Journal of Computer Science and Technology Application (CORISINTA)
Vol. 1, No. 2, 2024, pp. 96∼103
E-ISSN:XXXX-XXXX P-ISSN: 3046-7616, DOI:XXX

Enhancing Cybersecurity Risk Management Strategies in Financial Institutions: A Comprehensive Analysis of Threats and Mitigation Approaches

Agus Kristian[1], Achani Rahmania Az-Zahra[2*], Farhan Hidayat[3], Ahmad Yadi Fauzi[4], Evelin Kallas[5]
[1]Faculty of Social and Political Science, Muhammadiyah University of Tangerang, Indonesia
[2]Faculty of Information Technology, APTIKOM, Indonesia
[3,4]Faculty of Information Technology, University of Raharja, Indonesia
[5]Information Technology, Mfinitee Incorporation, Estonia
[1]aguschristian1589@gmail.com, [2]achani@raharja.info, [3]farhan.hidayat@raharja.info,
[4]ahmad.yadi@raharja.info, [5]evellin@mfinitee.co.za
***Corresponding Author**

Article Info

Article history:

Received June 23, 2024
Revised August 13, 2024
Accepted August 19, 2024

Keywords:

Cybersecurity
Financial Institutions
Risk Management
Phishing
Ransomware

ABSTRACT

This study investigates the cybersecurity risks faced by financial institutions, with a particular focus on identifying common threats, evaluating their impact, and assessing the effectiveness of risk management strategies. Utilizing a mixed-methods approach, data were collected from both primary and secondary sources, including expert interviews, surveys, and a review of academic and industry literature. The results highlight that phishing, ransomware, and malware are among the most prevalent threats, with email and websites being the primary attack vectors. The study also examines the significant financial and reputational impacts these threats pose. A case study of XYZ Bank demonstrates how a layered approach to cybersecurity, involving prevention, detection, response, and recovery strategies, can substantially reduce the frequency of cyber incidents. The findings emphasize the importance of continuous updates to security policies, regular employee training, and investment in advanced security technologies. The study concludes with recommendations for financial institutions to enhance their cybersecurity posture through comprehensive risk management strategies.

Corresponding Author:

Achani Rahmania Az-Zahra
Faculty of Information Technology, APTIKOM, Indonesia
achani@raharja.info

1. INTRODUCTION

Cybersecurity has become one of the most critical aspects of operational financial institutions in today's digital era [1]. Financial institutions, such as banks, insurance companies, and asset managers, store and process large amounts of sensitive data, including personal and financial information of customers [2]. This data is highly valuable to cyber attackers who use various methods to steal, alter, or destroy this data for financial gain or other malicious purposes [3]. In recent years, cyber attacks on financial institutions have increased in both frequency and complexity [4]. These attacks include phishing, ransomware, malware, Distributed Denial of Service (DDoS), and Advanced Persistent Threats (APT). For example, ransomware attacks can encrypt critical data and demand a ransom to restore access, while DDoS attacks can cripple online services by overwhelming servers with excessive traffic. The potential impact of cyber attacks on financial institutions

is significant. Besides the direct financial losses from theft or ransom payments, financial institutions may also suffer indirect losses such as reputational damage, loss of customer trust, and legal and regulatory costs. Cyber attacks can also disrupt daily operations, causing a decline in productivity and increased recovery costs [5]. Given the importance of cybersecurity, financial institutions must develop and implement effective risk management strategies [6]. Cybersecurity risk management involves identifying, assessing, and mitigating risks associated with cyber threats. This includes adopting advanced security technologies, establishing robust security policies and procedures, and educating employees on good security practices.

The main objective of this research is to identify the cybersecurity risks faced by financial institutions and to develop effective risk management strategies to address these risks [7]. This research aims to provide in-depth insights into the most common cyber threats, attack vectors used by attackers, and the potential impact of cyber attacks on financial institutions. Additionally, this research aims to evaluate the effectiveness of various risk management strategies employed by financial institutions in preventing, detecting, responding to, and recovering from cybersecurity incidents [8].

Specifically, this research aims to:

1. Identify and analyze the most common cyber threats faced by financial institutions.
2. Assess the potential impact of cyber threats on the operations and reputation of financial institutions.
3. Evaluate the effectiveness of security technologies, policies, and procedures used to protect financial data and systems.
4. Develop recommendations for financial institutions in developing and implementing more effective cybersecurity risk management strategies.

