

Improving the Security and Privacy in Malaysia Academic Digital Libraries

Zairul Nizam Zainol*, Saiful Farik Mat Yatin, Mad Khir Johari Abdullah Sani

Faculty of Information Science, Universiti Teknologi MARA Cawangan Selangor, Kampus Puncak Perdana, 40150 Shah Alam, Selangor, Malaysia

Corresponding Authors' Email Address: z.b.zainol@gmail.com

ARTICLE INFO

Article history:

Received: 17 Mac 2025

Revised: 10 May 2025

Accepted: 22 May 2025

Online first

Published: 1 August 2025

Keywords:

digital libraries,
security,
privacy,
technology disruption

<https://doi.org/10.24191/jikm.v15iSI2.7819>

ABSTRACT

Digital libraries have become an important and valuable platform because they provide easy access to various information and resources that users need. However, as the digital world continues to develop and the technological revolution and so-called technology disruption, becomes increasingly complex, concerns have emerged about the risk of cyber threats and their impact on user privacy and security when accessing digital libraries. Therefore, the objectives of this study focus on present key issues facing digital libraries in relation to privacy and security, evaluating the capacity of digital libraries to respond to emerging threats by studying their preparedness, and seeing if there are current policies or guidelines used by digital libraries in combating the cyber threats. The study outcome suggests developing a strategy for enhancement by looking at three areas, improving the current framework, producing new guidelines or policy suits for digital libraries, and developing a prototype based on AI technology to mitigate the cyber threats.

INTRODUCTION

In today's digital era, rapid technological developments have changed the way we obtain and share information. Digital libraries have become an important and valuable platform because they provide easy access to various information and resources that users need. However, as the digital world continues to develop and the technological revolution becomes increasingly complex, concerns have emerged about the risk of cyber threats and their impact on user privacy and security when accessing digital libraries. From a global perspective, the importance of privacy and security in digital libraries is enormous. United Nations Sustainable Development Goals (SDGs), the information and communication technologies (ICTs) are recognized as playing a crucial role in achieving sustainable development. SDG16 outlines the need to create peaceful and inclusive societies for sustainable development and it should also ensure justice and fairness for all and build effective, accountable, and inclusive institutions at all levels of society. Statistical records show how large and important the role played by digital libraries worldwide. According to a report from the International Federation of Library Associations and Institutions (IFLA), there are more than 320,000 libraries worldwide, and about 66% of these libraries provide services digitally. These libraries are suitable for all groups of users, including students, researchers, professionals, and the general public.

From a Malaysian perspective, it is important to assess the extent of Malaysia's efforts in ensuring the level of privacy and security of digital libraries. Today's digital libraries in Malaysia, under the National Library of Malaysia's supervision, have undergone numerous advancements and transformations in digital technology, ensuring public access to information. The National Library of Malaysia is actively transforming its collections into digital form and offering online access to many resources. Digitization efforts and online services have become more active during and after the world was hit by the COVID-19 pandemic. In fact, in 2021, the 9th Prime Minister of Malaysia launched 'MyDigital,' which outlined the government's efforts and aspirations to transform Malaysia into a high-income country with digital and technological capabilities, as well as becoming a regional leader in the digital economy. The Ministry of Digital Malaysia, administering the MyDigital aspiration, has outlined several objectives to fulfil these aspirations, particularly those pertaining to digital libraries. Although technological advances have made it easier for users to obtain and access information efficiently, there is no denying that there is still a feeling of concern about the level of security and privacy when using the digital platforms provided, whether through public libraries or academic libraries at higher education institutions.

The digitization of libraries provides opportunities to all users from various backgrounds, most of whom want to access information without limits. The National Library of Malaysia (PNM) 2020 statistical report, as shown in Table 1, indicate that approximately 13.6 million users accessed online services, including databases provided by the National Library of Malaysia (PNM), and increased by 17% to 16.1 million in 2021. In the meantime, the National Library of Malaysia (PNM) recorded a total of 367 thousand e-book transactions through the e-Pustaka platform, which then increased by 56% to 572 thousand transactions in the following year, 2021. These numbers clearly show the current trend of users in Malaysia increasingly accessing information sources, especially after the Covid-19 pandemic hit the world.

Table 1: PNM Online User Statistic between 2018 - 2021

	Virtual Users	The Usage of Virtual Services	Materials are Referred Online	e-borrowing Transaction
2018	281,894	10,198,051	1,158,806	115,575
2019	276,388	10,798,688	799,693	167,374
2020	887,747	13,680,177	1,612,744	367,306
2021	1,068,749	16,121,949	9,290,259	572,815

As shown in figure 1, academic libraries contributed to the biggest user populations compared to other types of libraries in Malaysia continue to face similar challenges, including those related to technological disruption. If examination the current state of academic libraries for higher education in Malaysia, which includes public universities, private universities, and institution/ colleges that provide student learning resources, it finds that there are approximately 12.9 million users. This figure is based on the membership registered in 2019 released by the National Library of Malaysia (PNM) as shown in figure 2. In that year, statistics showed that academic libraries in Malaysia had the highest number of users compared to other types of libraries. There were 83 million users recorded, including students, lecturers, the staff of the institution, and visitors who used the library services. The number shows an increase of 29.6% in users who visited the libraries the most compared to the previous year. This figure raises serious concerns regarding the level of security and privacy readiness of the library when users access to their digital platform physically at library premises or online.

