Sciences du Nord Nature Science and Technology
Vol. 1, No. 01, January, 2024: pp. 20~27
E-ISSN: xxxx-xxx
P-ISSN: xxx-xxx
DOI: -

Literature Review on Computer Network Security in the Financial Sector in Indonesia Challenges and Solutions in Facing Digital Security Threats

Loso Judijanto[1], Faiz Muqorrir Kaaffah[2], Hanifah Nurul Muthmainah[3], Arnes Yuli Vandika[4]
[1] IPOSS Jakarta and losojudijantobumn@gmail.com
[2] IAIN Syekh Nurjati Cirebon and faiz@syekhnurjati.ac.id
[3] Universitas Siber Muhammadiyah and hanifah20220200046@sibermu.ac.id
[4] Universitas Bandar Lampung and arnes@ubl.ac.id

ARTICLE HISTORY
Received: Jan, 2024 **Revised: Jan, 2024** **Accepted: Jan, 2024**

Coresponding Author: losojudijantobumn@gmail.com

ABSTRACT

In an era of rapid digitalization, the financial sector in Indonesia faces a transformative landscape, marked by technological innovation and an escalating array of digital security threats. This literature review explores the pivotal role of computer network security in safeguarding financial data, transactions, and customer trust within this dynamic context. As Indonesia's financial industry embraces digitalization, it becomes an appealing target for cybercriminals, necessitating a robust cybersecurity framework. Challenges such as resource constraints, evolving threats, and complex compliance issues underscore the need for collaborative efforts among financial institutions, policymakers, and stakeholders. This review comprehensively investigates the state of computer network security, identifies vulnerabilities and challenges, proposes effective solutions, and offers recommendations to fortify the cybersecurity posture of Indonesia's financial sector, underscoring its significance in an interconnected digital world.

Keywords: *Financial Sector Digitalization, Computer Network Security, Cybersecurity Challenges in Indonesia, Collaborative Solutions for Financial Cybersecurity*

INTRODUCTION

The rapid evolution of technology has transformed the financial sector in Indonesia, empowering organizations with innovative tools and platforms to enhance their operations, but it has also exposed them to a plethora of digital security threats[1], [2]. In this era of digitalization, computer network security has become paramount in safeguarding sensitive financial data, transactions, and the trust of customers. Understanding the challenges faced by the financial sector in Indonesia and identifying effective solutions for mitigating digital security threats is of utmost importance [3], [4], [5].

The financial sector in Indonesia has witnessed remarkable growth in recent years, driven by technological advancements and a surge in digital financial services [6], [7], [8]. As financial institutions and businesses continue to embrace digitalization, they have become attractive targets for cybercriminals seeking to exploit vulnerabilities in computer networks [7]. These threats include but are not limited to, data breaches, ransomware attacks, phishing scams, and insider threats. The consequences of such security breaches extend beyond financial losses, impacting customer trust, regulatory compliance, and the overall stability of the financial system [9], [10].

Despite the growing awareness of the importance of computer network security, the financial sector in Indonesia faces unique challenges in securing its digital infrastructure. These challenges may include resource constraints, limited expertise, regulatory compliance, and the ever-evolving nature of cyber threats. This research aims to delve into these challenges and identify the specific problems faced by financial institutions in Indonesia in their pursuit of robust network security.

This research endeavors to comprehensively investigate the current state of computer network security in the financial sector of Indonesia, aiming to uncover existing challenges, vulnerabilities, and the effectiveness of security measures employed by financial institutions. It also seeks to propose practical solutions and strategies to bolster computer network security in this critical sector. Furthermore, this study intends to provide policymakers and stakeholders with valuable recommendations to fortify the cybersecurity posture of the financial industry in Indonesia, ensuring the safeguarding of digital assets and the preservation of trust in an increasingly digitized financial landscape.

Underscores the broader societal implications of our research, emphasizing the importance of collective cybersecurity efforts in an increasingly interconnected world. By addressing the specific challenges faced by the financial sector in Indonesia, our findings can serve as a valuable resource for financial institutions striving to fortify their defenses, government authorities seeking to enact effective regulatory frameworks, cybersecurity experts engaged in developing cutting-edge solutions, and the general public, who rely on the security and stability of the financial industry. Ultimately, this research contributes not only to the resilience of Indonesia's financial sector but also to the global dialogue surrounding cybersecurity in the ever-evolving landscape of financial technology and digital transactions. It highlights that safeguarding sensitive financial data, upholding customer trust, and ensuring compliance with cybersecurity regulations are integral to economic stability and the continued vitality of the financial industry.

