ISSN: 3032-3908
Holistik Analisis Nexus

DATA PRIVACY AND SECURITY PROTECTION STRATEGIES IN LIBRARY ELECTRONIC RESOURCES MANAGEMENT

Pratama Dahlian Persadha[1], Loso Judijanto[2], Melly Susanti [3], Heru Kreshna Reza[4]
Sekolah Tinggi Inteljen Negara, Jakarta, Indonesia[1,] IPOSS, Jakarta, Indonesia[2,] Universitas Muhammadiyah Bengkulu, Indonesia[3] , Universitas Esa Unggul, Jakarta, Indonesia[4]
pratama@cissrec.org

Informasi Artikel
Vol: 1 No: 7 Juli 2024
Halaman : 115-122

Keywords:
Data Privacy
Electronic Resources
Cybersecurity
Confidentiality
Ethical Considerations

Abstract
Security is a crucial aspect in the digital age, especially in the management and protection of information. As the volume of information processed increases, the need to organize knowledge and provide adequate security becomes more pressing. This research emphasizes the importance of cybersecurity in the context of digital libraries, which must comply with certain technological and regulatory standards to protect user data and guarantee privacy when accessing electronic resources. Libraries face various challenges in protecting personal data on their electronic resources. This research addresses topics such as user privacy, data encryption, access management, and compliance with privacy laws. By addressing these issues comprehensively, libraries can ensure the protection of user privacy while optimizing the benefits of digital resources in today's information environment. The October 2023 cyberattack by a hacker group known as Rhysida on the British Library's internet information system emphasizes the importance of cybersecurity and data privacy for digital libraries. This research aims to provide insights and solutions to address these challenges, ensuring digital libraries can operate securely and efficiently.

Abstrak
Keamanan merupakan aspek penting dalam era digital, terutama dalam pengelolaan dan perlindungan informasi. Seiring dengan meningkatnya volume informasi yang diproses, kebutuhan untuk mengorganisir pengetahuan dan menyediakan keamanan yang memadai menjadi semakin mendesak. Penelitian ini menekankan pentingnya keamanan siber dalam konteks perpustakaan digital, yang harus memenuhi standar teknologi dan peraturan tertentu untuk melindungi data pengguna dan menjamin privasi saat mengakses sumber daya elektronik. Perpustakaan menghadapi berbagai tantangan dalam melindungi data pribadi pada sumber daya elektronik mereka. Penelitian ini membahas topik-topik seperti privasi pengguna, enkripsi data, manajemen akses, dan kepatuhan terhadap undang-undang privasi. Dengan menangani masalah ini secara komprehensif, perpustakaan dapat memastikan perlindungan privasi pengguna sekaligus mengoptimalkan manfaat sumber daya digital di lingkungan informasi saat ini. Serangan siber pada bulan Oktober 2023 oleh kelompok peretas yang dikenal sebagai Rhysida terhadap sistem informasi internet British Library menekankan pentingnya keamanan siber dan privasi data untuk perpustakaan digital. Penelitian ini bertujuan untuk memberikan wawasan dan solusi untuk mengatasi tantangan ini, memastikan perpustakaan digital dapat beroperasi dengan aman dan efisien.

Kata Kunci : Privasi Data, Sumber Daya Elektronik, Keamanan Siber, Kerahasiaan, Pertimbangan Etis

INTRODUCTION

Over the past decade, there has been an explosion of information in digital libraries around the world (Batool et al., 2024; Masood et al., 2024; Noah & Das, 2024). Libraries hold huge archives of information, including research databases, collections of digitized materials, and more. The ease of access to knowledge has become greater thanks to these resources. However, keeping users' personal data and intellectual property rights secure is a significant challenge (M & Murugan, 2024). This digital transformation has revolutionized the way we interact with information, democratizing access to knowledge and breaking down barriers that once limited academic and professional growth. Yet, as digital libraries become more integral to our educational and research infrastructure, the necessity for robust cybersecurity measures cannot be overstated (Sendjaja et al., 2024). Ensuring the protection of sensitive data and upholding intellectual property laws is paramount to maintaining the integrity and

trustworthiness of these digital repositories (Vargas & Torres, 2024). Without stringent security protocols, the potential for data breaches and misuse of intellectual property could undermine the very benefits that digital libraries aim to provide. Hence, it is essential for institutions to continually invest in advanced security technologies and develop comprehensive policies that address these evolving threats.