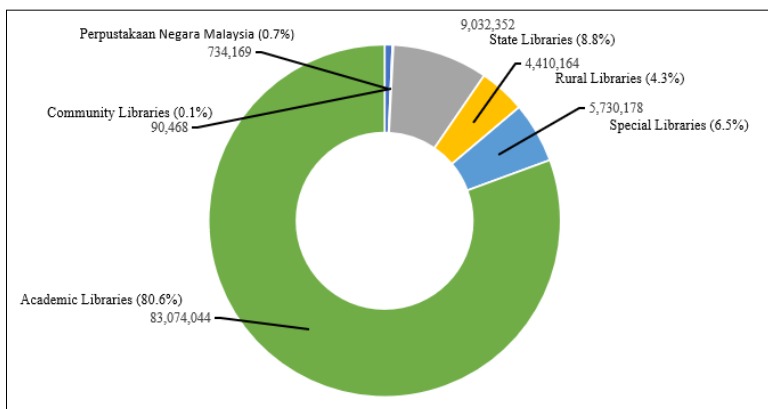


Figure 1: Number of users who visited Malaysian libraries in 2019

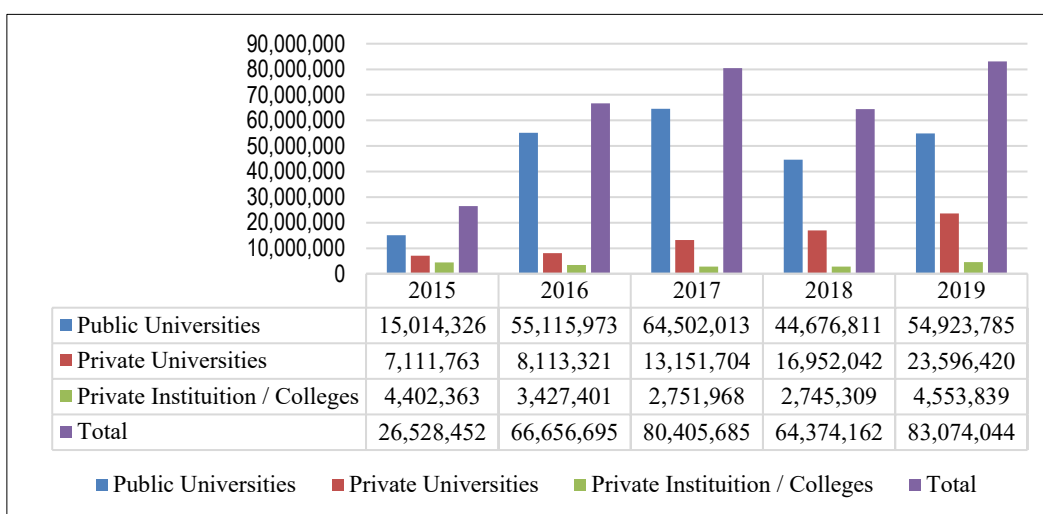


Figure 2: No of users visited the academic libraries in Malaysia between 2015 - 2019

Cyber threats that bring security and privacy concerns are not only affect library users but also educational institutions itself that need to protect sensitive information, especially student information. With the increasing use of digital library systems and online platforms, as reported by Universiti Teknologi Mara (2023) in their library statistics report, there are approximately used 26 online digital platforms that can be accessed via online by their students and staff. Among these platforms are "EzAccess, MyKnowledge Management, UiTM Website, Examination Paper Collection System, Mobile Applications, UiTM IR, OPAC, Open Access Discovery MOOCs, Local Content Hub, eKKM, Open Access Research Repository COMPRES," and many others. Based on this information, it becomes increasingly important for academic libraries to have effective strategies to overcome potential problems relating to security and privacy. It is crucial to investigate and identify strategies that academic libraries can implement to mitigating the negative impacts of these technological disruptions.

Importance of security and privacy in digital libraries

The ongoing discussion among researchers about the importance of privacy and security in digital libraries presents challenges and opportunities that need to be carefully considered and refined for action. Ram et al. (2023), in their study, have emphasized maintaining a balance between IoT technology and user

privacy. They suggest that the libraries can achieve the balance by enhancing the understanding of the specific risks associated with IoT use. For instance, neglecting this balance could lead to a risk of data leakage or unauthorized access to sensitive user information, thereby, it could raise ethical concerns about the use of such technology in libraries.

