SMATIKA : STIKI Informatika Jurnal
Accredited Sinta 4 Ministry of Higher Education, Science and Technology Republic of Indonesia SK No. 79/E/KPT/2023
E-ISSN: 2580-6939 || P-ISSN: 2087-0256

The Cyber Threat Landscape in Indonesia: Attacks and Security System Analysis

Hendi Sama[1*] , Stefanie[2] , Stefanus Eko Prasetyo[3]

[1,2,3]Universitas Internasional Batam, Faculty of Computer Science, Department of Informatics, BataJalan Gajah Mada, Baloi–Sei Ladi, Batam 29442, Riau Islands, Indonesia.

Keyword

cyber awareness; Cybersecurity; learning systems; risk assessment; security perception,

Corresponding Author:
hendi@uib.ac.id

Abstract

Cybersecurity in learning systems has become increasingly important as educational institutions rely more heavily on digital platforms such as learning management systems, online assessments, and cloud-based academic services. This rapid digital transformation exposes learning environments to sophisticated cyber threats that may disrupt academic activities and compromise sensitive information. However, many institutions still lack a clear understanding of how users perceive cyber risks and how these perceptions influence the effectiveness of cybersecurity systems. Currently, there is a significant research gap regarding empirical evidence that links user behavioral psychology with technical security outcomes in the Indonesian educational context. This study aims to empirically analyze the relationship between cyber awareness, perceived impact of cyber attacks, and perceived effectiveness of cybersecurity systems in digital learning environments. A quantitative research approach was applied using data collected from 402 respondents. The data were analyzed through descriptive statistics, correlation analysis, regression analysis, and group comparison tests to examine variable relationships and demographic differences. The findings indicate that cyber awareness significantly and positively predicts perceived system effectiveness ($\beta = 0.501$, $p < 0.001$), demonstrating that higher awareness levels enhance overall cybersecurity performance. Conversely, the perceived impact of cyber attacks does not show a significant effect on system effectiveness, suggesting that awareness is more influential than threat perception alone. Additional results reveal gender-based differences in cyber incident experiences, while awareness levels remain similar. The practical implications emphasize the importance of cybersecurity awareness programs, digital safety education, and proactive defense strategies to strengthen protection in learning systems and improve institutional cybersecurity readiness.

Cite: Sama, H., et al., (2026). The Cyber Threat Landscape in Indonesia: Attacks and Security System Analysis.. SMATIKA : STIKI Informatika Jurnal,16(1). doi: https://doi.org/10.32664/smatika.v16i01.2200

1. Introduction

The rapid expansion of internet-connected devices has shifted cybercrime into one of the most prevalent threats in the modern digital era [1]. This evolution forces organizations to protect the three fundamental pillars of cybersecurity: confidentiality, integrity, and availability [2]. Despite these goals, individuals remain highly susceptible to phishing and account takeover due to a lack of security awareness [3]. Consequently, understanding attacker behavior and identifying attack vectors have become essential for effective mitigation [4]. In Indonesia, this risk is exacerbated by the widespread use of digital services and web applications that often lack robust security measures [5]. Hackers frequently exploit these vulnerabilities, using sophisticated algorithms to breach authentication mechanisms for economic gain [6].

The urgency for advanced security is reflected in the growing threat landscape across Indonesia's critical sectors [7] While cybercrime has expanded to include diverse offenses such as cyberstalking and unauthorized system intrusions [8] the COVID-19 pandemic further accelerated these risks by forcing a global shift to remote work and online transactions [9]. In Indonesia, the banking sector faces increasing risks from identity theft, payment fraud, phishing, and account takeover attacks. Criminals exploit vulnerabilities in online payment systems, mobile banking applications, and digital authentication processes to obtain financial and personal information [10] These incidents underscore the need for stronger fraud detection tools, secure authentication protocols, and user awareness programs.