In today's digital age, privacy and security are crucial issues, especially in the context of library electronic resources (Filani, 2024; Wu, 2024; Zheng et al., 2023). With most information available and stored digitally, ensuring the privacy, availability, and integrity of library resources is of paramount importance. The introduction of electronic library resources has significantly changed the way people access and utilize information. However, along with these developments have come concerns about data security and privacy. Threats such as cyberattacks, unauthorized access, and compliance with data protection regulations are of concern (Hashem, 2024; Sharma & Nebhnani, 2024; Subramani et al., 2024; Wang, 2024).

The history of data privacy in libraries has undergone a significant evolution along with the development of information technology and the changing expectations of society regarding personal data security. In the pre-digital era, libraries focused more on managing physical collections such as books and manuscripts, with the main priority being maintaining the anonymity of patron records and borrowing history. At that time, the concept of data privacy was not yet a major concern, focusing more on the privacy of users of library services rather than the privacy of librarians.

The introduction of automated systems in the 1970s and 1980s marked the transition from manual record keeping to computerized databases. This change raised new questions regarding the security and privacy of electronically stored patron information (Bindra & Aggarwal, 2024; Brighente et al., 2024). The American Library Association (ALA) adopted a "Code of Ethics" in 1975, which governs moral considerations regarding user privacy, emphasizing the importance of privacy in library services.

With the rise of the internet and the digitization of library collections in the late 20th century came new opportunities as well as concerns about security and unauthorized access. Libraries began offering online resources and services, which increased the risks related to user data privacy. To address these concerns, libraries used digital rights management technologies to protect copyrighted content and restrict access to electronic resources.

As the volume of information processed and stored increases, digital libraries face challenges in protecting users' personal data. The implementation of international standards such as ISO 27001 and ISO 27701 helps libraries improve data protection procedures and comply with applicable privacy regulations, such as the GDPR in the European Union. Libraries also adopt strong privacy policies to ensure the security of user data and avoid privacy breaches.

This introduction emphasizes the importance of protecting users' and staff's personal information and maintaining data privacy and security in the context of library electronic resources. The historical development of data privacy in libraries shows that as technology advances and society changes, approaches to security and privacy must constantly evolve to address new challenges that arise. Digital libraries are required to comply with certain technological and regulatory standards to protect user data and guarantee privacy when accessing electronic resources.

METHODS

Anticipating changes in user behavior, new threats, and technological advances is key in predicting future trends in digital library security and privacy. The utilization of artificial intelligence (AI) and machine learning algorithms is crucial in identifying and preventing security threats. AI can analyze large datasets (big data) to detect unusual behavior patterns and automate responses to security incidents. This proactive approach helps in quickly mitigating potential risks before they escalate. Implementing privacy-preserving technologies such as federated learning and differential privacy can significantly enhance the protection of users' personal data. Federated learning allows data to be processed locally on devices without sharing raw data, while differential privacy ensures that statistical analyses do not compromise individual privacy. These technologies enable secure data

exchange and analysis, ensuring that user data remains confidential (Masood et al., 2024; Munilla Garrido et al., 2024; Wen et al., 2024; Wu, 2024).

Integrating biometric authentication technologies, including fingerprint, facial recognition, and iris scanning, enhances security by providing a more secure and convenient method for user authentication. Biometric data is unique to each individual, making it difficult for unauthorized users to gain access (Manalo & Gallardo, 2024; Wa Nkongolo, 2024). Adopting a trustless security model involves implementing systems that do not rely on traditional trust assumptions. This model restricts user access based on stringent verification processes and prevents lateral movement of threats within the library's infrastructure. It ensures that even if one part of the system is compromised, the threat cannot easily spread (Khan et al., 2024).

Ensuring compliance with data privacy regulations such as the General Data Protection Regulation (GDPR) is essential. This involves investing in robust data governance systems that manage data securely and transparently, ensuring that all data handling practices meet legal requirements (Kutschera et al., 2024). Educating users about cybersecurity best practices is vital in protecting digital libraries from social engineering and phishing attacks. Awareness programs can train users to recognize and respond appropriately to potential threats, significantly reducing the risk of security breaches (Manalo & Gallardo, 2024).