Furthermore, Biswas et al. (2022) present a positive emphasis on privacy, stating that this needs to be further explored in terms of how it is implemented. While differential privacy has its own theoretical framework for protecting sensitive data, it needs to be reviewed and evaluated for its effectiveness in real-world situations, especially in diverse library systems. Libraries may face technical challenges and resource constraints in implementing this measure, which could create varying levels of user security and privacy protection across institutions. Meanwhile, Sweeney and Davis's (2021) research demonstrates the significance of surveillance technology for library security and privacy. However, some argue that while surveillance can be beneficial in library security situations, it can also make users feel disengaged and under constant observation.

The importance of education and awareness in maintaining privacy in digital libraries cannot be questioned more. The research study by Kim (2022) states that the need to provide privacy education specifically for visually impaired users is essential to improve their online safety. This special attention is part of the wide range of needs that are being accepted for all users to understand online privacy risks and adopt protective measures, as emphasized by Massis (2017). But then, Zimmer (2013) in his research states the important role of developing a comprehensive educational framework and policy needs to address and solving privacy concerns, especially in the context of rapidly evolving Library 2.0 technologies.

The integration of ethical regulations and practices is essential to maintain trust and protect user information in digital library environments. Katalic et al. (2022) emphasise the important role of transparency in the processing and management of personal data, which is the basis for building user trust. The need to disclose this information is linking to the provision of clear privacy notices without protection, as stated by Burkell and Carey (2011), so that users can make informed and providing accurate decisions. The finding is consistent with Al-Suqri and Akomolafe-Fatuyi Sel (2012), who expect them to maintain confidentiality and practice good and prudent ways in managing user information.

In the face of the issue of protecting privacy in untrusted networks, Wu et al. (2021) share the importance of implementing a strong strategy to protect user information. This matter becomes more crucial if there are threats to user security and privacy. Furthermore, Wu et al. (2020) found in their study that the use of encryption techniques with the purpose of protecting the privacy of borrowers in digital libraries is workable.

Security measures and forms of risk in the digital world are diverse. One of them is the use of advertisement libraries in android applications, which can pose serious privacy concerns (Book & Wallach, 2013). In addition to that, Kuzma (2010) highlights that vulnerabilities in digital libraries in Europe demonstrate the importance of strong security measures to protect user data. The relationship between user privacy, trust, and academic freedom also demonstrates the need to proactively protect data to ensure user confidence and trust in the digital services used (Sutlieff & Chelin, 2010). These views emphasize the importance of a comprehensive security strategy to mitigate risks and protect user information across multiple library platforms.

Objectives

- to identify present key issues facing digital libraries in relation to privacy and security
- to evaluate the capacity of digital libraries to respond to emerging threats by studying their preparedness.

- to evaluate the current policies or guidelines used by digital libraries in combating the cyber threats.

LITERATURE REVIEW

The Overview and Key Issues

Technological disruptions increasingly threaten the security and privacy situation in Malaysian academic digital libraries, necessitating a deeper understanding of the issue and its solutions. With the growth of digital libraries, these institutions face a major challenge in maintaining user confidentiality while continuing to provide users with access to information. The use of new technologies, such as cloud computing and library 2.0 applications, has changed the way libraries function. However, this has also raised major concerns about how to protect users' personal data.

One of the main challenges is the collection of personal information when providing digital library services. Wu et al. (2021) stated that digital libraries do store personal information about users, such as their names, interests, and how they use the services. If not properly protected, this information is susceptible to misuse. The increasing reliance of libraries on cloud services makes the problem more complicated, as these platforms have data managed by third parties, which can jeopardize users' privacy (Kritikos & Zimmer, 2017). The ethical implications of this practice are significant, as libraries typically honor their promises to maintain confidentiality and user privacy (Singley, 2020). Therefore, libraries today need to urgently evaluate and improve their privacy policies to make them fit with the current digital usage landscape.

The rapid development in technology, as well as the increasing use of online or cloud storage, big data analytics, and artificial intelligence (AI), has raised new concerns about the level of security and privacy in digital. Anuradha (2019) asserts that the aforementioned technology use has resulted in data sovereignty issues. This is due to the possibility of storing crucial library information and user personal details outside Malaysia, a country that potentially has different security and privacy regulations. Furthermore, Anuradha (2019) asserts that the use of big data analytics and artificial intelligence (AI) tools, which can provide user recommendations and organize content, has raised concerns about the privacy of user data and the potential for unauthorized access or possibly misuse.

In addition, the lack of awareness and training among library staff on privacy issues has made the situation worse. Many librarians do not receive sufficient education on the security and privacy implications of the technologies they use, which can lead to weak protection measures (Zimmer, 2013). This lack of knowledge on the subject highlights the importance of proper education and efforts to help librarians learn the skills needed to overcome digital privacy issues (Avuglah et al., 2020). Conducting comprehensive and periodic privacy audits and assessments that can help to detect problems in the library system and inform better practices (Angell, 2023).