LITERATURE REVIEW

Computer Network Security and Financial Sector

Computer Network Security is a critical component of modern information technology systems designed to protect networks, devices, and data from unauthorized access, cyberattacks, and data breaches [11], [12]. In the financial sector, which encompasses banks, insurance companies, stock exchanges, and various other financial institutions, the importance of network security cannot be overstated [13]. Financial institutions handle vast amounts of sensitive data, including customer information, financial transactions, and confidential business records [14]. Ensuring the confidentiality, integrity, and availability of this data is paramount to maintaining trust, compliance with regulations, and the overall stability of the financial system [15], [16]. Computer network security in the financial sector involves deploying robust firewalls, intrusion detection and prevention systems, encryption technologies, access controls, and continuous monitoring to detect and mitigate threats such as phishing attacks, ransomware, and insider threats. It also involves staying up-to-date with emerging threats and evolving security measures to adapt to the dynamic nature of cyber risks [17].

In the context of the financial sector in Indonesia, rapid digitalization and the proliferation of financial technology (fintech) have amplified the importance of computer network

security. Indonesia's financial sector has seen substantial growth, with a burgeoning number of digital payment platforms, mobile banking services, and online investment opportunities [18]. However, this digital transformation has also made it a prime target for cybercriminals [19]. The financial sector in Indonesia faces unique challenges, including resource limitations, skills gaps in cybersecurity personnel, and compliance with a complex regulatory landscape [20]. Financial institutions must not only invest in cutting-edge security technologies but also prioritize employee training, cybersecurity best practices, and collaboration with government authorities to tackle these challenges effectively [21]. As the financial sector continues to evolve, maintaining a strong and adaptive computer network security infrastructure is essential to safeguarding the interests of both financial institutions and their customers [22].

Digital Security Threats

Digital security threats, often referred to as cybersecurity threats, encompass a wide range of malicious activities and risks targeting digital assets, systems, and networks [23]. These threats pose significant challenges to individuals, organizations, and governments worldwide [24]. Some common types of digital security threats include malware, which includes viruses, ransomware, and Trojans that can infect computers and compromise data; phishing attacks, where attackers use deceptive emails or websites to trick users into revealing sensitive information like passwords or financial details; and denial-of-service (DoS) attacks that overwhelm a system or network, causing disruptions or downtime [25], [26], [27].

Additionally, digital security threats can take the form of data breaches, where unauthorized access to sensitive information occurs, often leading to data theft or exposure; insider threats, involving individuals within an organization who misuse their access to compromise security; and advanced persistent threats (APTs), which are sophisticated, long-term attacks designed to infiltrate networks and steal valuable data or information over an extended period [28], [29], [30]. These digital security threats continually evolve in complexity and scale, requiring robust cybersecurity measures, employee awareness, and proactive defense strategies to mitigate their impact and protect digital assets and privacy [30], [31].

METHODS

The primary source of data for this study is scholarly literature, research papers, reports, and relevant publications related to computer network security in the financial sector. A comprehensive search will be conducted in academic databases, including but not limited to IEEE Xplore, ACM Digital Library, Google Scholar, and relevant government publications, to gather a diverse and representative selection of materials. Initially, a broad range of literature will be collected. Subsequently, a systematic screening process will be employed to select only the most relevant and high-quality sources. Inclusion and exclusion criteria will be established to ensure the literature aligns with the research objectives and provides valuable insights. The selected literature will undergo a rigorous analysis process, including categorization, thematic analysis, and synthesis. Themes related to challenges, vulnerabilities, security measures, and best practices in computer network security within the Indonesian financial sector will be identified and analyzed.

RESULTS AND DISCUSSION

Current State of Computer Network Security in Financial Sector in Indonesia

The current state of computer network security in the financial sector in Indonesia reflects a complex landscape shaped by both progress and challenges [32]. On one hand, the rapid digitalization and modernization of financial services in the country have ushered in a wave of technological advancements, offering convenience and accessibility to consumers [33]. Financial institutions have invested significantly in upgrading their digital infrastructure to cater to the increasing demand for online banking, mobile payments, and electronic transactions [22]. However, this heightened reliance on technology has exposed financial institutions to a host of cybersecurity risks [34]. Despite efforts to fortify security measures, numerous vulnerabilities persist, threatening the confidentiality and integrity of sensitive financial data [34].