At a national level, Indonesia is particularly vulnerable due to its large digital population. Internet users increased from approximately 2 million in 2000 to over 171 million by 2019, highlighting rapid digital penetration [11]. For instance, Indonesia has ranked among the most affected countries in global malware and worm attacks, such as Stuxnet, and has experienced multiple cases of government system infiltration and data breaches [11]. The increasing number of cyber threats highlights the critical importance of robust cybersecurity measures across sectors—particularly in banking, government systems, telecommunications, and essential services. As both state and non-state actors can launch cyber operations, detecting perpetrators in cyberspace remains challenging due to its borderless nature.[12] Technical implementations, such as the use of AES-128 encryption and biometric authentication, also contribute to the overall resilience of data security systems.

Problem Formulation & Research Question Despite the high frequency of attacks and the rapid growth of Indonesia’s digital population, there remains a critical gap in empirical research that specifically links user behavioral psychology with the actual effectiveness of security systems. Most studies focus on technical vulnerabilities, yet the human element—specifically how user awareness and risk perception influence system resilience in Indonesia's digital learning environments—is often overlooked. To address this gap, this study seeks to answer the following research question: To what extent do cyber awareness and user security perceptions influence the perceived effectiveness of cybersecurity systems in Indonesia's digital learning environments? This research provides a significant scientific contribution by offering an empirical framework that specifically links user psychology with cybersecurity resilience in the Indonesian educational context. By shifting the focus from purely technical infrastructure to human-centric factors, this study provides actionable insights for academic institutions to develop socio-technical governance strategies that prioritize digital literacy as a primary defense mechanism.

2. Research Method

2.1 Research Design

This study uses a quantitative descriptive design to analyze the cyber threat landscape in Indonesia. The research combines secondary data from cybersecurity reports, government publications, and academic studies, along with primary survey data collected from cybersecurity professionals in key sectors such as banking, e-commerce, and healthcare. [13] The cross-sectional approach enables the evaluation of current cyber threats and the effectiveness of cybersecurity measures at a specific point in time.[14]

2.2 Participants and Sampling Method

Participants were selected using convenience sampling due to accessibility and relevance to the research focus. Respondents included IT managers, cybersecurity officers, and network administrators. [15] The

sample size was determined using the Slovin formula with a 5% margin of error, resulting in approximately 400 participants to ensure statistical reliability and representation.

This study acknowledges several sampling limitations. The use of convenience sampling may introduce potential bias, as respondents were selected based on their accessibility within specific professional networks. This could result in a sample that is more technologically proficient than the general population, potentially overestimating the average level of cyber awareness. However, to mitigate this, the study strictly targeted IT managers and security officers who are directly responsible for institutional security, ensuring that the findings remain relevant to the research objectives.

2.2 Data Collection

Data were collected through two sources:

1. Secondary Data — Reports from cybersecurity firms (Symantec, Kaspersky), the National Cyber and Encryption Agency of Indonesia (BSSN), and academic literature to gain insights into attack trends.

2. Primary Data — A structured survey was distributed to 406 respondents, focusing on cybersecurity experts and IT managers in the banking and healthcare sectors. To ensure construct alignment with the research objectives, sample items from the survey included: "I am confident in my ability to identify phishing attempts" for the Cyber Awareness construct (Q6–Q10) and "The current security measures effectively mitigate potential data breaches" for the Effectiveness construct (Q16–Q20). A structured survey was distributed to 400 respondents. To ensure construct alignment with the research objectives, sample items from the survey included: 'I am confident in my ability to identify phishing attempts' for the Cyber Awareness construct (Q6–Q10) and 'The current security measures effectively mitigate potential data breaches' for the Effectiveness construct (Q16–Q20).

2.3 Data Analysis

Quantitative data were processed using descriptive and inferential statistics. This study follows a confirmatory research approach to test the relationships between cybersecurity awareness and system effectiveness. To ensure the reliability of the research instrument, internal consistency was validated using Cronbach's alpha, where all constructs achieved a score above 0.87, indicating high reliability. Furthermore, factor analysis was conducted to confirm the underlying structure of the variables before performing correlation and regression analysis.