The culture and lack of resources in academic digital libraries make the challenge even more difficult. Why has this happened. Libraries mainly focus on service quality and user satisfaction while they are ignoring privacy aspects. This leads to actions being taken only after problems arise, rather than taking preventive measures early on to guard against security and privacy breaches. As libraries strive to improve their digital services, they need to find ways to engage users while maintaining the security of personal information. Striking this balance is crucial and difficult because if privacy is not protected, it can erode users' trust in the service and subsequently deter users from using the digital resource services.

Anuradha (2019) revealed that the rise of free digital repositories and with more libraries using external platforms to deliver and share content and collaborate has led to new security risks. This includes the possibility of data theft, malware attacks, and unauthorized access to important information. However,

these third-party platform accesses may have adequate security measures in place, such as encryption, access control, and regular security checks. This can improve the security of academic digital libraries (Anuradha, 2019), but there is no guarantee that cyber threats will not occur. Another major problem is the need for a well-organized, complete system to manage cybersecurity risks in academic digital libraries in Malaysia and other countries. Although some institutions have taken basic security measures, the effectiveness and consistency of these measures vary. This clearly shows that there is an urgent need for a more comprehensive approach to addressing cybersecurity risks. New research must be conducted so that these measures can have a better impact on all digital libraries.

Previous Theoretical Framework

Here are the previous theoretical frameworks used by other researchers in study in security and privacy issues.

Table 2: Past theories and frameworks applied to security and privacy issues studies

Theory/Framework	Description	Application
Socio-Technical Systems Theory (Al-Suqri & Akomolafe-Fatuyi, 2012; Rahmani, 2022).	Shows the importance of the relationship between social and technical aspects in an organization or system.	Understands the multi-dimensional nature of security and privacy challenges in academic digital libraries.
Privacy by Design Framework (Zimmer, 2013; Avuglah et al., 2020).	Acts as a guide to actively applying privacy principles in the design and structure of information systems.	Guides the development of secure and privacy-preserving digital library platforms and services.
Information Privacy Management Framework (Angell, 2023; Burkell & Carey, 2011; Lambert et al., 2015).	Give attention to the basics, working methods, and steps required to handle the collection, use, and care of personal information.	Develops comprehensive data management strategies and privacy education programs for academic libraries.
Privacy Literacy Approach (Magi, 2011; Dongseok & Noh, 2014; Witt, 2017).	State how important and powerful it is to provide clear information to library users so they can learn to control their own privacy.	Increases privacy awareness and the adoption of privacy-protection technologies among academic library users.
Networked Privacy Framework (Wu et al., 2021; Wu et al., 2018).	Considers the challenges of protecting privacy in networked and cloud-based environments	Guides the development of best practices for academic libraries implementing cloud-based Library 2.0 services.
Ethical Data Management Principles (Lambert et al., 2015; ALA; IFLA).	Provides guidance on the ethical use and protection of patron data	Informs data management practices and policies adopted by academic libraries when using learning analytics