One prominent issue in Indonesia's financial sector is the prevalence of cyberattacks, including phishing, ransomware, and distributed denial-of-service (DDoS) attacks [32]. These threats have the potential to disrupt operations, compromise customer data, and damage the reputation of financial institutions [33]. Resource constraints, both in terms of financial investment and skilled cybersecurity personnel, pose significant challenges for many institutions [35]. Additionally, compliance with the intricate web of national and international cybersecurity regulations remains a complex task [22]. The dynamic nature of cyber threats requires constant adaptation and investment in security solutions. In light of these challenges, the financial sector in Indonesia must prioritize cybersecurity to safeguard the interests of both financial institutions and their customers in an increasingly digitized financial landscape [34].

Primary Challenges and Vulnerabilities

The financial sector in Indonesia faces several primary challenges and vulnerabilities in its quest to maintain robust computer network security [33], [36]. Firstly, resource constraints represent a significant impediment [37]t. Many financial institutions, particularly smaller ones, often lack the financial means to invest in cutting-edge cybersecurity technologies and hire experienced cybersecurity professionals [38]. This imbalance in resources can leave them ill-prepared to defend against sophisticated cyber threats, making them attractive targets for attackers [39].

Secondly, the evolving nature of cyber threats presents an ongoing vulnerability [40]. Cybercriminals continually adapt their tactics and techniques, making it challenging for financial institutions to keep pace [41]. Phishing attacks, for example, have become increasingly sophisticated and difficult to detect, posing a severe threat to the security of sensitive financial data [42]. Additionally, insider threats, whether intentional or accidental, can undermine security measures from within an organization [43]. These challenges highlight the need for constant vigilance, employee training, and staying updated with the latest threat intelligence to effectively mitigate vulnerabilities within the financial sector in Indonesia [44].

Exploration and Evaluation of Security Measures and Practices

To gain a comprehensive understanding of the security measures and practices employed within the financial sector in Indonesia, it is essential to explore and evaluate the existing landscape [45]. Financial institutions in the country have implemented a range of security measures, such as firewalls, intrusion detection systems, encryption protocols, and access controls, to protect their digital assets [46]. Evaluating the effectiveness of these measures is crucial in determining their ability to withstand evolving cyber threats [47], [48]. Through systematic assessment, it is possible to identify gaps or weaknesses in the current security infrastructure [49].

Furthermore, the evaluation process should extend to examining cybersecurity practices within these institutions [50]. This entails scrutinizing policies and procedures related to employee training, incident response, data encryption, and access management [51]. Assessing the level of compliance with cybersecurity standards and regulations is also critical, as it ensures that financial institutions adhere to best practices [52]. By thoroughly exploring and evaluating security measures and practices, this research aims to provide insights into what is working effectively and where

improvements or adjustments are needed to enhance the computer network security of the financial sector in Indonesia [53]. This comprehensive assessment will contribute to strengthening the cybersecurity posture of financial institutions, reducing vulnerabilities, and mitigating potential risks [54].

Effective Solutions and Strategies to Enhance Computer Network Security in Financial Sector

Enhancing computer network security within the financial sector in Indonesia requires the implementation of effective solutions and strategies tailored to the unique challenges faced by this industry [55]. One key solution is the development and adoption of advanced threat detection and response mechanisms [56]. Financial institutions can invest in state-of-the-art security technologies, such as artificial intelligence (AI) and machine learning (ML)-powered security tools, which can detect and respond to emerging threats in real-time [57]. By leveraging AI and ML algorithms, these solutions can identify anomalies and unusual patterns in network traffic, providing early warnings of potential cyberattacks and enabling proactive measures [58], [59].

Another crucial strategy is fostering a culture of cybersecurity within financial organizations. This entails continuous employee training and awareness programs to educate staff about the latest cybersecurity threats and best practices [60]. Encouraging a strong cybersecurity mindset among employees is essential, as they play a significant role in safeguarding the network [61]. Additionally, financial institutions should establish robust incident response plans that outline clear steps to follow in the event of a security breach [62]. Regular security audits and penetration testing should also be conducted to identify vulnerabilities and ensure that security measures are up-to-date and effective [63]. By combining technological solutions with a culture of cybersecurity and proactive incident response strategies, the financial sector in Indonesia can significantly enhance its computer network security, minimizing vulnerabilities and strengthening overall resilience [63].