1.1. Literature Review

1.1.1. Cybersecurity in Financial Institutions

Financial institutions face a multitude of cyber threats that continually evolve in complexity and frequency [9]. These threats pose significant risks to the integrity, confidentiality, and availability of sensitive financial data and systems. Common cyber threats to financial institutions include phishing, ransomware, malware, Distributed Denial of Service (DDoS) attacks, and Advanced Persistent Threats (APT). Phishing is a prevalent attack method where attackers use deceptive emails, messages, or websites to trick individuals into disclosing sensitive information such as login credentials or financial information [10]. These attacks exploit human vulnerabilities and are often the precursor to more extensive breaches. Ransomware attacks involve malicious software that encrypts an organization's data, rendering it inaccessible until a ransom is paid [11]. Financial institutions are prime targets due to their reliance on data availability and the potential for significant financial loss if operations are disrupted. Malware encompasses various types of malicious software, including viruses, worms, and Trojans, designed to damage, disrupt, or gain unauthorized access to systems [12]. Financial institutions often face malware attacks aimed at stealing sensitive information or compromising system integrity.

DDoS attacks flood a targeted system or network with excessive traffic, overwhelming the infrastructure and causing service outages. These attacks can disrupt online banking services, causing reputational damage and financial losses [13]. Advanced Persistent Threats (APT) are prolonged and targeted cyber attacks in which an intruder gains access to a network and remains undetected for an extended period [14]. APTs are often used to steal sensitive information or disrupt operations and are characterized by their sophistication and persistence.

1.1.2. Risk Management Framework

Effective cybersecurity risk management involves a structured approach to identifying, assessing, and mitigating risks [15]. Several theoretical frameworks and models are relevant to cybersecurity risk management in financial institutions. The NIST Cybersecurity Framework is widely adopted and provides a comprehensive guide for managing and reducing cybersecurity risk. It consists of five core functions: Identify, Protect, Detect, Respond, and Recover [16]. This framework helps organizations develop a robust cybersecurity strategy by providing guidelines and best practices.

- Identify: Understanding the organization's environment to manage cybersecurity risks to systems, assets, data, and capabilities. This includes asset management, business environment, governance, risk assessment, and risk management strategy [17].

- Protect: Implementing safeguards to ensure the delivery of critical infrastructure services. This includes access control, awareness training, data security, information protection processes and procedures, maintenance, and protective technology.
- Detect: Developing and implementing appropriate activities to identify the occurrence of a cybersecurity event. This includes anomalies and events, continuous monitoring, and detection processes [18].
- Respond: Taking action regarding a detected cybersecurity incident. This includes response planning, communications, analysis, mitigation, and improvements.
- Recover: Involves maintaining resilience plans and restoring any capabilities or services that have been impaired due to a cybersecurity incident. This process includes recovery planning, implementing improvements, and ensuring effective communication.

ISO/IEC 27001 is another widely recognized standard that specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) [19]. It helps organizations manage the security of assets such as financial information, intellectual property, employee details, and information entrusted by third parties [20]. COBIT (Control Objectives for Information and Related Technologies) provides a framework for developing, implementing, monitoring, and improving IT governance and management practices. It aligns IT goals with business objectives and includes comprehensive guidelines for cybersecurity risk management [21].

1.1.3. Related Research

Numerous studies have examined the challenges and strategies of cybersecurity risk management in the financial sector. A study explores the decision-making processes in cybersecurity risk management and highlights the importance of integrating risk management frameworks with organizational decision-making structures [22]. The study suggests that financial institutions need to adopt a holistic approach to cybersecurity, integrating technical, organizational, and human factors.

Investigate the cost-benefit analysis of information security investments in the financial sector [23]. Their research emphasizes the need for financial institutions to balance the costs of implementing security measures with the potential financial losses from cyber incidents. The study provides a quantitative approach to evaluating the effectiveness of different security investments [23]. Examines the role of cybersecurity metrics in risk management [24]. The authors argue that financial institutions should develop and use cybersecurity metrics to assess the effectiveness of their security controls and to inform risk management decisions [25]. The study highlights the need for continuous monitoring and assessment to adapt to evolving cyber threats. On the financial impact of cyber attacks on stock prices reveals the significant financial consequences that cyber incidents can have on financial institutions [26]. The study shows that cyber attacks can lead to immediate stock price declines and long-term reputational damage, underscoring the critical need for robust cybersecurity risk management practices.

