0361526X.2014.939324

Han, Z., Huang, S., Li, H., & al., e. (2016). Risk assessment of digital library information security: a case study. *Electron Library,* 471-487.

Hess, A. N., LaPorte-Fiori, R., & Engwall, K. (2014). Preserving patron privacy in the 21st century academic library. *The Journal of*

Academic Librarianship. doi:http://dx.doi.org/10.1016/j.acalib.2014.10.010

Hess, A., LaPorte-Fiori, R., & Engwall, K. (2015). Preserving patron privacy in the 21st century academic library. *J Acad Lib,* 105-114.

Ibinovia, M. O., & Ishola, B. C. (2023). Cyber security in university libraries and implication for library and information science in Nigeria. *Digital Library Perspectives.*

Ibrahim, H. O., & Umar, F. A. (2020). Cyber security threats and its emerging trends on academic libraries. *International Journal of Academic Library and Information Science.*

IFLA. (2015, August 14). Retrieved from IFLA Statement on Privacy in the Library: https://www.ifla.org/wp-content/uploads/2019/05/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf

IFLA. (2022). *IFLA Repository.* Retrieved from IFLA Statement on Cybersecurity: https://repository.ifla.org/bitstream/123456789/1912/1/IFLA%20Statement%20on%20Cybersecurity.pdf

Igbinovia, M. O., & Okuonghae, O. (2021). Internet of things in contemporary academic. *Library Hi Tech News.* doi:10.1108/LHTN-05-2021-0019

Ikolo, V. (2019). Information ethics in 21st century. In K. Igwe, & S. a. Sadiku, *Themes and Trends in Information Science* (pp. 198-213). Lagos: Zea Commuications.

Khan, A., Ibrahim, M., & Hussain, A. (2021). An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. *International Journal of Information Management Data Insights.*

Kitchenham, B., et al. (2009). Systematic literature reviews in software engineering - a systematic literature review. *Information and Software Technology,* 7-15. doi:https://doi.org/10.1016/j.infsof.2008.09.009

Kumar, N., & Mittal, P. (2016). A review of Internet of Things (IoT) in the perspective of Privacy and Security. *International Computer Application.*

Kyle, M., A, B. K., Goben, A., Salo, D., Asher, A., & Perry, M. R. (2020). A comprehensive primer to library learning analytics practices, initiatives and privacy issues. *College & Research Libraries.*

Marino, B. (2021). Privacy concerns and the prevalence of third party tracking cookies on ARL Library homepages. *Reference Services Review,* 115-131. doi:10.1108/RSR-03-2021-0009

Moher, D., Shamseer, L & Clarke, M. (2015). Preferred reporting items for systematic review and meta analysis protocols (PRISMA-P) 2015 Statement. *Syst Review* 4(1), 1-9.

Oakleaf, M. (2015). The library's contribution to student learning: inspirations and aspirations. *College and Research Libraries.*

Palmer, M. (2020). I always feel lik eel like somebody e somebody's watching me: student p atching me: student perceptions ceptions. *Library and Information sience Commons.* doi:https://doi.org/10.51221/sc.scl.2020.4.1.9

Ram, B., Kumar, A., & Pal, S. K. (2023). Applications of the internet of things in library and data privacy. *IP Indian Journal of Library Science and Information,* 14-19.

Sarkar, I. (2018). Data breach: key to prevention and intrusion detection the risk of a library. *Indian Journal of Information Sources and Services,* 8-11.

Scavo, T., & Cantor, S. (2005). Shibboleth architecture technical overview: working draft 02.

Shen, W. Z. (1999). Attack and protection with hacker. *Communication of Information Security,* 86-96.

Sun, M., & Ma, L. (2014). Research on information security and privacy of libraries in big data era. *Avanced Material Research.* doi:10.4028/www.scientific.net/AMR.1049-1050.1934

Sun, N., & Ma, L. (2014). Big data, data privacy, users' privacy information security. *Advanced Materials Research. United Nations: Peace, dignity, equality on a healthy planet.* (2018, November 21). Retrieved from Universal Declaration of Human Rights at 70: 30 Articles on 30 Articles - Article 12: https://www.ohchr.org/en/press-releases/2018/11/universal-declaration-human-rights-70-30-articles-30-articles-article-12

Whitman, M., & Mattord, H. (2021). Principles of Information security. *Boston, MA: Cengage learning.*

Wu, Z., Shen, S., Li, H., Zhou, H., & Zou, D. (2022). Acomprehensive study to the protection of digital library readers' privacy underan untrusted network environment. *Library Hi Tech.* doi:10.1108/LHT-07-2021-0239

Zhang, L. (2019). Blockchain: the new technology and its applications for libraries. *Journal of Electronic Resources Librarianship,* 278-280. doi:https://doi.org/10.1080/1941126X.2019.1670488

Zhao, X., Chang, Y., Feng, H., & Huang, M. (2022). The data security problems discussion in application of library service platform. *SHS Web of Conferences.* doi://doi.org/10.1051/shsconf/202214001026