Recommendations for Policymakers and Stakeholders

To strengthen the cybersecurity posture of the financial industry in Indonesia, it is imperative to provide concrete recommendations for policymakers and stakeholders [8]. Firstly, policymakers should consider the development and implementation of comprehensive cybersecurity regulations and standards tailored specifically to the financial sector [7]. These regulations should encompass a wide range of security measures, including data encryption, incident reporting, and mandatory cybersecurity training for employees [9]. Clear and stringent penalties for non-compliance should be established to incentivize financial institutions to invest in cybersecurity [64]. Moreover, collaboration between the government and industry stakeholders should be encouraged to ensure that regulations remain up-to-date and aligned with emerging cyber threats [65].

Secondly, stakeholders, including financial institutions, industry associations, and cybersecurity experts, should prioritize information sharing and collaboration [1]. Establishing industry-specific Information Sharing and Analysis Centers (ISACs) can facilitate the exchange of threat intelligence and best practices among financial organizations [2]. Stakeholders should also engage in joint cybersecurity exercises and drills to enhance preparedness and response capabilities [3]. Furthermore, financial institutions should allocate adequate resources to cybersecurity, not only in terms of technology but also in employee training and awareness programs [4]. By fostering a culture of collaboration and shared responsibility among stakeholders and adhering to robust regulatory frameworks, the financial sector in Indonesia can collectively bolster its cybersecurity defenses and minimize the impact of digital security threats [6].

CONCLUSION

In conclusion, this literature review provides a comprehensive exploration of the challenges and solutions related to computer network security in the financial sector in Indonesia, amidst the backdrop of digital security threats. The rapid digitalization of financial services has brought both

opportunities and vulnerabilities, necessitating a robust cybersecurity framework. Challenges such as resource limitations, evolving cyber threats, and compliance complexities require a concerted effort from financial institutions, policymakers, and stakeholders. The adoption of advanced security technologies, a strong cybersecurity culture, and collaborative information sharing are vital strategies for enhancing network security. Recommendations for policymakers emphasize the importance of tailored regulations, while stakeholders should prioritize collaboration and resource allocation. Ultimately, this review underscores the critical role of cybersecurity in maintaining trust, safeguarding digital assets, and preserving the integrity of Indonesia's financial industry in an increasingly interconnected digital landscape.

REFERENCES

[1] P. P. Sugarda and M. R. Wicaksono, "ENHANCING THE COMPETITIVENESS OF INDONESIA'S FINANCIAL SERVICES SECTOR IN THE DIGITAL ERA THROUGH OPEN BANKING: LESSONS LEARNED FROM THE UK'S EXPERIENCE," *Journal of Central Banking Law and Institutions*, vol. 2, no. 1, pp. 153–178, 2023.

[2] S. Atkins and C. Lawson, "Cooperation amidst competition: cybersecurity partnership in the US financial services sector," *J Cybersecur*, vol. 7, no. 1, p. tyab024, 2021.

[3] A. I. Al-Alawi and M. S. A. Al-Bassam, "The significance of cybersecurity system in helping managing risk in banking and financial sector," *Journal of Xidian University*, vol. 14, no. 7, pp. 1523–1536, 2020.

[4] H. Muttaqin and K. Ramli, "Designing An Information Security Framework For The Indonesia Water Industry Sector," *Cakrawala Repositori IMWI*, vol. 6, no. 3, pp. 771–780, 2023.

[5] I. Harsono and I. A. P. Suprapti, "The Role of Fintech in Transforming Traditional Financial Services," *Accounting Studies and Tax Journal (COUNT)*, vol. 1, no. 1, pp. 81–91, 2024.

[6] M. Sidik, "Cyber Security Applied For Financial Sector In Indonesia," *Jurnal Pajak dan Bisnis (Journal of Tax and Business)*, vol. 1, no. 1, pp. 30–47, 2020.