Correlation and regression analysis are theoretically appropriate for this study to determine the strength and direction of relationships between behavioral predictors and system outcomes. Variables were operationalized by measuring Cyber Awareness through self-efficacy items and System Effectiveness through perceived resilience metrics, allowing for a quantitative test of the research hypotheses in a confirmatory approach. Quantitative data were processed using descriptive statistics (frequency, percentage, mean) to summarize trends in cyber threats and cybersecurity practices. Inferential statistics, including Chi-Square tests and correlation analysis, were applied to examine relationships between variables such as cybersecurity readiness and incident frequency.[16][17]

2.4 Ethical Considerations

All participants provided informed consent. Data confidentiality and anonymity were ensured, and all collected data were securely stored in compliance with ethical research standards.

2.5 Research Procedure

This study was conducted through several systematic stages to analyze the cyber threat landscape in Indonesia. First, a literature review was performed to examine previous research related to cybersecurity threats, attack patterns, and security system strategies in digital environments, particularly within the Indonesian context. Based on insights from the literature, a methodology design was developed to structure the research process, including the selection of analytical approaches and data sources relevant to cyber threat assessment. The data collection stage involved gathering cybersecurity incident reports, publicly available threat intelligence data, and documentation from relevant cybersecurity agencies and reports. For the sampling stage, selected cyber incidents and threat reports were chosen based on their relevance to major cyberattack categories and their occurrence within the Indonesian digital ecosystem. Subsequently, data analysis was conducted using qualitative and descriptive analytical techniques to identify patterns of cyberattacks, common vulnerabilities, and the effectiveness of existing security systems. The findings were then discussed through result interpretation, focusing on how the identified attack trends reflect the evolving cybersecurity challenges in Indonesia and how current security frameworks respond to these threats. Finally, the study also includes the identification of limitations, acknowledging potential constraints such as limited access to confidential cybersecurity data, reliance on publicly reported incidents, and the dynamic nature of cyber threats that may change rapidly over time.

3. Result and Discussions

This section presents the results of the study and discusses the findings in relation to the research objectives and existing literature. All results are presented to improve readers' understanding of the cyber threat landscape in Indonesia through measurable indicators. A total of 406 responses were collected, and 402 valid responses remained after data cleaning. These data formed the basis of all analyses in this chapter.

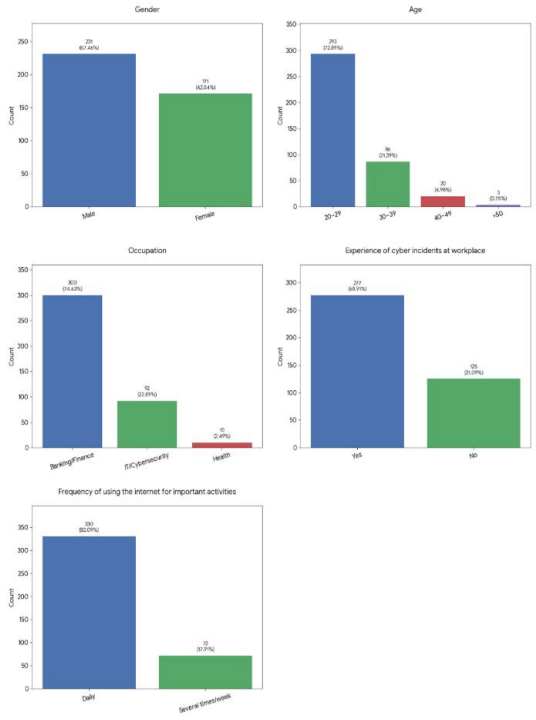

Figure 1 . Demographic Profile of Respondents (n = 402)

- Gender: 57.46% male, 42.54% female
- Age: 72.89% aged 20–29
- Sector: 74.63% Banking/Finance, 22.89% IT/Cybersecurity, 2.49% Health
- Experienced workplace cyber incidents: 68.91% yes
- Daily use of the internet for essential tasks: 82.09%

Most respondents are young adults who actively use digital platforms and work in sectors with high cybersecurity exposure. The high percentage of respondents who experienced cyber incidents demonstrates the urgency of cybersecurity preparedness in Indonesian organizations.