2. THE COMPREHENSIVE THEORETICAL BASIS

2.1. Research Design

The research approach used in this study is a mixed-methods approach that combines qualitative and quantitative analysis to identify and analyze cybersecurity risks in financial institutions. This approach is chosen to provide a comprehensive understanding of the various technical, operational, and human aspects related to cybersecurity [27]. The study involves data collection from primary and secondary sources, followed by an in-depth analysis to identify and evaluate the factors influencing the success and challenges in implementing cybersecurity risk management strategies.

2.2. Data Collection

Data collection is conducted through several steps, utilizing both primary and secondary data sources. The primary data sources include expert interviews and surveys. In-depth interviews are conducted with industry experts, technologists, regulators, and academics with expertise in cybersecurity. These interviews are designed to gain deep insights into cyber threats, best practices in risk management, and the challenges faced by financial institutions [28]. Additionally, surveys are distributed to industry practitioners, technology companies, and risk managers in financial institutions to collect quantitative data on their perceptions, expectations, and experiences with cybersecurity risks.

Secondary data sources are also crucial to this study. The academic literature is reviewed to gather journal articles, conference papers, and previous research reports relevant to the topic of cybersecurity, providing a theoretical foundation and context for further analysis [29]. Industry and government reports are collected to provide information on best practices, regulatory policies, and market statistics related to cybersecurity in the financial sector. The data collection methods employed include documentation and participant observation. Relevant documents, such as white papers, technical reports, and regulations related to cybersecurity technologies, are collected and reviewed [30]. Additionally, participant observation is conducted by observing the implementation of cybersecurity risk management strategies in real-world situations, such as field trials and pilot projects, to understand best practices and challenges faced during implementation.

2.3. Data Analysis

The data analysis techniques used in this study include both qualitative and quantitative analysis methods. Qualitative analysis involves thematic analysis, where data from interviews and observations are analyzed to identify key themes related to cyber threats and risk management strategies [31]. This technique includes coding the data and identifying significant patterns and relationships. Furthermore, case studies are used to analyze the implementation of cybersecurity risk management strategies in various financial institutions, helping to understand specific contexts and lessons learned from practical experiences. Quantitative analysis is conducted using descriptive and inferential statistics. Survey data are analyzed with descriptive statistics to identify trends and patterns in users' perceptions and experiences with cybersecurity risks, including frequency analysis, mean, median, and data distribution. Inferential analysis involves statistical tests such as t-tests, analysis of variance (ANOVA), and regression to test research hypotheses and evaluate relationships between the collected variables.

Finally, data triangulation is performed by combining findings from both qualitative and quantitative analyses to ensure the validity and reliability of the research results. This triangulation helps confirm findings and provides a more holistic understanding of the research problem.

3. RESULTS AND DISCUSSION

3.1. Identification of Cybersecurity Risks

Table 1. Frequency of Cyber Threats Faced by Financial Institutions

Type of Cyber Threat	Frequency (%)
Phishing	85%
Ransomware	70%
Malware	65%
DDoS Attacks	50%
APT	45%

The data from this study reveal several major risks faced by financial institutions. Table 1 shows the types of cyber threats and their frequency based on surveys from various financial institutions. This data highlights that phishing is the most common cyber threat, followed by ransomware and malware, which together account for a significant portion of the cyber risks faced by these institutions.

Table 2. Frequency of Attack Vectors

Attack Vector	Frequency (%)
Email	80%
Websites	60%
Networks	55%
Software Applications	50%
Insiders	40%

Table 2 illustrates the frequency of different attack vectors used to breach the cybersecurity defenses of financial institutions. The data reveals that email is the most frequently exploited vector, followed by websites and network intrusions. Understanding these vectors is crucial for developing targeted defense strategies.

3.2. Impact of Cyber Threats

Table 3. Potential Impact of Cyber Threats on Financial Institutions

Impact	Frequency (%)
Financial Loss	75%
Operational Disruption	60%
Reputational Damage	65%
Regulatory Consequences	50%
Data Compromise	55%
Legal Implications	45%

The potential impact of various cyber threats on the operations and reputation of financial institutions is significant. Table 3 summarizes the potential impacts, with financial loss being the most commonly reported consequence, followed by reputational damage and operational disruption. This table underscores the severe repercussions that cyber threats can have on financial institutions.