[7] A. Muftiasa, L. A. Wibowo, and A. Rahayu, "Is intellectual capital related to telecommunications industry financial performance during COVID-19?," *International Journal of Learning and Intellectual Capital*, vol. 20, no. 1, pp. 29–46, 2023.

[8] N. Surantha, F. Ivan, and R. Chandra, "A case analysis for Kubernetes network security of financial service industry in Indonesia using zero trust model," *Bulletin of Electrical Engineering and Informatics*, vol. 12, no. 5, pp. 3134–3141, 2023.

[9] M. A. Kafi and N. Akter, "Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection," *American Journal of Trade and Policy*, vol. 10, no. 1, pp. 15–26, 2023.

[10] D. Riristuningsia, I. H. Wahyunadi, and I. Harsono, "Public Participation in Rural Development Planning," *Jurnal Ekonomi dan Studi Pembangunan*, vol. 9, no. 1, pp. 57–65, 2017.

[11] S. Vaithyasubramanian, A. Christy, and D. Saravanan, "Two factor authentications for secured login in support of effective information preservation and network security," *ARPN Journal of Engineering and Applied Sciences*, vol. 10, no. 5, pp. 2053–2056, 2015.

[12] I. HARSONO, "The Impact Of E-Money On Inflation In Indonesia," *Ganec Swara*, vol. 17, no. 3, pp. 1160–1164, 2023.

[13] M. A. Rahman, "Subduing Cyber Threats to Secure the Financial Sector of Bangladesh," *Cybersecurity, Privacy, & Networks eJournal*, vol. 2, no. 78, 2019.

[14] M. R. Islam and M. M. Rashid, "A Survey on Blockchain Security and Its Impact Analysis," in *2023 9th International Conference on Computer and Communication Engineering (ICCCE)*, IEEE, 2023, pp. 317–321.

[15] H. U. Khan, M. Z. Malik, S. Nazir, and F. Khan, "Utilizing bio metric system for enhancing cyber security in banking sector: a systematic analysis," *IEEE Access*, 2023.

[16] I. Harsono, "Determinants of Economic Growth, Poverty, and Unemployment: A Path Analysis Study," *Jurnal Ilmu Sosial dan Humaniora*, vol. 12, no. 2, pp. 359–366, 2023.

[17] S. Dambra, L. Bilge, and D. Balzarotti, "SoK: Cyber insurance–technical challenges and a system security roadmap," in *2020 IEEE Symposium on Security and Privacy (SP)*, IEEE, 2020, pp. 1367–1383.

[18] L. Judijanto, R. L. Rahardian, H. N. Muthmainah, and M. Erkamim, "Analysis of Threat Detection, Prevention Strategies, and Cyber Risk Management for Computer Network Security in Government Information Systems in Indonesia," *West Science Information System and Technology*, vol. 1, no. 02, pp. 90–98, 2023.

[19] D. Setyantoro, V. Afifah, R. A. Hasibuan, N. Aprilia, and N. P. Sari, "The WIRELESS COMPUTER NETWORK MANAGEMENT SECURITY ANALYSIS," *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, vol. 7, no. 2, pp. 105–110, 2022.

[20] S. Mishra, "Exploring the Impact of AI-Based Cyber Security Financial Sector Management," *Applied Sciences*, vol. 13, no. 10, p. 5875, 2023.

[21] A. Y. A. B. Ahmad, S. S. Kumari, S. MahabubBasha, S. K. Guha, A. Gehlot, and B. Pant, "Blockchain Implementation in Financial Sector and Cyber Security System," in *2023 International Conference on Artificial Intelligence and Smart Communication (AISC)*, IEEE, 2023, pp. 586–590.

[22] S. D. Rosadi, S. Yuniarti, and R. Fauzi, "Protection of Data Privacy in The Era of Artificial Intelligence in The Financial Sector in Indonesia," *Journal of Central Banking Law and Institutions*, vol. 1, no. 2, pp. 353–366, 2022.

[23] C. Alcaraz and J. Lopez, "Digital twin: A comprehensive survey of security threats," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1475–1503, 2022.

[24] B. Hammi, S. Zeadally, and J. Nebhen, "Security threats, countermeasures, and challenges of digital supply chains," *ACM Comput Surv*, 2023.

[25] H. M. Alzoubi *et al.*, "Cyber Security Threats on Digital Banking," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, IEEE, 2022, pp. 1–4.