Proposed Framework

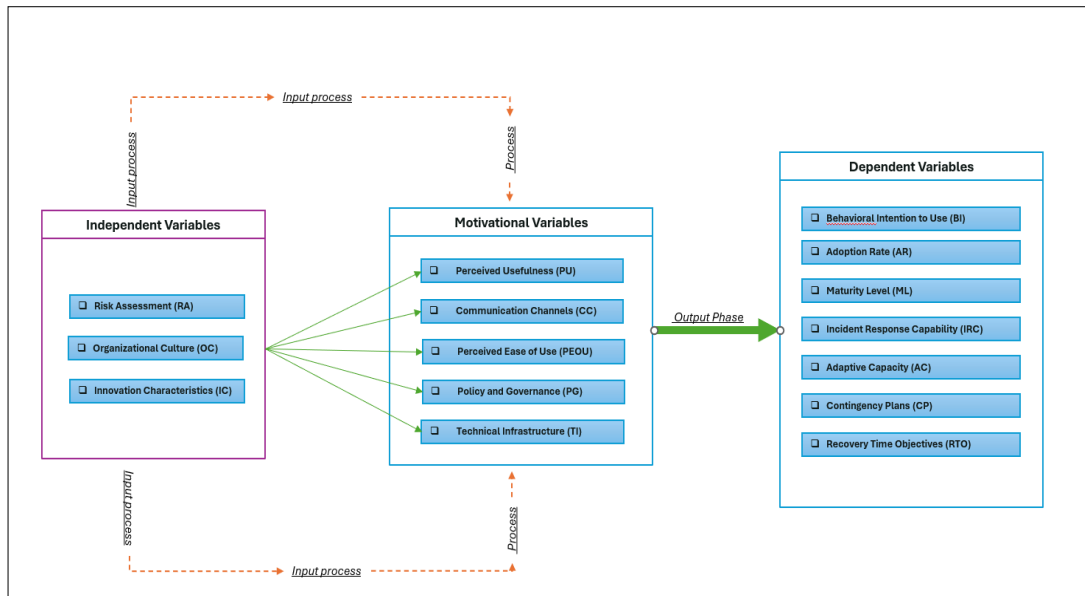


Figure 3: Proposed Framework

METHODOLOGY

Past studies indicate that researchers use a variety of methodologies to explore this topic and to investigate further and not just rely one. It has few types of methodologies applied in security and privacy, but it depends on the research objective of the study. The table below shows the types of methodologies used by the researcher who studied this topic. This study adopts content analysis to investigate and analyse literature for possible explanation and solutions related to this topic.

Table 3: Previous used types of methodologies

Methodology Categories	References
Rational Unified Process (RUP) and System Development Methodologies	Mohd et al. (2016)
Qualitative and Mixed Methods Approaches	Connolly et al. (2017); Wilcox (2016); Chukwuma (2022); Foley & Rooney (2018)
Soft Systems Methodology (SSM)	Mshangi et al. (2018)
Risk Assessment and Evaluation Methodologies	Malamas et al. (2021); Kumar et al. (2020); Kryshtanovych et al. (2021); Kumar et al. (2020); Huang et al. (2016)
Security Requirements Engineering Methodologies	Ansari et al. (2022); Pavlidis et al. (2017); Bulusu et al. (2017)
Integrated Frameworks and Methodologies	Kumar et al. (2020); Mshangi et al. (2017); Gupta (2023); Georgiadou et al. (2020)
Computer-Aided and Ontology-Based Methodologies	Bialas (2016)
Behavioral and Psychological Approaches	Downer & Bhattacharya (2022); Kearney & Kruger (2016)

Drawing from previous research methodologies as shared above table, this topic will employ a mixed methodology, incorporating both quantitative and qualitative elements. A set of questions will be designed based on the framework that will be developed to cover all instruments of individual variables (IV), motivational variables (MV), and dependable variables (DV). For the qualitative section, the number of leaders in academic libraries, especially those who are responsible for the ICT/IT department/unit, will be interviewed. A guidelines question will be droughted and piloted first before we set the official interview session. The study will used NVivo software and thematic analysis as our primary analytical approach for qualitative interviews. But then, MY-PLS will be used to analyse the quantitative data using the descriptive and regression analysis that the data will be gathered through a survey. Strategies for enhancing security and privacy in academic digital libraries.

Improvement measures, best practices, and recommendations for improving security and privacy in academic digital libraries are essential to overcome the problems arising from technological disruptions. Past review studies, provide comprehensive insights, that libraries can use to protect user and library resources while maintaining the quality of their services. One of the main strategies is to use a different approach to security and privacy, which combines technical and managerial solutions. Al-Suqri and Akomolafe-Fatuyi (2012) emphasize that the security and privacy issues of digital libraries are not just technical problems but need to be viewed holistically, encompassing various aspects of library management. This includes establishing clear policies and regulations and measures to regulate and program how data is handled and who can access it and safeguarding user privacy.

Another strategy that could be considered is for digital libraries to develop and implement a comprehensive cybersecurity risk management system. This framework designed should involve several different steps and variables, including:

- Routinely conducting risk assessments to identify and prioritize security and privacy risks according to the recommended framework for an Enhanced Privacy (Dioubate et al., 2022)
- Implementing strong security measures, such as good passwords and encryption, to protect digital data.
- Creating clear rules and procedures for properly managing and storing sensitive information (Dioubate et al., 2022)
- Ensuring that security training and education are provided comprehensively to library staff and users so that they better understand how to best maintain cybersecurity (Ajis et al., 2020)
- Collaborating with industry partners and government agencies to learn about the latest security threats and ways to mitigate them (Ajis et al., 2020)

By using a more complete and robust cybersecurity risk management approach without leaving any room for weakness, academic digital libraries can improve their security levels and better protect digital assets and user data from emerging threats. Using secure technology is one of the key areas that needs to be improved. Gardner (2021) suggests that libraries should consider not using third-party tracking tools such as Google Analytics or at least try to change them to be more privacy-friendly by using features such as IP address copying. In addition, using secure connections (HTTPS) is important to maintain the confidentiality of sensitive information sent between users and library systems, as stated by Thomchick and Nicolas-Rocca (2018). Using such methods and technologies can help reduce the risk of data leaks and unauthorized access.

Previous literature suggests that libraries need to use more effective ways to manage data, especially in relation to learning analytics. A study conducted by Briney (2019) talks about the importance of using ways to obtain consent and ensure that libraries store aggregate data only. This is important to reduce the risk of leakage of users' personal information. This practice pertains to safeguarding users' privacy rights and ensuring data security. For example, cloud-based solutions can provide additional security features, such

as automatic backups, intrusion detection, and monitoring rules, which can help mitigate the risks associated with on-site infrastructure. Meanwhile, the use of big data analytics can provide important insights into user behavior and habits that may lead to security issues, allowing libraries to plan security measures to mitigate risks before they become more serious.