3.3. Discussion

Table 4. Incident Frequency Before and After Implementation of Cybersecurity Risk Management Strategies at XYZ Bank

Period	Incident Frequency (%)
Before Implementation	60%
After Implementation	20%

The findings of the study indicate that the implementation of comprehensive cybersecurity risk management strategies can significantly reduce the risks faced by financial institutions. The XYZ Bank case study demonstrates the effectiveness of a layered approach involving prevention, detection, response, and recovery strategies. Table 4 shows the changes in the frequency of cyber incidents before and after the implementation of cybersecurity risk management strategies at XYZ Bank. The data clearly indicates a substantial reduction in incidents, highlighting the effectiveness of the implemented strategies.

3.4. Practical Implications

Based on the research findings, several practical implications for financial institutions can be drawn. Table 1 and Table 2 provide insights into the types and frequencies of cyber threats and attack vectors, respectively. These findings suggest that financial institutions must continuously update and strengthen their security policies to address evolving threats. Regular updates to these policies will enable institutions to stay ahead of emerging threats and protect their assets more effectively. Additionally, ongoing education and training are necessary. As indicated by the common attack vectors in Table 2, human error often plays a role in cybersecurity breaches. Thus, financial institutions should mandate cybersecurity awareness training for all employees, ensuring that they are knowledgeable about the latest threats and best practices in mitigating them. Moreover, investment in advanced security technologies, as implied by the frequency of threats and impacts in Tables 1 and 3, is essential. Financial institutions need to adopt cutting-edge technologies such as Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) to enhance their security posture. Effective response and recovery strategies, supported by the data in Table 4, are also vital. Financial institutions must develop well-structured incident response plans and disaster recovery plans, which should be regularly tested to ensure they function as intended during a real crisis.

Finally, collaboration and cooperation are key to managing cybersecurity risks comprehensively. The data from Tables 1 through 4 indicate the importance of a coordinated approach to cybersecurity. Financial institutions should foster both internal and external collaboration, working closely with other institutions, industry groups, and regulatory bodies to share information and strategies.

3.5. Limitations of the Research

This study has several limitations that should be considered when interpreting the results. One significant limitation is the generalizability of the findings. While the XYZ Bank case study provides valuable

insights into the effectiveness of cybersecurity risk management strategies, these findings may not be fully applicable to all financial institutions. The specific context and characteristics of XYZ Bank might differ from those of other institutions, potentially limiting the broader applicability of the results. Additionally, the study relies on data from a single financial institution, which poses another limitation. The inclusion of data from multiple institutions with varying profiles and sizes would have provided a more comprehensive understanding of cybersecurity risks and management strategies across the financial sector. Future research should consider incorporating a broader range of institutions to enhance the generalizability of the findings.

Another limitation concerns the evolution of cyber threats. Cyber threats are continuously evolving, and strategies that are effective today may not be sufficient in the future. The dynamic nature of the cybersecurity landscape requires constant adaptation and updates to risk management strategies. This study's findings should be viewed as relevant within the current context, with the understanding that they may need to be revisited as new threats emerge. Finally, the human factor remains a critical vulnerability in cybersecurity. Despite the implementation of advanced technologies and strategies, human error or negligence can still lead to significant security breaches. Further research is needed to explore more effective ways to address this vulnerability, including improving employee training, enhancing user interfaces to reduce errors, and developing systems that are more resilient to human factors.

4. CONCLUSION

This research reveals that financial institutions face significant cybersecurity threats, including phishing, ransomware, malware, DDoS attacks, and Advanced Persistent Threats (APT). The analysis of survey data from various financial institutions highlights the frequency and impact of these threats, as well as the most commonly used attack vectors by cybercriminals. The case study of XYZ Bank underscores the effectiveness of a layered approach that involves prevention, detection, response, and recovery strategies in managing cybersecurity risks. Based on the findings of this research, several practical implications for financial institutions include enhanced security policies, ongoing education and training, investment in technology, effective response and recovery, and collaboration and cooperation. Financial institutions should continuously update and strengthen their security policies to address evolving threats, including strict access controls, data encryption, and personal device usage procedures. Cybersecurity awareness training should be an integral part of corporate culture, with training programs regularly updated to reflect the latest threats and best practices in cybersecurity. Additionally, investment in advanced security technologies such as Security Information and Event Management (SIEM) systems, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) is crucial for real-time threat detection and response. Having well-developed and tested incident response and disaster recovery plans is essential for ensuring operational continuity following a cyber incident. Finally, collaboration within departments, as well as with external partners and regulatory authorities, is vital for ensuring a coordinated and comprehensive response to cybersecurity incidents.