[26] A. N. Alahmadi, S. U. Rehman, H. S. Alhazmi, D. G. Glynn, H. Shoaib, and P. Solé, "Cyber-Security Threats and Side-Channel Attacks for Digital Agriculture," *Sensors*, vol. 22, no. 9, p. 3520, 2022.

[27] J. Zhang, "Research on Information Security Threats and Defense Strategies of Smart Grid," in *E3S Web of Conferences*, EDP Sciences, 2020, p. 02003.

[28] M. A. Haque, S. Haque, K. Kumar, and N. K. Singh, "A comprehensive study of cyber security attacks, classification, and countermeasures in the internet of things," in *Handbook of research on digital transformation and challenges to data security and privacy*, IGI Global, 2021, pp. 63–90.

[29] J. Zhang, "Research on Information Security Threats and Defense Strategies of Smart Grid," in *E3S Web of Conferences*, EDP Sciences, 2020, p. 02003.

[30] S. El Kafhali, I. El Mir, and M. Hanini, "Security threats, defense mechanisms, challenges, and future directions in cloud computing," *Archives of Computational Methods in Engineering*, vol. 29, no. 1, pp. 223–246, 2022.

[31] M. Xue, C. Yuan, H. Wu, Y. Zhang, and W. Liu, "Machine learning security: Threats, countermeasures, and evaluations," *IEEE Access*, vol. 8, pp. 74720–74742, 2020.

[32] H. Muttaqin and K. Ramli, "Designing An Information Security Framework For The Indonesia Water Industry Sector," *Cakrawala Repositori IMWI*, vol. 6, no. 3, pp. 771–780, 2023.

[33] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks," *Information*, vol. 13, no. 9, p. 413, 2022.

[34] N. P. SINAGA, "Perlindungan Hukum Bagi Konsumen Yang Data Pribadinya Diperjualbelikan Di Aplikasi Fintech Peer-To-Peer Lending," 2021.

[35] K. Razikin and A. Widodo, "General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance," *CommIT (Communication and Information Technology) Journal*, vol. 15, no. 2, pp. 91–104, 2021.

[36] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity challenges in the maritime sector," *Network*, vol. 2, no. 1, pp. 123–138, 2022.

[37] V. Maphosa, "An overview of cybersecurity in Zimbabwe's financial services sector," *F1000Res*, vol. 12, p. 1251, 2023.

[38] T. Alquraan, A. Alqisie, and A. Al Shorafa, "Do behavioral finance factors influence stock investment decisions of individual investors?(Evidences from Saudi Stock Market)," *Am Int J Contemp Res*, vol. 6, no. 3, pp. 159–169, 2016.

[39] R. M. Permana, "Analysis of the Financial Performance of State-Owned Enterprises (SOEs) in the Mining Sector Listed on the Indonesia Stock Exchange in 2018-2022," *Indo-Fintech Intellectuals: Journal of Economics and Business*, vol. 3, no. 2, pp. 371–383, Sep. 2023, doi: 10.54373/ifijeb.v3i2.250.

[40] M. Makbul and M. Ismail, "KEBIJAKAN CYBER DEFEND INDONESIA DALAM RANGKA MENANGANI INTERNATIONAL CYBER THREATS," *Jurnal Yustitia*, vol. 23, no. 2, 2023.

[41] S. Sjamsoeddin, P. Yusgiantoro, H. J. R. Saragih, and B. S. Soepandji, "The Analysis of Civil-Military Cooperation in Implementation of Indonesia National Defense Policy," *Journal of Namibian Studies: History Politics Culture*, vol. 33, pp. 56–66, 2023.

[42] A. S. Rahim, P. Widodo, A. H. S. Reksoprodjo, and A. Alsodiq, "Identify Cyber Intelligence Threats in Indonesia," *International Journal Of Humanities Education and Social Sciences*, vol. 3, no. 1, 2023.

[43] A. Rizki and F. G. C. Timur, "SYNERGY OF MULTI-STAKEHOLDERS IN DEFENDING INDONESIA FROM CYBER THREATS," *Journal of Social Political Sciences*, vol. 2, no. 4, pp. 342–354, 2021.

[44] M. S. Rofii, "Strengthening digital ecosystems for sustainable development in Indonesia: anticipating cyber threats," in *IOP Conference Series: Earth and Environmental Science*, IOP Publishing, 2020, p. 012026.