Table 1 . Summary of Descriptive Statistics

Variable	Survey Items	Mean	Standard Deviation	Interpretation
Cyber Awareness	Q6 – Q10	3.46	0.8	Moderate
Impact of Cyber Attacks	Q11 – Q15	4.60	0.71	High
Effectiveness of Cybersecurity Systems	Q16 – Q20	3.36	0.84	Moderate

Cyber awareness is moderate, indicating room for improvement. The perceived impact of cyber attacks is very high, showing strong recognition of risks. Perceived system effectiveness is only moderate, suggesting a gap between threat levels and preparedness.

Table 2 . Correlation Matrix for Awareness, Impact, and Effectiveness Constructs

Relationship	**Correlation Coefficient**	**Significnance**	**Interpretation**
Awareness ↔ Effectiveness	0.501	$p < 0.001$	Significant positive correlation
Awareness ↔ Impact	0.042	Not significant	No meaningful relationship
Impact ↔ Effectiveness	-0.068	Not significant	No meaningful relationship

Cyber awareness is significantly associated with perceived system effectiveness. However, awareness and impact, as well as impact and effectiveness, show no meaningful relationship. A linear regression was performed to determine predictors of perceived cybersecurity effectiveness.

Table 3 . Regression Analysis Summary

Predictor Variable	Beta (β)	t-value	p-value	Significance
Cyber Awareness	0.501	6.124	< 0.001	Significance
Perceived Impact	-0.068	-0.832	0.406	Not Significant

$R^2 = 0.253$, $F(2,399) = 67.45$, $p < 0.001$

The coefficient of determination R^2 was calculated to measure the proportion of variance in cybersecurity effectiveness that can be explained by the independent variables. A higher R^2 value indicates a stronger explanatory power of the model, signifying that factors such as user awareness and risk perception are critical predictors of overall system resilience.

Cyber awareness significantly predicts perceived effectiveness, while perceived impact does not. Increasing awareness can directly enhance overall cybersecurity perceptions. Respondents show good awareness of cyber threats and clearly recognize the severe impact that cyber-attacks can have on individuals and organizations. Cyber awareness is moderately correlated with the perceived effectiveness of cybersecurity systems, indicating that respondents who are more aware tend to view their security systems as more effective. Male respondents reported experiencing more cyber incidents than female respondents; however, there is no significant difference in overall awareness levels between genders. Cyber awareness significantly predicts the perceived effectiveness of cybersecurity systems, while the perceived impact of cyber-attacks does not.

The regression results confirm that cyber awareness plays a significant role in predicting perceived system effectiveness ($\beta = 0.501$, $p < 0.001$). In contrast, the perceived impact of cyber-attacks does not contribute significantly. This suggests that improving user awareness directly enhances perceptions of cybersecurity

effectiveness, highlighting the importance of continuous training and structured awareness programs.

This study highlights the important role of user-related factors in strengthening cybersecurity effectiveness within learning systems. The findings show that cyber awareness has a significant and positive influence on the perceived effectiveness of cybersecurity systems ($\beta = 0.501$, $p < 0.001$). This result indicates that users who understand basic cybersecurity principles, such as safe password practices, phishing awareness, and data protection, tend to perceive institutional security systems as more effective. This finding is consistent with previous studies which emphasize that human awareness is a critical component of cybersecurity readiness, particularly in digital learning and organizational environments [6], [7].

The descriptive analysis reveals that respondents generally demonstrate a moderate level of cyber awareness. This suggests that although users are familiar with common cyber risks, continuous education and structured awareness programs are still required. Similar conclusions were reported by earlier studies, which found that insufficient user awareness remains one of the main contributors to system vulnerabilities despite the presence of technical security controls [8], [9]. These results reinforce the argument that cybersecurity effectiveness cannot rely solely on technological solutions but must be supported by user-oriented strategies.

Interestingly, the perceived impact of cyber attacks does not significantly affect the perceived effectiveness of cybersecurity systems. This finding implies that users' fear or perception of attack severity alone does not necessarily translate into confidence in system security. This result differs from some prior research suggesting that higher perceived threat levels encourage protective behavior [10]. The discrepancy may be influenced by contextual factors, such as users' trust in institutional security mechanisms or limited understanding of how cyber incidents directly affect system performance.

