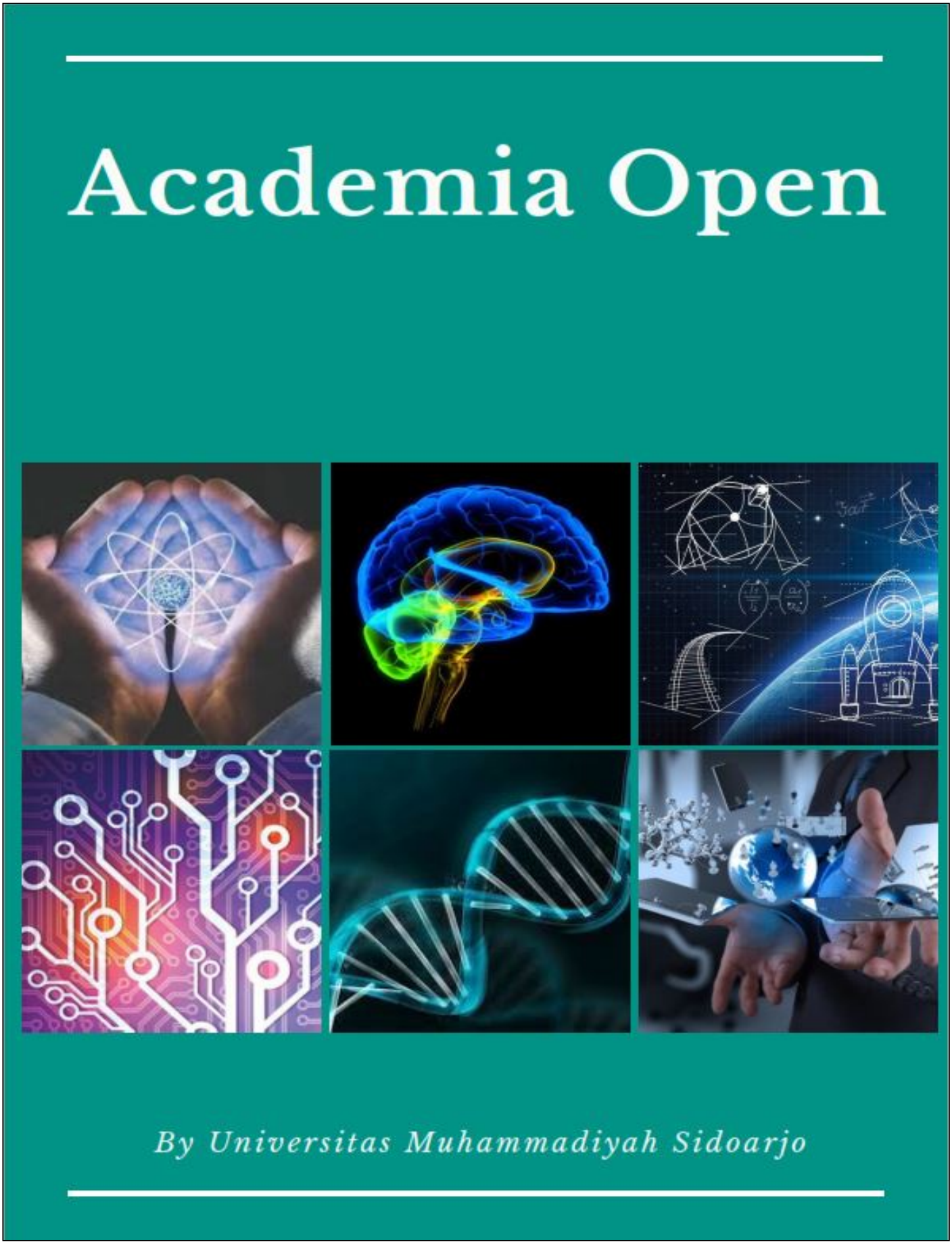
Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.11495 . Article type: (Language and Literature)

Table Of Content

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.11495 . Article type: (Language and Literature)



ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.11495 . Article type: (Language and Literature)

Originality Statement

The author[s] declare that this article is their own work and to the best of their knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the published of any other published materials, except where due acknowledgement is made in the article. Any contribution made to the research by others, with whom author[s] have work, is explicitly acknowledged in the article.