Implementing automated incident response systems and real-time monitoring helps in the quick identification and resolution of security incidents. These systems continuously monitor the digital environment for suspicious activities and trigger automated responses to contain and mitigate threats (Khan et al., 2024). Being prepared to deal with emerging threats is crucial as technology advances. New challenges include attacks on cloud infrastructure, Internet of Things (IoT) devices, and Augmented Reality/Virtual Reality (AR/VR) systems. Staying ahead of these threats requires continuous research and the development of advanced security measures (Aldaej, 2021; Aldhaheri et al., 2024; Alwahedi et al., 2024; Kumari et al., 2024; Sangwan, 2024; Singh et al., 2023; Szymanski, 2024). By applying these methods, digital libraries are expected to face future security and privacy challenges more effectively and responsively. These proactive and comprehensive strategies will help safeguard digital resources, ensuring their availability and integrity for all users.

RESULT AND DISCUSSION

Result

The physical infrastructure of digital libraries is vulnerable to various threats, including virus and malware attacks, theft, and vandalism (H. Chen & Babar, 2024; Sulaiman et al., 2024). To prevent this, measures such as hardware protection, networking, as well as regular data backup teratur (Aksoy, 2024; T. Chen et al., 2024; Shen et al., 2024).

Attention to law and ethics is essential in the administration, distribution, and use of digital resources. Matters to be considered include copyright and intellectual property rights, where copyright protection and recognition of creators are key in the digitization and distribution of works (Davies, 2023); privacy and data protection, which necessitate the protection of user data by implementing privacy policies that comply with applicable data protection regulations (Demirer et al., 2024; Filani, 2024; Wu, 2024); and accessibility, ensuring that everyone, including people with disabilities, can easily access digital libraries (Wu, 2024).

Furthermore, content curation and filtering systems are needed to ensure conformity with moral and legal guidelines (Davies, 2023). Libraries have a responsibility to protect and preserve their digital content through techniques such as file format migration and backup (Demirer et al., 2024). The implementation of open access and the use of open licenses such as Creative Commons enable the reuse and redistribution of digital content (Wu, 2024). Data collection and use should be conducted ethically and transparently to maintain user freedom and privacy (Wu, 2024).

In addition, the use of digital rights management technologies should be balanced with the rights of users (Davies, 2023). Ethical considerations in collection development are also crucial, where libraries should consider diversity, equity, and inclusion in the selection of digital collections (Wu, 2024).

ISO provides a series of standards that libraries can use to strengthen data security, including ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017, ISO/IEC 27018, ISO 27701, and ISO 15489 (ISO, year). These standards provide frameworks and guidelines for information security management, data privacy, and records management.

Cybersecurity threats that digital libraries need to be aware of include data breaches, tampering devices, circumvention, and distributed denial-of-service attacks.

This research identifies some key strategies for privacy protection and data security in the management of library electronic resources. These strategies encompass technical, legal, and educational aspects that are all necessary to ensure the security and privacy of user data. The results showed that implementing international standards such as ISO 27001 and ISO 27701 is essential in managing library data security. These standards provide a comprehensive framework for information security management and the protection of user data privacy.

The use of data encryption and strict access management can effectively prevent unauthorized access and protect the confidentiality of user data. Multifactor authentication systems were also identified as an effective method to enhance security, adding an extra layer of protection against potential breaches. Compliance with privacy regulations, such as the General Data Protection Regulation (GDPR) in the European Union, is critical for libraries. Adhering to these regulations ensures that user data is protected in accordance with applicable laws, and a robust privacy policy helps avoid privacy breaches while building user trust.

Education on cybersecurity best practices for library staff and users is equally essential. Increasing awareness of threats such as social engineering and phishing can significantly reduce the risk of cyberattacks. Libraries should implement training programs to educate both staff and users on how to recognize and respond to these threats, thereby enhancing the overall security posture of the institution.

Additionally, the utilization of artificial intelligence (AI) and machine learning algorithms can greatly enhance the detection and prevention of security threats. Big data analysis assists in identifying unusual behavior patterns and automating responses to incidents, thereby providing a proactive approach to cybersecurity. By integrating these technologies, libraries can effectively manage the security and privacy of their electronic resources, ensuring a safer environment for all users.

Discussion

The results show that digital libraries face significant challenges in protecting the privacy and security of user data. The implementation of international standards and advanced encryption technologies can help overcome some of these challenges. However, technology alone is not enough. Libraries also need to ensure compliance with applicable privacy regulations and educate users and staff about the importance of data security.