[45] H. S. Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, and S. R. Cotten, "Understanding online safety behaviors: A protection motivation theory perspective," *Comput Secur*, vol. 59, pp. 138–150, 2016.

[46] R. Dwianto, H. W. Utama, F. D. Saputra, G. A. Wijaya, F. Aisyah, and E. Kartini, "Peran Otoritas Jasa Keuangan Dalam Menjaga Stabilitas dan Keamanan Sistem Keuangan," *Jurnal Ilmu Manajemen, Ekonomi dan Kewirausahaan*, vol. 3, no. 2, pp. 120–127, 2023.

[47] D. Maček, I. Magdalenić, and N. Ivković, "Risk Assessment of the Bank's Noncompliance with Payment Card Industry Data Security Standard," in *Information Systems Security: Central European Conference on Information and Intelligent Systems (CECIIS 2012)*, 2012, pp. 19–21.

[48] H. Eka, "Investment opportunity and industrial growth in Indonesia," *International journal of business and society*, vol. 19, no. 2, pp. 295–312, 2018.

[49] R. Mendelsohn and S. N. Seo, "Environmental and social safeguards framework," 2007.

[50] A. P. G. Putra, F. Humani, F. W. Zakiy, M. R. Shihab, and B. Ranti, "Maturity Assessment of Cyber Security in The Workforce Management Domain: A Case Study in Bank Indonesia," in *2020 International Conference on Information Technology Systems and Innovation (ICITSI)*, IEEE, 2020, pp. 89–94.

[51] R. Ganesen, A. A. Bakar, R. Ramli, F. A. Rahim, and M. N. A. Zawawi, "Cybersecurity Risk Assessment: Modeling Factors Associated with Higher Education Institutions," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, 2022.

[52] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," *PeerJ Comput Sci*, vol. 7, p. e703, 2021.

[53] A. Aliyu *et al.*, "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," *Applied Sciences*, vol. 10, no. 10, p. 3660, 2020.

[54] L. Oliveira *et al.*, "Assessing Cybersecurity Hygiene and Cyber Threats Awareness in the Campus-A Case Study of Higher Education Institutions in Portugal and Poland," in *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, IEEE, 2023, pp. 168–173.

[55] O. P. Onyia and J. Tuyon, "Disruptions, innovations and transformations in the global financial services market: the impacts of emerging cybersecurity, geopolitical and sustainability risks," *Journal of Financial Services Marketing*, pp. 1–4, 2023.

[56] K. Lampropoulos *et al.*, "White paper on cybersecurity in the healthcare sector. The HEIR solution," *arXiv preprint arXiv:2310.10139*, 2023.

[57] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput Secur*, vol. 105, p. 102248, 2021.

[58] I. Mustapha, Y. Vaicondam, A. Jahanzeb, B. A. Usmanovich, and S. H. B. Yusof, "Cybersecurity Challenges and Solutions in the Fintech Mobile App Ecosystem.," *International Journal of Interactive Mobile Technologies*, vol. 17, no. 22, 2023.

[59] H. Muttaqin and K. Ramli, "Designing An Information Security Framework For The Indonesia Water Industry Sector," *Cakrawala Repositori IMWI*, vol. 6, no. 3, pp. 771–780, 2023.

[60] H. Muttaqin and K. Ramli, "Designing An Information Security Framework For The Indonesia Water Industry Sector," *Cakrawala Repositori IMWI*, vol. 6, no. 3, pp. 771–780, 2023.

[61] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks," *Information*, vol. 13, no. 9, p. 413, 2022.

[62] K. Razikin and A. Widodo, "General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance," *CommIT (Communication and Information Technology) Journal*, vol. 15, no. 2, pp. 91–104, 2021.

[63] N. P. SINAGA, "Perlindungan Hukum Bagi Konsumen Yang Data Pribadinya Diperjualbelikan Di Aplikasi Fintech Peer-To-Peer Lending," 2021.

[64] D. M. A. Putri, S. T. Cantika, R. C. Ningtyas, and F. M. Leon, "Determining Factors in the Indirect Financial Distress Cost in Companies in the Basic and Chemical Industry Sector Listed on the Indonesia Stock Exchange".

[65] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks," *Information*, vol. 13, no. 9, p. 413, 2022.