Conflict of Interest Statement

The author[s] declare that this article was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Copyright Statement

Copyright © Author(s). This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at http://creativecommons.org/licences/by/4.0/legalcode

Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.11495 . Article type: (Language and Literature)

EDITORIAL TEAM

Editor in Chief

Mochammad Tanzil Multazam, Universitas Muhammadiyah Sidoarjo, Indonesia

Managing Editor

Bobur Sobirov, Samarkand Institute of Economics and Service, Uzbekistan

Editors

Fika Megawati, Universitas Muhammadiyah Sidoarjo, Indonesia

Mahardika Darmawan Kusuma Wardana, Universitas Muhammadiyah Sidoarjo, Indonesia

Wiwit Wahyu Wijayanti, Universitas Muhammadiyah Sidoarjo, Indonesia

Farkhod Abdurakhmonov, Silk Road International Tourism University, Uzbekistan

Dr. Hindarto, Universitas Muhammadiyah Sidoarjo, Indonesia

Evi Rinata, Universitas Muhammadiyah Sidoarjo, Indonesia

M Faisal Amir, Universitas Muhammadiyah Sidoarjo, Indonesia

Dr. Hana Catur Wahyuni, Universitas Muhammadiyah Sidoarjo, Indonesia

Complete list of editorial team (link)

Complete list of indexing services for this journal (link)

How to submit to this journal (link)

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.11495 . Article type: (Language and Literature)

Article information

Check this article update (crossmark)

Check this article impact (*)

Save this article to Mendeley

(*) Time for indexing process is various, depends on indexing database platform

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.11495 . Article type: (Language and Literature)

The Urgency of Cyber Resilience in the Governance of Digital Libraries in Indonesia

Dwi Fajar Saputra, dwifajar@upnvj.ac.id, (1)

Departement of Information Science, Faculty of Social and Political Sciences, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia.
Doctoral Program in Information Studies, Faculty of Cultural Sciences, Universitas Indonesia, Indonesia

(1) Corresponding author

Abstract

General Background: The rapid digital transformation of libraries in Indonesia has expanded access to knowledge but also exposed institutions to escalating cybersecurity threats. **Specific Background:** Increasing ransomware attacks, data breaches, and phishing incidents targeting educational institutions underscore the fragility of current library information systems. **Knowledge Gap:** Conventional cybersecurity measures often fail to ensure service continuity during cyber incidents, leaving a gap in sustainable protection strategies for digital library infrastructure. **Aims:** This study examines national data from Indonesia's Badan Siber dan Sandi Negara (BSSN), evaluates TLS/SSL adoption in institutional repositories, and analyzes the British Library ransomware incident to identify systemic vulnerabilities. **Results:** Findings reveal insufficient encryption practices, fragmented incident response, and limited cross-institutional coordination. **Novelty:** The research advances a holistic cyber resilience framework—integrating flexibility, redundancy, diversity, and connectivity—and positions hybrid cloud infrastructure as a foundational enabler, complemented by international collaboration for knowledge sharing and collective defense. **Implications:** The study emphasizes the strategic role of the National Library of Indonesia in orchestrating global partnerships and aligning domestic cybersecurity policies with international standards, fostering sustainable governance and resilient digital library ecosystems.

Highlights:

- Highlights vulnerabilities in Indonesia's digital library infrastructure.
- Proposes a holistic cyber resilience framework with hybrid cloud adoption.
- Emphasizes global collaboration led by the National Library of Indonesia.