Furthermore, gender-based analysis shows differences in cyber incident experiences, where male respondents report higher exposure to cyber incidents. However, cyber awareness levels remain relatively similar across genders. This finding aligns with previous research indicating that exposure to cyber risks does not automatically lead to higher awareness or better security behavior [14]. Therefore, cybersecurity awareness initiatives should be designed inclusively, rather than being based solely on demographic exposure.

Overall, the discussion confirms that improving cyber awareness through continuous training, digital literacy programs, and policy enforcement is essential for enhancing cybersecurity effectiveness in learning systems. Integrating awareness initiatives with technical safeguards can significantly improve institutional resilience against evolving cyber threats. The Coefficient of Determination R^2 further supports the statistical robustness of this study's model. The R^2 value reflects the proportion of variance in the perceived effectiveness of cybersecurity systems that can be explained by cyber awareness and user perception. A significant R^2 indicates that human-centric variables are strong predictors of security success, confirming that technical infrastructure alone cannot guarantee system resilience without high user literacy.

Furthermore, this study provides critical institutional policy implications. Organizations should shift to a 'human-centric' governance framework by mandating periodic cybersecurity audits for user competency and mandatory training programs. Since awareness is a primary driver of effectiveness ($\beta = 0.501$), budget allocations should be balanced between hardware upgrades and continuous digital literacy initiatives to build a sustainable cybersecurity culture.

The impact of cyber-attacks was perceived as high (mean = 4.60), suggesting that respondents clearly recognize the severe consequences of cyber incidents, including financial loss, data leakage, and reputational damage. Likewise, [11] emphasized that recognizing the seriousness of cyber threats motivates institutions to adopt technologies such as blockchain and artificial intelligence for defense. However, [18] provided a different perspective by arguing that the psychological impact of disinformation and misinformation attacks is often underestimated, meaning that some forms of cyber threats may not be perceived as "severe" even though their social consequences are significant. This contrast suggests that perceptions of impact may vary depending on the threat type and its visibility.[19]The perceived effectiveness of cybersecurity systems was relatively low (mean = 3.36). This implies that although respondents acknowledge the importance of cybersecurity, they are not fully confident in their organizations' defense mechanisms. These findings which noted that many institutions—especially in developing countries—face structural and financial barriers in implementing comprehensive cybersecurity systems. In contrast,[20] proposed that advanced access control models and integrated cyber–physical–social policies can significantly enhance security reliability, implying that Indonesia's moderate perception of effectiveness may stem from the absence of such sophisticated

systems. Furthermore, [21] argued that adopting predictive and preventive frameworks (such as blockchain and AI-based anomaly detection) can transform cybersecurity from reactive to proactive—a capability still developing in Indonesia's context.

The correlation analysis further shows a moderate positive relationship between cyber awareness and perceived system effectiveness ($r = 0.501$, $p < 0.001$). This finding supports [5] , who found that improved awareness correlates with better cybersecurity performance in organizational environments. Similarly, [22] found that awareness and training increase the accuracy of cyber threat assessments even in "storyless" systems without prior incident data. Conversely. Furthermore, the integration of technical measures such as AES-128 encryption and biometric authentication remains a relevant strategy in modern digital security systems. [23] This study provides a significant scientific contribution by empirically establishing that human-centric factors, specifically cyber awareness, are more critical predictors of cybersecurity system effectiveness than the perceived severity of attacks. With a significant influence ($\beta = 0.501$) and a robust R2 value, this research confirms that institutional security resilience in Indonesia's digital learning environments depends heavily on user literacy rather than just technical safeguards.