One of the main challenges is maintaining a balance between accessibility and security. Library resources must be easily accessible to authorized users while remaining protected from unauthorized access. Digital rights management (DRM) and biometric authentication technologies can help address this challenge but also require sophisticated infrastructure and significant investment. Compliance with laws such as GDPR and other privacy laws is essential to protect user rights and avoid legal sanctions. Libraries should have a clear and transparent privacy policy and ensure that all staff understand and comply with the policy. Additionally, libraries should consider ethical considerations in data management, including the ethical use of algorithms and respect for intellectual property rights.

Continuous education of library staff and users is key to ensuring that they are aware of security and privacy threats. Regular training programs and awareness campaigns can help reduce the risk of cyberattacks and improve compliance with best security practices. Utilizing new technologies such as AI and machine learning can improve libraries' ability to detect and respond to threats. These technologies enable early detection of suspicious behavior and faster automated responses, thereby reducing the potential impact of a security incident.

Overall, digital libraries need to adopt a comprehensive approach to protecting data privacy and security. This includes the implementation of advanced technology, regulatory compliance, and ongoing education for all parties involved. Only with this integrated approach can libraries ensure the security and integrity of their digital resources in the ever-evolving digital age.

CONCLUSION

This research shows that privacy protection and data security in the management of library electronic resources are very important aspects and require serious attention. The implementation of international security standards such as ISO 27001 and ISO 27701 has proven essential in ensuring effective information security management. In addition, encryption technologies and strict access management systems, including multifactor authentication, have proven effective in protecting user data from unauthorized access. Compliance with privacy regulations such as GDPR is critical to protecting users' privacy rights and building their trust, as well as reducing legal risks for digital libraries.

Continued education on cybersecurity best practices for library staff and users is also critical to reducing the risk of cyberattacks. Awareness of threats such as phishing and social engineering can improve preparedness and response to security incidents. The use of artificial intelligence (AI) and machine learning algorithms can also improve libraries' ability to detect and respond to security threats in real-time, enabling more in-depth data analysis and automation in security incident management.

Overall, digital libraries need to adopt a holistic and integrated approach to achieve optimal privacy protection and data security. This approach includes the implementation of advanced technologies, compliance with applicable regulations, and continuous education and training for all parties involved. By doing so, digital libraries can ensure the security and integrity of their electronic resources and maintain user trust in the evolving digital age.

REFERENCES

Aksoy, C. (2024). Building a Cyber Security Culture for Resilient Organizations Against Cyber Attacks. In *İşletme Ekonomi ve Yönetim Araştırmaları Dergisi* (Vol. 7, Issue 1, pp. 96–110). Bayburt Universitesi. https://doi.org/10.33416/baybem.1374001

Aldaej, A. (2021). Notice of Retraction: Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI). In *IEEE Access* (p. 1). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/ACCESS.2019.2893445

Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. In *Internet of Things and Cyber-Physical Systems* (Vol. 4, pp. 110–128). Elsevier BV. https://doi.org/10.1016/j.iotcps.2023.09.003

Alwahedi, F., Aldhaheri, A., Ferrag, M. A., Battah, A., & Tihanyi, N. (2024). Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models. In *Internet of Things and Cyber-Physical Systems* (Vol. 4, pp. 167–185). Elsevier BV. https://doi.org/10.1016/j.iotcps.2023.12.003

Batool, H., Anjum, A., Khan, A., Izzo, S., Mazzocca, C., & Jeon, G. (2024). A secure and privacy preserved infrastructure for VANETs based on federated learning with local differential privacy. In *Information Sciences* (Vol. 652, p. 119717). Elsevier BV. https://doi.org/10.1016/j.ins.2023.119717

Bindra, S. S., & Aggarwal, A. (2024). Security in cyber physical systems: Transformation and challenges. In *Journal of Autonomous Intelligence* (Vol. 7, Issue 4). Frontier Scientific Publishing Pte Ltd. https://doi.org/10.32629/jai.v7i4.1336

Brighente, A., Conti, M., Renzone, G. Di, Peruzzi, G., & Pozzebon, A. (2024). Security and Privacy of Smart Waste Management Systems: A Cyber-Physical System Perspective. In *IEEE Internet of Things Journal* (Vol. 11, Issue 5, pp. 7309–7324). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/JIOT.2023.3322532