Keywords: Cyber Resilience, Digital Libraries, Cybersecurity, Hybrid Cloud

Published date: 2025-08-12 00:00:00

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

Academia Open
Vol 10 No 2 (2025): December
DOI: 10.21070/acopen.10.2025.11495 . Article type: (Language and Literature)

Introduction

Digital transformation in Indonesian libraries has undergone significant development in the past decade. The initiative of the National Library of the Republic of Indonesia to promote web-based electronic systems in the management and access of digital collections has become one of the main milestones in the modernization of library services [1]. By 2025, the number of libraries in Indonesia increased by 35% compared to 2018, reaching a total of 222,179 units [2]. However, this acceleration of digitalization presents complex cybersecurity challenges, which have not yet been fully accommodated systemically within the national policy framework.

The increased reliance on digital platforms makes library systems vulnerable to various forms of cyberattacks, such as ransomware, phishing, and systemic data breaches. Data from the Badan Siber dan Sandi Negara (BSSN) reveals that 31% of government information technology infrastructure, including libraries, have critical vulnerabilities, while 72% of cyber incidents in 2023 targeted educational and knowledge institutions [3]. These vulnerabilities are exacerbated by a deficit of human resources skilled in cybersecurity, overlapping authorities among institutions, and dependence on foreign technology especially open-source systems widely used in regional libraries without adequate maintenance and security reinforcement support [9].

Globally, the development of digital libraries continues to be shaped by advancements in digitization, the development of metadata standards, user-centered interface design, and the integration of artificial intelligence and social media technologies [11]. However, cybersecurity remains one of the structural weaknesses that have not yet been fully addressed, particularly in developing regions. The case study of the ransomware attack on the British Library in 2023 highlights the fatal consequences of weak digital infrastructure relying on legacy systems, with losses amounting to £6–7 million, service disruptions lasting for months, and a leak of 600 GB of sensitive data [4].

This development underscores the need for a paradigm shift in the management of digital libraries. The traditional approach that focuses solely on preventing attacks (cybersecurity) has proven increasingly inadequate in facing the dynamics of modern cyber threats that are becoming more complex. Therefore, the approach of cyber resilience has developed, which emphasizes not only on prevention efforts but also on the institution's ability to withstand, respond to, and recover from cyber incidents effectively [5]. For the Indonesian digital library ecosystem, the implementation of cyber resilience is not merely a technical necessity, but rather a strategic imperative to ensure service continuity, protect national knowledge assets, and maintain public trust amidst a globally interconnected information ecosystem.

Method

This research uses a descriptive qualitative approach based on conceptual studies and case studies. The review was conducted systematically by collecting and analyzing secondary data from various relevant sources to build an argument regarding the urgency of cyber resilience in digital library management. Data collection was carried out through literature review, examination of official documents, and analysis of actual incidents relevant to the context of cybersecurity in library institutions.

The primary data source comes from the official report of the Badan Siber dan Sandi Negara (BSSN), which provides an overview of the cyber security threat landscape in Indonesia, including the education and knowledge sectors that have become the dominant targets of cyber attacks in recent years [3]. In addition, the research also utilizes empirical study results by Ali [6], who examined the implementation of TLS/SSL network security protocols on institutional repositories at several public and private universities in Indonesia. This study provides empirical data regarding the actual security conditions of the national digital library infrastructure.

As an analytical reinforcement, this research presents a case study of the ransomware attack that occurred on the British Library in 2023, which substantially illustrates the impact of vulnerabilities in digital infrastructure based on poorly managed legacy systems [7]. This incident is used as a real illustration of the

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

risks that could also potentially threaten the digital library ecosystem in Indonesia if there are no systemic improvements in cybersecurity governance.

On the conceptual side, this research adopts the theoretical foundation from international studies related to the evolution of cyber resilience. The conceptual framework is derived from the study conducted by Akinsanya et al. [1], which traces the development of the cyber resilience framework in network security, as well as the historical-conceptual discussion examined by Tzavara and Vassiliadis [10]. Furthermore, the literature on the global development of digital libraries, the design of hybrid cloud-based information systems, and the principles of resiliency in digital library services is drawn from the works of Wang and Xie [11], Yap and Manabat [12], DataCore Software [5], and the PCI Security Standards Council [6].