Wu et al. (2021) emphasize the importance of continuously evaluating and changing privacy practices in response to evolving threats and user needs. This collaborative approach can help libraries better understand data protection laws and ensure that their information management practices adhere to ethical standards. Finally, libraries should conduct regular privacy and risk audits to identify weaknesses in their systems and practices. This approach allows libraries to address potential problems before they become serious issues involving user privacy. By routinely scaling through security audits, libraries can improve their resilience to new threats.

REAL CASE STUDIES INCIDENTS

In the last two years, there have been five recorded cyberattacks on libraries. Solano County Public Library, Heriot-Watt University Library (2022), Oxford University, Bodleian Library (2022), London Public Library (2023), and Toronto Public Library (2023) are some of the places affected. Although there are no official reports of cyberattacks on libraries in Malaysia, especially academic libraries, it does not mean the environment of security and privacy systems in libraries is safe and free from any attacks. These five cases proven that this issue happen and it cost the institutions a lot to recovery the system effected. Therefore, conducting this research topic is crucial to inform industry players about the current situation and their preparedness level, should they face any impact. Most libraries handle these issues internally and do not inform others. So, it is important for researcher to continue research and understand the current state of academic digital libraries in Malaysia, as well as how they protect their digital resources. The table below provides a summary of the incidents. With this real scenario, it is evident that cyber-attack still can happen in the libraries.

Table 4: List of incidents involving libraries between 2022 – 2023

Institution	Year	Details	Source
Solano County's public libraries, US	2024	<ul style="list-style-type: none"> Ransomware Attack. Interruption of telephone lines, Computer services, WiFi connectivity in all nine library branches 	The Star. (2024, July 4).
London Public Library, UK	Dec, 2023	<ul style="list-style-type: none"> Affected the library's online catalogue, digital services, public computers, printing facilities, and public Wi-Fi access Libby/OverDrive digital book inaccessible 	CBC News. (2024, December 19).
Toronto Public Library, Canada	Oct, 2023	<ul style="list-style-type: none"> Ransomware attack, possibly data breach Library's website, public computers, and online services were rendered inaccessible 	Bitdefender. (2024, December 18).
Heriot-Watt University	Mac, 2022	<ul style="list-style-type: none"> Massive disruption to its IT infrastructure and services 	Edinburgh Live. (2024, March 22).

Libraries, Scotland		<ul style="list-style-type: none"> • Disruption of vital infrastructure, including as VPNs, financial services, and student data. • Library website & online services inaccessible 	
University of Oxford, Bodleian Libraries	2022	<ul style="list-style-type: none"> • Ransomware Attack by Group of Rhysida • Malware Attack • All electronic resources inaccessible 	Oxford Student. (2024, February 14).

DISCUSSION ON THE IMPLEMENTATION AND POTENTIALS BARRIERS

Derived from the issues raised from the previous studies, there are several important implications. Firstly, comprehensive research needs to be conducted and to address the intricate security and privacy concerns, particularly given the current circumstances. This includes creating well-organized technical and managerial solutions as described by Zimmer (2013) and Singley (2020). But then several researchers, such as Anttila and Jussila (2017), highlight the need for multidisciplinary collaboration among stakeholders, Gligorijevic (2023) then argues similarly against prioritising security over privacy and proposing a balanced approach.

Proposing acceptable practices for cloud-based 2.0 platforms is also important to safeguard user privacy. Education and training for librarians is important too. Modifying curricula to include privacy related lessons and providing ongoing training to librarians will help them meet these challenges (Haska, 2013; Maceli & Burke, 2016; Maceli, 2018). In addition, several researchers in their studies, such as Maceli (2018) and Avuglah et al. (2020), states that it is important to increase the level of understanding of privacy among users through developed programs and campaigns to express about data protection laws and regulations. Effective and proficient data management plays a crucial role in safeguarding user privacy when utilizing learning analytics technologies, while also guaranteeing a transparent and accountable process. Briney (2019) and Robertshaw & Asher (2019) concur with this viewpoint, emphasizing that library space must align with institutional objectives, and that ensuring security and privacy necessitates effective planning, collaboration, and coordination.

CONCLUSION AND RECOMMENDATIONS

This study aims to enhance the security and privacy of academic digital libraries in Malaysia by providing a few approaches. Based on review articles, current practices reveal that academic libraries are aware of these dangers and the need for good security and privacy protection measures. It also illustrated the various approaches being tried to find solutions to these technological disruptions. A combination of solutions including technology, policy development and user education to raise awareness is urgently needed.