Chen, H., & Babar, M. A. (2024). Security for Machine Learning-based Software Systems: A Survey of Threats, Practices, and Challenges. In *ACM Computing Surveys* (Vol. 56, Issue 6, pp. 1–38). Association for Computing Machinery (ACM). https://doi.org/10.1145/3638531

Chen, T., Zeng, H., Lv, M., & Zhu, T. (2024). CTIMD: Cyber threat intelligence enhanced malware detection using API call sequences with parameters. In *Computers and Security* (Vol. 136, p. 103518). Elsevier BV. https://doi.org/10.1016/j.cose.2023.103518

Davies, J. (2023). Enhanced scalability and privacy for blockchain data using Merklized transactions. In *Frontiers in Blockchain* (Vol. 6). Frontiers Media SA. https://doi.org/10.3389/fbloc.2023.1222614

Demirer, M., Jiménez Hernández, D., Li, D., & Peng, S. (2024). Data, Privacy Laws and Firm Production: Evidence from the GDPR. In *SSRN Electronic Journal*. Elsevier BV. https://doi.org/10.2139/ssrn.4718871

Dong, C., Weng, J., Li, M., Liu, J. N., Liu, Z., Cheng, Y., & Yu, S. (2024). Privacy-Preserving and Byzantine-Robust Federated Learning. In *IEEE Transactions on Dependable and Secure Computing* (Vol. 21, Issue 2, pp. 889–904). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/TDSC.2023.3264697

Filani, J. (2024). Data Privacy in the Digital Age: Analyzing the impact of Technology of U.S Privacy Regulations. In *SSRN Electronic Journal*. Elsevier BV. https://doi.org/10.2139/ssrn.4762809

Hashem, T. N. (2024). Examining marketing cyber-security in the digital age: Evidence from marketing platforms. In *International Journal of Data and Network Science* (Vol. 8, Issue 2, pp. 1141–1150). Growing Science. https://doi.org/10.5267/j.ijdns.2023.11.020

Khan, I. A., Razzak, I., Pi, D., Khan, N., Hussain, Y., Li, B., & Kousar, T. (2024). Fed-Inforce-Fusion: A federated reinforcement-based fusion model for security and privacy protection of IoMT networks against cyber-attacks. In *Information Fusion* (Vol. 101, p. 102002). Elsevier BV. https://doi.org/10.1016/j.inffus.2023.102002

Kumari, S., Tulshyan, V., & Tewari, H. (2024). Cyber Security on the Edge: Efficient Enabling of Machine Learning on IoT Devices. In *Information (Switzerland)* (Vol. 15, Issue 3, p. 126). MDPI AG. https://doi.org/10.3390/info15030126

Kutschera, S., Slany, W., Ratschiller, P., Gursch, S., Deininger, P., & Dagenborg, H. (2024). Incidental Data: A Survey towards Awareness on Privacy-Compromising Data Incidentally Shared on Social Media. In *Journal of Cybersecurity and Privacy* (Vol. 4, Issue 1, pp. 105–125). MDPI AG. https://doi.org/10.3390/jcp4010006

M, V., & Murugan, R. (2024). The Role of Artificial Intelligence in Cyber Security. In *International Journal of Innovative Research in Computer and Communication Engineering* (Vol. 12, Issue 03, pp. 1635–1641). Ess & Ess Research Publications. https://doi.org/10.15680/ijircce.2024.1203044

Manalo, M. L. B., & Gallardo, R. D. (2024). Cyber Security Awareness and Educational Outcomes of Grade 4 Learners. In *International Journal of Innovative Science and Research Technology (IJISRT)* (pp. 1390–1422). International Journal of Innovative Science and Research Technology. https://doi.org/10.38124/ijisrt/ijisrt24apr1261

Masood, I., Daud, A., Wang, Y., Banjar, A., & Alharbey, R. (2024). A blockchain-based system for patient data privacy and security. In *Multimedia Tools and Applications*. Springer Science and Business Media LLC. https://doi.org/10.1007/s11042-023-17941-y

Munilla Garrido, G., Nair, V., & Song, D. (2024). SoK: Data Privacy in Virtual Reality. In *Proceedings on Privacy Enhancing Technologies* (Vol. 2024, Issue 1, pp. 21–40). Privacy Enhancing Technologies Symposium Advisory Board. https://doi.org/10.56553/popets-2024-0003

Noah, N., & Das, S. (2024). Privacy and Security in Extended Reality: Exploring the Risks of External Biometric Data Collection. In *SSRN Electronic Journal*. Elsevier BV. https://doi.org/10.2139/ssrn.4780358