All the collected data were analyzed descriptively-critically, integrating empirical findings, conceptual frameworks, and real case illustrations to build a problem mapping and strategic recommendations for strengthening cyber resilience in the governance of digital libraries in Indonesia. The focus of the analysis is directed towards identifying vulnerability points, strengthening incident response capacities, and modeling adaptive multi-level collaboration within the national and global cybersecurity ecosystem.

Results and Discussion

A. Results

An in-depth study of the cybersecurity conditions in the management of digital libraries in Indonesia reveals several structural vulnerabilities that could potentially hinder the sustainability of the ongoing digital transformation. Although the number of libraries has significantly increased in line with national digitalisation policies [8], the readiness of security infrastructure supporting the sustainability of digital systems still shows a disparity between service expansion and the strengthening of supporting systems.

One of the important findings comes from national data published by the Badan Siber dan Sandi Negara (BSSN). In the Indonesian cyber security landscape of 2024, it was recorded that 31% of the total government information technology infrastructure, including library infrastructure, has critical vulnerabilities that could be exploited by malicious cyber actors [3]. Moreover, BSSN data shows that 72% of the total cyber incidents recorded throughout 2023 specifically targeted educational and knowledge institutions as the main attack sectors [3]. This fact shows that the ecosystem of educational institutions, including libraries, has become a primary target in the escalation of cyber attacks, as the dependence on information technology in knowledge management activities increases.

The empirical research results by Ali [2], which specifically examine the security aspects of network protocols in institutional repositories within Indonesian higher education environments, further reinforce the picture of vulnerability in digital library systems. By conducting tests on the implementation of TLS/SSL on several state and private university repositories, this research reveals that most institutions do not have adequate security protocol implementations. The majority of the tested systems showed weaknesses in TLS/SSL configuration that allowed for man-in-the-middle attacks, session hijacking, and potential leakage of sensitive data. These findings indicate a weak implementation of basic security principles at the network level, even though the repository manages various types of strategic knowledge assets, including research results, academic documents, and personal data of the academic community.

In addition to domestic conditions, this study also examines global case studies that provide relevant reflections on the magnitude of the impact that may occur when cybersecurity vulnerabilities are not anticipated systematically. The ransomware attack on the British Library in 2023 became one of the key references in this analysis. The attack not only caused service disruptions for months but also resulted in financial losses of £6–7 million and the leakage of 600 GB of data classified as sensitive [4]. The official report released after the incident revealed three main factors that exacerbated the impact of the attack. First, the continued use of legacy systems that have operated without security updates for years, particularly on remote access terminal systems without multi-factor authentication implementation. Second, the absence of a robust cloud-based disaster recovery system, causing the service restoration process to be slow after the main server was sabotaged by hackers. Third, the fragmentation of security management systems between internal divisions and external vendors leads to minimal coordination during emergency incident handling

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

[4]. The incident at the British Library illustrates how a combination of technical factors and governance weaknesses can lead to a highly significant operational crisis for knowledge management institutions.

From the review of the conceptual literature, there appears to be a paradigm shift in information security management practices towards a more comprehensive cyber resilience approach. Akinsanya et al. [9] explain that cyber resilience does not merely rely on efforts to prevent attacks through strengthening defence systems (defense-in-depth), but also on building the organization's capacity to withstand, respond adaptively, and quickly recover systems post-cyber incident. This paradigm has evolved with the awareness that the complexity and dynamics of modern cyber attacks are difficult to address with traditional security models based purely on prevention. The COVID-19 pandemic even accelerated the adoption of this concept because it demonstrated how the resilience of digital systems became the key to maintaining the continuity of public services amid global uncertainty [10].