The following suggestions are made to enhance the security and privacy. First, develop a comprehensive library security and privacy policy. Every library must have a comprehensive policy that can address the security of digital and physical resources. This policy includes actions to be taken before, during and after an incident occurs. Second, using latest technology. Take advantage of the latest technologies such as artificial intelligent (AI), cloud computing and others. Libraries must be willing to invest in these technologies. Third, ongoing user education and awareness. Training sessions, awareness programs and conducting mock emails to educate users should be ongoing and not seasonal only. Fourth, periodic security audits. Periodic reviews should be conducted to identify current weaknesses and risks and

suggest improvements. The involvement of external auditors such as inviting SIRIM representatives to libraries in Malaysia, is a positive action. Finally, encourage open dialogue. Libraries should establish open communication channels with users regarding security and privacy concerns. This way it will bring the library closer to the users and they will feel more protected.

ACKNOWLEDGEMENT

This paper was presented at the 6th International Conference of Information Science 2025. The authors would like to thank the management and colleagues at Universiti Teknologi MARA, Puncak Perdana Campus of UiTM Selangor Branch for research support and opportunities.

REFERENCES

- Angell, K. (2023). Privacy audit of public access computers and networks at a public college library. *Information Technology and Libraries*, 42(3). <https://doi.org/10.5860/ital.v42i3.16233>
- Ansari, T. M., Pandey, D., & Alenezi, M. (2022). Store: security threat oriented requirements engineering methodology. *Journal of King Saud University - Computer and Information Sciences*, 34(2), 191-203. <https://doi.org/10.1016/j.jksuci.2018.12.005>
- Avuglah, B. K., Owusu-Ansah, C. M., Tachie-Donkor, G., & Yeboah, E. B. (2020). Privacy practices in academic libraries in ghana: insight into three top universities. *IFLA Journal*, 47(2), 196-208. <https://doi.org/10.1177/0340035220966605>
- Al-Suqri, M. N. and Akomolafe-Fatuyi, E. (2012). Security and privacy in digital libraries:. *International Journal of Digital Library Systems*, 3(4), 54-61. <https://doi.org/10.4018/ijdls.2012100103>
- Anttila, J., & Jussila, K. (2017, December). Challenges for the comprehensive and integrated information security management. In *2017 13th International Conference on Computational Intelligence and Security (CIS)* (pp. 586-589). IEEE.
- Bialas, A. (2016). Computer-aided sensor development focused on security issues. *Sensors*, 16(6), 759. <https://doi.org/10.3390/s16060759>
- Bitdefender. (2024, December 18). Hackers attack Toronto Public Library. *Hot for Security*. <https://www.bitdefender.com/en-us/blog/hotforsecurity/hackers-attack-toronto-public-library>
- Briney, K. (2019). Data management practices in academic library learning analytics: a critical review. *Journal of Librarianship and Scholarly Communication*, 7(1). <https://doi.org/10.7710/2162-3309.2268>
- Bulusu, S. T., Laborde, R., Wazan, A. S., Barrère, F., & Benzekri, A. (2017). Towards the weaving of the characteristics of good security requirements. *Lecture Notes in Computer Science*, 60-74. https://doi.org/10.1007/978-3-319-54876-0_5

- CBC News. (2024, December 19). London Public Library cyber attack: System restoration services. *CBC News*. <https://www.cbc.ca/news/canada/london/london-public-library-cyber-attack-system-ressoration-services-1.7065676>
- Connolly, L. Y., Lang, M., Gathegi, J. N., & Tygar, D. (2017). Organisational culture, procedural countermeasures, and employee security behaviour. *Information & Computer Security*, 25(2), 118-136. <https://doi.org/10.1108/ics-03-2017-0013>
- Downer, K. and Bhattacharya, M. (2022). Byod security: a study of human dimensions. *Informatics*, 9(1), 16. <https://doi.org/10.3390/informatics9010016>
- Edinburgh Live. (2024, March 22). Edinburgh Heriot-Watt University admits cyber attack. *Edinburgh Live*. <https://www.edinburghlive.co.uk/news/edinburgh-news/edinburgh-heriot-watt-university-admits-23490612>
- Foley, S. N. and Rooney, V. M. (2018). A grounded theory approach to security policy elicitation. *Information & Computer Security*, 26(4), 454-471. <https://doi.org/10.1108/ics-12-2017-0086>
- Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, 62(3), 452-462. <https://doi.org/10.1080/08874417.2020.1845583>
- Gligorijevic, J. (2023). Tort-Based Protections for Data Privacy. *Data and Private Law*.
- Haska, E. (2013). Development of higher education in albania: the case of the public university libraries in efforts to build digital and electronic services for the academic community. *Academicus International Scientific Journal*, 7, 137-148. <https://doi.org/10.7336/academicus.2013.07.13>
- Huang, S., Han, Z., Yang, B., & Ren, N. (2016). Factor identification and computation in the assessment of information security risks for digital libraries. *Journal of Librarianship and Information Science*, 51(1), 78-94. <https://doi.org/10.1177/0961000616668572>
- Kritikos, K. C. and Zimmer, M. (2017). Privacy policies and practices with cloud-based services in public libraries: an exploratory case of bibliocommons. *Journal of Intellectual Freedom & Privacy*, 2(1), 23-37. <https://doi.org/10.5860/jifp.v2i1.6252>
- Kumar, R., Pandey, A., Baz, A., Alhakami, H., Alhakami, W., Agrawal, A., & Khan, R. A. (2020). Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security. *Symmetry*, 12(4), 664. <https://doi.org/10.3390/sym12040664>
- Kryshantovych, S., Gutsulyak, V., Huzii, I., Helzhynska, T., & Shepichak, V. (2021). Modeling the process of risk management response to the negative impact of risks as the basis for ensuring economic security. *Business, Management and Economics Engineering*, 19(02), 289-302. <https://doi.org/10.3846/bmee.2021.14798>
- Maceli, M. and Burke, J. J. (2016). Technology skills in the workplace: information professionals' current use and future aspirations. *Information Technology and Libraries*, 35(4), 35-62. <https://doi.org/10.6017/ital.v35i4.9540>