4. Conclusions and Future Works

The perceived effectiveness of cybersecurity systems was found to be relatively low, indicating that although respondents recognize the importance of cybersecurity, they are not fully confident in their organizations' defense mechanisms. This finding is consistent with previous studies highlighting that many institutions, particularly in developing countries, encounter structural and financial constraints that limit the implementation of comprehensive cybersecurity systems. In contrast, prior research has suggested that the adoption of advanced access control models and the integration of cyber–physical–social security policies can substantially enhance system reliability. This implies that the moderate perception of cybersecurity effectiveness in Indonesia may be attributed to the limited implementation of such sophisticated security frameworks. Furthermore, other studies have emphasized that predictive and preventive approaches, including blockchain-based solutions and artificial intelligence–driven anomaly detection, can transform cybersecurity from a reactive to a proactive approach—capabilities that are still in the developmental stage within the Indonesian context.

The correlation analysis indicates a positive relationship between cyber awareness and the perceived effectiveness of cybersecurity systems. This finding supports earlier research demonstrating that higher levels of user awareness are associated with improved cybersecurity performance in organizational environments. Similarly, previous studies have shown that awareness and training initiatives enhance the accuracy of cyber threat assessment, even in systems that lack prior incident data. Conversely, some researchers have argued that awareness alone is insufficient without strong enforcement of security policies and continuous monitoring, suggesting that effective cybersecurity requires the coexistence of human awareness and robust technical measures such as encryption mechanisms and biometric authentication remains a relevant strategy in strengthening modern digital security systems.

This study makes a significant scientific contribution by empirically demonstrating that human-centric factors, particularly cyber awareness, play a more critical role in determining cybersecurity system effectiveness than the perceived severity of cyberattacks. The findings indicate that institutional cybersecurity resilience in Indonesia's digital learning environments depends heavily on user literacy rather than solely on technical safeguards. This perspective shifts the cybersecurity discourse from a purely technological focus toward a balanced socio-technical approach.

Despite these contributions, several limitations must be acknowledged. First, the reliance on self-reported perceptions may introduce subjectivity and social desirability bias, as respondents may overestimate their level of awareness. Second, the cross-sectional design captures user perceptions at a single point in time and does not reflect how security behaviors evolve alongside rapidly changing cyber threats. Finally, the study primarily focuses on individual perceptions, which may overlook the influence of organizational security maturity and governance frameworks. To address these limitations, future research should adopt longitudinal designs to observe behavioral changes over time.

Additionally, incorporating organizational-level variables, such as security governance maturity and policy enforcement, would provide a more comprehensive understanding of cybersecurity effectiveness. Employing mixed-method approaches, including qualitative interviews and technical vulnerability assessments, would

also offer deeper insights beyond those obtainable through quantitative surveys alone.

5. References

[1] O. Goni, "Cyber Crime and Its Classification," *Int. J. Electron. Eng. Appl.*, vol. 10, no. 2, 2021, doi: 10.30696/ijeea.x.i.2022.01-17.

[2] C. Whelan and D. Harkin, "Civilianising specialist units: Reflections on the policing of cyber-crime," *Criminol. Crim. Justice*, vol. 21, no. 4, 2021, doi: 10.1177/1748895819874866.

[3] T. T. Nguyen and V. J. Reddi, "Deep Reinforcement Learning for Cyber Security," *IEEE Trans. Neural Networks Learn. Syst.*, vol. 34, no. 8, 2023, doi: 10.1109/TNNLS.2021.3121870.

[4] T. Tan, H. Sama, T. Wibowo, G. Wijaya, and O. E. Aboagye, "Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam Cybersecurity Awareness among University Students in Batam City," *J. Teknol. dan Inf.*, vol. 14, 2024, doi: 10.34010/jati.v14i2.

[5] A. Bilen and A. B. Özer, "Cyber-attack method and perpetrator prediction using machine learning algorithms," *PeerJ Comput. Sci.*, vol. 7, 2021, doi: 10.7717/PEERJ-CS.475.

[6] S. E. Prasetyo, H. Haeruddin, and K. Ariesryo, "Website Security System from Denial of Service attacks, SQL Injection, Cross Site Scripting using Web Application Firewall," *Antivirus J. Ilm. Tek. Inform.*, vol. 18, no. 1, pp. 27–36, May 2024, doi: 10.35457/antivirus.v18i1.3339.

[7] W. Robert, A. Sunday, and F. U. O Y E Journal, "F U O Y E Journal of Criminology and Security Studies (IJCSS) CYBERCRIME AND ITS IMPLICATIONS FOR HUMAN CAPITAL DEVELOPMENT: A STUDY OF OTUOKE COMMUNITY, FUO STUDENTS," Online, 2024.

[8] D. A. Marelino, "Understanding the Types of Cyber Crime and Its Prevention," *Math. Stat. Eng. Appl.*, vol. 71, no. 1, 2022, doi: 10.17762/msea.v71i1.50.

[9] O. Goni, Md. Haidar Ali, Showrov, Md. Mahbub Alam, and Md. Abu Shameem, "The Basic Concept of Cyber Crime," *J. Technol. Innov. Energy*, vol. 1, no. 2, 2022, doi: 10.56556/jtie.v1i2.113.

[10] A. Rachh, "Spatial and temporal analysis of cyber-crime cases in India," *Lett. Spat. Resour. Sci.*, vol. 17, no. 1, 2024, doi: 10.1007/s12076-023-00360-w.

[11] A. B. I. For. Oluwatoyin Ajoke FarREVOLUTIONIZING BANKING SECURITY: INTEGRATING ARTIFICIAL INTELLIGENCE, BLOCKCHAIN, "ENHANCED CYBERSECURITY," *Financ. Account. Res. J.*, vol. 6, no. 4, pp. 501–514, Apr. 2024, doi: 10.51594/farj.v6i4.990.

[12] N. N. Cele and S. Kwenda, "Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review," 2024, *Emerald Publishing*. doi: 10.1108/JFC-10-2023-0263.

[13] G. Sakellariou, P. Fouliras, I. Mavridis, and P. Sarigiannidis, "A Reference Model for Cyber Threat Intelligence (CTI) Systems," *Electron.*, vol. 11, no. 9, 2022, doi: 10.3390/electronics11091401.

[14] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," 2024. doi: 10.1016/j.csa.2023.100031.

[15] T. N. Nguyen, H. Chi, M. City, and V. Correspondence, "A review of cyber crime," *J. Soc. Rev. Dev.*, vol. 2, no. 1, 2023.

[16] E. Irshad and A. Basit Siddiqui, "Cyber threat attribution using unstructured reports in cyber threat intelligence," *Egypt. Informatics J.*, vol. 24, no. 1, 2023, doi: 10.1016/j.eij.2022.11.001.

[17] Md. Asaad Raza, "Cyber Security and Data Privacy in the Era of E-Governance," *Soc. Sci. J. Adv. Res.*, vol. 4, no. 1, 2024, doi: 10.54741/ssjar.4.1.2.

[18] K. M. Caramancion, Y. Li, E. Dubois, and E. S. Jung, "The Missing Case of Disinformation from the

Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats," *Data*, vol. 7, no. 4, 2022, doi: 10.3390/data7040049.

[19] D. P. Saputri, Surryanto D. W., and Helda Risman, "The Indonesian Cyber Diplomacy: ASEAN-Japan Online Cyber Exercise," *Tech. Soc. Sci. J.*, vol. 9, 2020, doi: 10.47577/tssj.v9i1.911.

[20] Y. Cao, C. Ke, D. Fan, Y. Ping, Q. Yang, and M. K. Yao, "State-aware access control for cyber-physical-social space: Model and policy security assurance," *Egypt. Informatics J.*, vol. 31, Sep. 2025, doi: 10.1016/j.eij.2025.100749.

[21] N. Tatipatri and S. L. Arun, "A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security," *IEEE Access*, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3361039.

[22] P. H. Meland, D. A. Nesheim, K. Bernsmed, and G. Sindre, "Assessing cyber threats for storyless systems," *J. Inf. Secur. Appl.*, vol. 64, 2022, doi: 10.1016/j.jisa.2021.103050.

[23] H. H. Amirullah, A. Eviyanti, and S. Sumarno, "Aplikasi Keamanan Berkas dengan Enkripsi AES dan Biometrik Sidik Jari Berbasis Android," *SMATIKA J.*, vol. 14, no. 01, pp. 23–32, Jun. 2024, doi: 10.32664/smatika.v14i01.1130.