In the context of digital libraries, the concept of cyber resilience is translated into four main pillars, as outlined by Yap and Manabat [12], namely flexibility, redundancy, diversity, and connectivity. Flexibility reflects the system's ability to quickly adapt to changing conditions or unexpected threats. Redundancy refers to the existence of layered system and data backups, so that the failure of the main system does not automatically halt service operations. Diversity means the presence of a variety of resources, platforms, and service distribution channels that allow for alternative services when the main channels are disrupted. Meanwhile, connectivity emphasises the importance of an integrated system capable of coordinating across components when incidents escalate, in order to reduce response time and minimise the impact of losses.

This study also emphasises that strengthening hybrid cloud-based infrastructure has the potential to become a key foundation in efforts to enhance the cybersecurity resilience of digital libraries. Cloud offers data scalability flexibility, automatic backup systems, and accelerated post-disruption recovery processes [5]. Moreover, amidst the internal resource limitations often faced by libraries in the regions, cloud adoption enables partnership schemes between institutions, allowing technical capacities to be collectively strengthened. Conceptually, the implementation of hybrid cloud categorises digital library systems as critical systems, which are systems that have a strategic function in maintaining the sustainability of information access and national data resilience [6].

B. Discussion

The findings previously presented indicate that the digital library ecosystem in Indonesia remains vulnerable to increasingly complex forms of cyber threats. In this context, the urgency of adopting a cyber resilience approach becomes very relevant, considering the limitations of conventional cybersecurity approaches that tend to focus solely on preventive measures. Digital libraries, as part of the national knowledge infrastructure, require strategies that not only protect digital assets from potential attacks but also ensure the continuity of information services amid the uncertainties of the global digital environment.

The cyber resilience approach provides a more adaptive conceptual framework to the dynamics of cyber attacks. Unlike cyber security, which is reactive and preventive towards attacks, cyber resilience encompasses broader aspects, such as the ability to withstand, respond in a timely manner, and recover systems quickly after an incident [1], [10], [14]. This approach emphasises that attacks cannot be completely avoided, but their impact can be controlled and minimised through robust systems designed holistically.

One of the important implications of this paradigm shift is the need for changes in the governance and strategic planning of digital library systems. As illustrated in the British Library incident, the failure to identify and follow up on risks that have been detected early can result in significant systemic losses [4]. British Library has received warnings about its system vulnerabilities since 2020, but the mitigation recommendations were not fully implemented. This highlights the importance of cybersecurity governance that is not only technical but also integrated into institutional culture and decision-making. In the context of Indonesia, research findings by Ali [11] indicate that libraries in higher education institutions have not yet fully adopted basic network security best practices such as TLS/SSL protocols. This fact indicates that the vulnerabilities of digital library systems are not only at the application level but also at the most fundamental layer of the digital infrastructure used. This is where the role of the cyber resilience approach becomes

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

crucial, as it encompasses cross-level strategies ranging from technology architecture design, human resource capacity development, to strengthening external collaboration.

The four main characteristics of cyber resilience proposed by Yap and Manabat [12] — flexibility, redundancy, diversity, and connectivity — need to be embedded in the planning of Indonesia's digital library system. The concepts of diversity and interoperability are also highly relevant in the context of digital libraries, as they directly intersect with metadata management and information structures capable of supporting recovery scenarios and multi-system integration [13]. With the diversity of sources and systems, libraries have alternative pathways to reach users and ensure the continuity of information distribution when the main systems are disrupted. The implementation of hybrid cloud architecture has become one of the technological solutions that aligns with the spirit of cyber resilience. Cloud infrastructure offers advantages in terms of scalability, high availability, and integration with automatic backup systems that can accelerate data recovery after disruptions [14]. For digital libraries spread across various regions of Indonesia with resource disparities, cloud-based solutions enable system decentralisation without compromising security standards. Even with a consortium approach, small libraries can utilise a jointly managed platform that is cost-efficient yet remains secure.