- Maceli, M. (2018). Encouraging patron adoption of privacy-protection technologies. *IFLA Journal*, 44(3), 195-202. <https://doi.org/10.1177/0340035218773786>
- Mohd, H., Robie, M. A. M., Baharom, F., Darus, N. M., Saip, M. A., & Yasin, A. (2016). Adapting rational unified process (rup) approach in designing a secure e-tendering model. *AIP Conference Proceedings*. <https://doi.org/10.1063/1.4960906>
- Mshangi, M., Nfuka, E. N., & Sanga, C. (2018). Human sensor web crowd sourcing security incidents management in tanzania context. *Journal of Information Security*, 09(03), 191-208. <https://doi.org/10.4236/jis.2018.93014>
- Oxford Student. (2024, February 14). Bodleian services still impacted by British Library cyber attack. *Oxford Student*. <https://www.oxfordstudent.com/2024/02/14/bodleian-services-still-impacted-by-british-library-cyber-attack/>
- Pavlidis, M., Mouratidis, H., Panaousis, E., & Argyropoulos, N. G. (2017). Selecting security mechanisms in secure tropos. *Trust, Privacy and Security in Digital Business*, 99-114. https://doi.org/10.1007/978-3-319-64483-7_7
- 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 Technology*, 8(1), 14-19. <https://doi.org/10.18231/j.ijlsit.2023.003>
- Robertshaw, M. B. and Asher, A. (2019). Unethical numbers? a meta-analysis of library learning analytics studies. *Library Trends*, 68(1), 76-101. <https://doi.org/10.1353/lib.2019.0031>
- Shashi Kant Gupta, A. S. D. (2023). Analysis and development of security framework for iot device. *Tuijin Jishu/Journal of Propulsion Technology*, 44(4), 995-1008. <https://doi.org/10.52783/tjpt.v44.i4.955>
- Singley, E. (2020). A holistic approach to user privacy in academic libraries. *The Journal of Academic Librarianship*, 46(3), 102151. <https://doi.org/10.1016/j.acalib.2020.102151>
- The Star. (2024, July 4). Why would you hack a library? US county still struggling months after cyberattack. *The Star*. <https://www.thestar.com.my/tech/tech-news/2024/07/04/039why-would-you-hack-a-library039-us-county-still-struggling-months-after-cyberattack>
- Wilcox, L. (2016). Securing methods, practicing critique: a review of methods and critical security studies. *International Studies Review*, viw026. <https://doi.org/10.1093/isr/viw026>
- Wu, Z., Shen, S., Lu, C., Li, H., & Su, X. (2020). How to protect reader lending privacy under a cloud environment: a technical method. *Library Hi Tech*, 40(6), 1746-1765. <https://doi.org/10.1108/lht-07-2020-0178>
- Wu, Z., Shen, S., Li, H., Zhou, H., & Zou, D. (2021). A comprehensive study to the protection of digital library readers' privacy under an untrusted network environment. *Library Hi Tech*, 40(6), 1930-1953. <https://doi.org/10.1108/lht-07-2021-0239>
- Wilcox, L. (2016). Securing methods, practicing critique: a review of methods and critical security studies. *International Studies Review*, viw026. <https://doi.org/10.1093/isr/viw026>

- Willis, S. and O'Reilly, F. (2018). Enhancing visibility of vendor accessibility documentation. *Information Technology and Libraries*, 37(3), 12-28. <https://doi.org/10.6017/ital.v37i3.10240>
- Zimmer, M. (2013). Assessing the treatment of patron privacy in library 2.0 literature. *Information Technology and Libraries*, 32(2), 29-41. <https://doi.org/10.6017/ital.v32i2.3420>