This research has several limitations. The case study of XYZ Bank provides valuable insights, but its findings may not be fully generalizable to all financial institutions, as each institution has unique characteristics and challenges that may require tailored strategies. This study also relies on data from a single financial institution, so further research involving various institutions with different profiles and sizes is needed to obtain a more comprehensive understanding. Cyber threats continue to evolve, and strategies that are effective today may require updates in the future. This research reflects the threat conditions at the time of the study and may not fully represent future threats. Additionally, despite the importance of training and cybersecurity awareness, the human factor remains a critical weakness in cybersecurity, necessitating further research to explore more effective ways of addressing these vulnerabilities. Given the limitations of this study, several recommendations for future research include diverse case studies, longitudinal studies, a focus on human factors, research on technological advancements, and investigations into the impact of regulations. Future research should include a broader range of financial institutions with varying sizes, profiles, and geographical locations to provide more generalized findings. Longitudinal studies that observe how cybersecurity threats and effective responses evolve over time will offer deeper insights into the long-term effectiveness of different strategies. Further exploration of human factors in cybersecurity, such as behavioral analysis and training effectiveness, can provide strategies to mitigate risks associated with human error. Research into new technologies and their applications in cybersecurity, such as artificial intelligence (AI) and machine learning (ML), can offer innovative solutions for detecting and responding to sophisticated cyber threats. Finally, investigations into the impact of various

regulatory frameworks on cybersecurity practices and how compliance affects the overall security posture of financial institutions are also necessary.

REFERENCES

[1] L. K. Choi, N. Iftitah, and P. Angela, "Developing technopreneur skills to face future challenges," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 127–135, 2024.

[2] W. Setyowati, R. Widayanti, and D. Supriyanti, "Implementation of e-business information system in indonesia: Prospects and challenges," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2, pp. 180–188, 2021.

[3] D. Nugroho and P. Angela, "The impact of social media analytics on sme strategic decision making," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 169–178, 2024.

[4] I. Amsyar, E. Christopher, A. Dithi, A. N. Khan, and S. Maulana, "The challenge of cryptocurrency in the era of the digital revolution: A review of systematic literature," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 2, no. 2, pp. 153–159, 2020.

[5] R. Hardjosubroto, U. Rahardja, N. A. Santoso, and W. Yestina, "Penggalangan dana digital untuk yayasan disabilitas melalui produk umkm di era 4.0," *ADI Pengabdian Kepada Masyarakat*, vol. 1, no. 1, pp. 1–13, 2020.

[6] N. N. Halisa, "Peran manajemen sumber daya manusia" sistem rekrutmen, seleksi, kompetensi dan pelatihan" terhadap keunggulan kompetitif: Literature review," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 1, no. 2 Desember, pp. 14–22, 2020.

[7] Z. Kedah, "Use of e-commerce in the world of business," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 1, pp. 51–60, 2023.

[8] T. Alam, "Cloud computing and its role in the information technology," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 1, no. 2, pp. 108–115, 2020.

[9] A. Leffia, S. A. Anjani, M. Hardini, S. V. Sihotang, and Q. Aini, "Corporate strategies to improve platform economic performance: The role of technology, ethics, and investment management," *CORISINTA*, vol. 1, no. 1, pp. 16–25, 2024.

[10] A. G. Prawiyogi, A. S. Anwar *et al.*, "Perkembangan internet of things (iot) pada sektor energi: Sistematik literatur review," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 1, no. 2, pp. 187–197, 2023.

[11] E. N. Pratama, E. Suwarni, and M. A. Handayani, "The effect of job satisfaction and organizational commitment on turnover intention with person organization fit as moderator variable," *Aptisi Transactions on Management*, vol. 6, no. 1, pp. 74–82, 2022.

[12] B. Rawat, S. Purnama *et al.*, "Mysql database management system (dbms) on ftp site lapan bandung," *International Journal of Cyber and IT Service Management*, vol. 1, no. 2, pp. 173–179, 2021.

[13] N. Ramadhona, A. A. Putri, and D. S. S. Wuisan, "Students' opinions of the use of quipper school as an online learning platform for teaching english," *International Transactions on Education Technology*, vol. 1, no. 1, pp. 35–41, 2022.

[14] H. Nusantoro, P. A. Sunarya, N. P. L. Santoso, and S. Maulana, "Generation smart education learning process of blockchain-based in universities," *Blockchain Frontier Technology*, vol. 1, no. 01, pp. 21–34, 2021.

[15] D. S. Wuisan and T. Handra, "Maximizing online marketing strategy with digital advertising," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 1, pp. 22–30, 2023.

[16] M. Wahyudi, V. Meilinda, and A. Khoirunisa, "The digital economy's use of big data," *International Transactions on Artificial Intelligence*, vol. 1, no. 1, pp. 62–70, 2022.

[17] D. Manongga, U. Rahardja, I. Sembiring, N. Lutfiani, and A. B. Yadila, "Dampak kecerdasan buatan bagi pendidikan," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 3, no. 2, pp. 110–124, 2022.

[18] R. M. Thamrin, E. P. Harahap, A. Khoirunisa, A. Faturahman, and K. Zelina, "Blockchain-based land certificate management in indonesia," *ADI journal on recent innovation*, vol. 2, no. 2, pp. 232–252, 2021.

[19] D. Bennet, S. A. Anjani, O. P. Daeli, D. Martono, and C. S. Bangun, "Predictive analysis of startup ecosystems: Integration of technology acceptance models with random forest techniques," *CORISINTA*, vol. 1, no. 1, pp. 70–79, 2024.

[20] M. Kamil, Y. Muhtadi, B. M. Sentosa, and S. Millah, "Tindakan operasionalisasi pemahaman sains dan

teknologi terhadap islam," *Alfabet Jurnal Wawasan Agama Risalah Islamiah, Teknologi dan Sosial*, vol. 1, no. 1, pp. 16–25, 2021.

[21] D. S. S. Wuisan, T. Mariyanti *et al.*, "Analisa peran triple helik dalam mengatasi tantangan pendidikan di era industri 4.0," *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, vol. 1, no. 2, pp. 123–132, 2023.

[22] D. A. Kurniawan and A. Z. Santoso, "Pengelolaan sampah di daerah sepatan kabupaten tangerang," *ADI Pengabdian Kepada Masyarakat*, vol. 1, no. 1, pp. 31–36, 2020.

[23] R. Sivaraman, M.-H. Lin, M. I. C. Vargas, S. I. S. Al-Hawary, U. Rahardja, F. A. H. Al-Khafaji, E. V. Golubtsova, and L. Li, "Multi-objective hybrid system development: To increase the performance of diesel/photovoltaic/wind/battery system." *Mathematical Modelling of Engineering Problems*, vol. 11, no. 3, 2024.

[24] Q. Aini, D. Manongga, U. Rahardja, I. Sembiring, and Y.-M. Li, "Understanding behavioral intention to use of air quality monitoring solutions with emphasis on technology readiness," *International Journal of Human–Computer Interaction*, pp. 1–21, 2024.

[25] R. Supriati, E. R. Dewi, D. Supriyanti, N. Azizah *et al.*, "Implementation framework for merdeka belajar kampus merdeka (mbkm) in higher education academic activities," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 3, no. 2, pp. 150–161, 2022.

[26] S. Sayyida, S. Hartini, S. Gunawan, and S. N. Husin, "The impact of the covid-19 pandemic on retail consumer behavior," *Aptisi Transactions on Management*, vol. 5, no. 1, pp. 79–88, 2021.

[27] U. Rahardja, "The economic impact of cryptocurrencies in indonesia," *ADI Journal on Recent Innovation*, vol. 4, no. 2, pp. 194–200, 2023.

[28] A. K. Yaniaja, H. Wahyudrajat, and V. T. Devana, "Pengenalan model gamifikasi ke dalam e-learning pada perguruan tinggi," *ADI Pengabdian Kepada Masyarakat*, vol. 1, no. 1, pp. 22–30, 2020.

[29] A. Argani and W. Taraka, "Pemanfaatan teknologi blockchain untuk mengoptimalkan keamanan sertifikat pada perguruan tinggi," *ADI Bisnis Digit. Interdisiplin J*, vol. 1, no. 1, pp. 10–21, 2020.

[30] E. Sana, A. Fitriani, D. Soetarno, M. Yusuf *et al.*, "Analysis of user perceptions on interactive learning platforms based on artificial intelligence," *CORISINTA*, vol. 1, no. 1, pp. 26–32, 2024.

[31] H. Sulistiani, A. Yuliani, F. Hamidy *et al.*, "Perancangan sistem informasi akuntansi upah lembur karyawan menggunakan extreme programming," *Technomedia Journal*, vol. 6, no. 1 Agustus, pp. 1–14, 2021.