Furthermore, discussions on cyber resilience cannot be separated from issues of policy governance and the supporting legal framework. In the global context, differences in privacy and information security regulations pose a unique challenge in building cross-border collaboration. For example, the GDPR regulation in the European Union strictly governs the management of users' personal data, while in other countries, similar regulations may not be in place or may not be as stringent. This condition implies limitations on cross-border information sharing between libraries, especially if there is no mutually agreed framework [15]. The role of the National Library of Indonesia becomes crucial in this context. As the national library policy institution, Perpusnas has the authority and legitimacy to formulate a national strategic framework that integrates cyber resilience principles into digital library management standards. This includes the development of cybersecurity guidelines based on critical systems, ongoing technical training for library managers, and the facilitation of cloud-based collaborative platforms that can be used nationally. In the formulation of this strategy, it is also important to consider an approach based on measurable and auditable indicators as developed in recent research on cyber resilience metrics for the public sector [16].

In addition to national coordination, solidarity among institutions is also an important element in building collective cyber resilience. Large library institutions such as the British Library, the National Library of Australia, or the National Diet Library in Japan have resource capacities that can be utilised to support small-scale libraries through consortium mechanisms or technology transfer. On the other hand, conceptual approaches such as those offered by Furner [15] also expand the understanding that digital library data is not just a technical entity, but also a form of evidence with social and cognitive value. Therefore, protecting this data through a resilient system is essentially also a protection of the community's right to information and the nation's collective memory.

Conclusion

The digital transformation of libraries in Indonesia, although showing significant quantitative development, still faces crucial challenges in terms of cybersecurity infrastructure readiness. This study emphasises that conventional preventive security approaches are unable to respond to the complexities of contemporary digital threats, especially in institutions that play a strategic role in knowledge management, such as libraries. Therefore, the adoption of the cyber resilience paradigm has become an urgent necessity in order to ensure the sustainability of inclusive, safe, and adaptive information services in response to changing situations.

The study results show that the vulnerabilities of Indonesia's digital library system are reflected in the weak implementation of basic security protocols, the suboptimal disaster recovery system, and the low coordination in incident management. The British Library case study provides a real reflection of the systemic impact that can occur when security approaches are not thoroughly integrated into institutional governance. In the national context, data from BSSN and local research such as that conducted by Ali, show

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

that real threats are not only global in nature but have also taken root within the local digital library ecosystem.

Through literature analysis, the cyber resilience approach is understood as a strategy that emphasises the ability to withstand, respond to, and recover from cyber incidents. The implementation of four main characteristics — flexibility, redundancy, diversity, and connectivity — becomes the foundation of a system's resilience capable of addressing contemporary challenges. Hybrid cloud-based technology infrastructure has been identified as a key technical solution that enables scalability, reliability, and efficiency in service recovery post-attack. Moreover, global collaboration among library institutions, whether in the form of information exchange, best practices, or the development of shared security platforms, is a strategic element that must be strengthened moving forward.

The National Library of Indonesia, as the main authority in the field of national libraries, plays a central role in formulating the cyber resilience policy framework, developing technical guidelines, and building collaborative networks with national and international partners. These efforts need to be accompanied by strengthening human resource capacity, updating privacy and data security policies, and long-term investment in secure and resilient digital infrastructure.

Thus, this study recommends that digital libraries in Indonesia not only pursue the acceleration of technological transformation but also instill a paradigm of digital resilience systematically. A planned, data-driven, and collaborative cyber resilience approach will be key in creating library services that are not only technically modern but also safe, inclusive, and sustainable in the long term.

Acknowledgement

This study was conducted independently, and no specific acknowledgements are applicable.

References

[1] M. O. Akinsanya, C. C. Ekechi, and C. D. Okeke, “The Evolution of Cyber Resilience Frameworks in Network Security: A Conceptual Analysis,” Computer Science & IT Research Journal, vol. 5, no. 4, pp. 926–949, Apr. 2024, doi: 10.51594/csitrj.v5i4.1081.