Sangwan, U. (2024). Efficient Cyber Security Framework for IoT Using Machine Learning Algorithms. In *Journal of Electrical Systems* (Vol. 20, Issue 6, pp. 2444–2451). Science Research Society. https://doi.org/10.52783/jes.3233

Sendjaja, T., Irwandi, Prastiawan, E., Suryani, Y., & Fatmawati, E. (2024). Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks. In *International Journal of Science and Society* (Vol. 6, Issue 1, pp. 1008–1019). Goacademica Research and Publishing. https://doi.org/10.54783/ijsoc.v6i1.1098

Sharma, S., & Nebhnani, M. (2024). Securing the Digital Frontier: Data Science Applications in Cyber security and Anomaly Detection. In *International Journal of Food and Nutritional Sciences* (Vol. 09, Issue 03). Institute for Advanced Studies. https://doi.org/10.48047/ijfans/09/03/33

Shen, X., Liu, Y., Li, F., & Li, C. (2024). Privacy-Preserving Federated Learning Against Label-Flipping Attacks on Non-IID Data. In *IEEE Internet of Things Journal* (Vol. 11, Issue 1, pp. 1241–1255). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/JIOT.2023.3288886

Singh, J., Reddy, A. M., Bande, V., Lakshmanarao, A., Rao, G. S., & Samunnisa, K. (2023). Enhancing Cloud Data Privacy with a Scalable Hybrid Approach: HE-DP-SMC. In *Journal of Electrical Systems* (Vol. 19, Issue 4, pp. 350–375). Science Research Society. https://doi.org/10.52783/jes.643

Subramani, J., Maria, A., Rajasekaran, A. S., & Lloret, J. (2024). Physically secure and privacy-preserving blockchain enabled authentication scheme for internet of drones. In *Security and Privacy* (Vol. 7, Issue 3). Wiley. https://doi.org/10.1002/spy2.364

Sulaiman, M., Waseem, M., Ali, A. N., Laouini, G., & Alshammari, F. S. (2024). Defense Strategies for Epidemic Cyber Security Threats: Modeling and Analysis by Using a Machine Learning Approach. In *IEEE Access* (Vol. 12, pp. 4958–4984). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/ACCESS.2024.3349660

Szymanski, T. H. (2024). A Quantum-Safe Software-Defined Deterministic Internet of Things (IoT) with Hardware-Enforced Cyber-Security for Critical Infrastructures. In *Information* (Vol. 15, Issue 4, p. 173). MDPI AG. https://doi.org/10.3390/info15040173

Vargas, E. T., & Torres, E. (2024). Legal Challenges of Digital Copyright Laws in the Circulation of Digital Content. In *Law and Economy* (Vol. 3, Issue 1, pp. 1–10). Aurora Publishing House Limited. https://doi.org/10.56397/le.2024.01.01

Wa Nkongolo, M. (2024). Infusing Morabaraba game design to develop a cybersecurity awareness game (CyberMoraba). In *International Conference on Cyber Warfare and Security* (Vol. 19,

Issue 1, pp. 240–250). Academic Conferences International Ltd. https://doi.org/10.34190/iccws.19.1.1957

Wang, W. (2024). Research on Data Security and Privacy Protection in the Context of Big Data. In *Frontiers in Computing and Intelligent Systems* (Vol. 7, Issue 1, pp. 29–33). Darcy & Roy Press Co. Ltd. https://doi.org/10.54097/astapa66

Wen, X., Chen, Y., Zhang, W., Jiang, Z. L., & Fang, J. (2024). Quantum protection scheme for privacy data based on trusted center. In *Optics and Laser Technology* (Vol. 169, p. 110130). Elsevier BV. https://doi.org/10.1016/j.optlastec.2023.110130

Wu, C. (2024). Data privacy: From transparency to fairness. In *Technology in Society* (Vol. 76, p. 102457). Elsevier BV. https://doi.org/10.1016/j.techsoc.2024.102457

Zheng, Y., Zhu, H., Lu, R., Guan, Y., Zhang, S., Wang, F., Shao, J., & Li, H. (2023). PHRkNN: Efficient and Privacy-Preserving Reverse kNN Query Over High-Dimensional Data in Cloud. In *IEEE Transactions on Dependable and Secure Computing* (pp. 1–15). Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/TDSC.2023.3291715