[2] I. Ali, “Examining Cyber Security Implementation Through TLS/SSL on Academic Institutional Repository in Indonesia,” Berkala Ilmu Perpustakaan dan Informasi, vol. 17, no. 2, pp. 238–249, 2021, doi: 10.22146/bip.v17i2.2082.

[3] Badan Siber dan Sandi Negara (BSSN), “Lanskap Keamanan Siber Indonesia 2024,” IlmuBersama.com, Mar. 30, 2025. [Online]. Available: https://ilmubersama.com/2025/03/30/lanskap-keamanan-siber-indonesia-2024-bssn/. [Accessed: Apr. 3, 2025].

[4] The British Library, “Cyber Incident Update: Information & FAQs,” British Library. [Online]. Available: https://www.bl.uk/cyber-incident. [Accessed: Apr. 3, 2025].

[5] DataCore Software, “Cybersecurity vs. Cyber Resilience: What’s the Difference,” Feb. 24, 2025. [Online]. Available: https://www.datacore.com/glossary/cybersecurity-vs-cyber-resilience/. [Accessed: Apr. 3, 2025].

[6] PCI Security Standards Council, “Critical Systems,” Jul. 1, 2024. [Online]. Available: https://www.pcisecuritystandards.org/glossary/critical-systems-critical-technologies/. [Accessed: Apr. 3, 2025].

[7] Perpustakaan Nasional Republik Indonesia, “Perpusnas Dorong Transformasi Digital dan Literasi Baca di Indonesia.” [Online]. Available: https://www.perpusnas.go.id/berita/perpusnas-dorong-transformasi-digital-dan-literasi-baca-di-indonesia. [Accessed: Apr. 3, 2025].

[8] Perpustakaan Nasional Republik Indonesia, “Total Perpustakaan di Indonesia Berbasis Wilayah.” [Online]. Available: https://data.perpusnas.go.id/. [Accessed: Apr. 3, 2025, 11:35 WIB].

[9] A. I. Saleh and M. D. Winata, “Indonesia’s Cyber Security Strategy: Problems and Challenges,” in Advances in Social Science, Education and Humanities Research, vol. ..., 2023, pp. 1675–1696, doi: 10.2991/978-2-38476-152-4_169.

Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).

[10] V. Tzavara and S. Vassiliadis, "Tracing the Evolution of Cyber Resilience: A Historical and Conceptual Review," International Journal of Information Security, vol. 23, pp. 1695–1719, 2024, doi: 10.1007/s10207-023-00811-x.
[11] S. Wang and I. Xie, "Digital Libraries: Key Concepts in Their Evolution," in Elsevier e-Books, 2024, pp. 162–174, doi: 10.1016/B978-0-323-95689-5.00148-6.
[12] J. Yap and A. Manabat, "Managing a Sustainable Work-From-Home Scheme: Library Resiliency in Times of Pandemic," International Journal of Librarianship, vol. 5, no. 2, Art. no. 2, 2020, doi: 10.23974/ijol.2020.vol5.2.168.
[13] M. L. Zeng and J. Qin, Metadata, 2nd ed., Chicago, IL, USA: ALA Neal-Schuman, 2022.
[14] L. Reddy and D. K. Rao, "Resilience-Centric Strategies for Cyberinfrastructure in Academic Institutions," International Journal of Information Management, vol. 61, p. 102412, 2021, doi: 10.1016/j.ijinfomgt.2021.102412.
[15] M. Furner, "Conceptual Analysis: A Method for Understanding Information as Evidence, and Evidence as Information," Archival Science, vol. 20, pp. 195–224, 2020, doi: 10.1007/s10502-019-09325-z.
[16] G. M. Mazarakis and P. Antoniou, "Cyber Resilience Metrics for Public Sector Institutions: A Practical Framework," Government Information Quarterly, vol. 40, no. 2, p. 101811, 2023, doi: 10.1016/j.giq.2023.101811.

ISSN 2714-7444 (online), https://acopen.umsida.ac.id, published by Universitas Muhammadiyah Sidoarjo
Copyright © Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY).