





Challenges in Securing Data and Networks from Modern Cyber Threats

Irma Shantilawati¹ , Jihan Zanubiya^{2*} , Fajriannoor Fanani³ , Henrik Jensen⁴, Shofiyul Millah⁵ ,

Ninda Lutfiani⁶ 

¹Department of Management, Ichsan Satya University, Indonesia

²Department of Digital Business, CAI Sejahtera Indonesia, Indonesia

³Department of Communication, University of Semarang, Indonesia

⁴Department of Computer System, Rey Incorporation, USA

⁵Department of Digital Business, University of Raharja, Indonesia

⁶Association of Higher Education Informatics and Computers, Indonesia

¹irmashan.uis@gmail.com, ²jihan.zanubiya@raharja.info, ³fajrian@usm.ac.id, ⁴henrik@rey.zone, ⁵shofiyul@raharja.info,

⁶ninda@raharja.info

*Corresponding Author

Article Info

Article history:

Submission July 20, 2024

Revised August 12, 2024

Accepted September 20, 2024

Published October 6, 2024

Keywords:

Cybersecurity

Challenge

Cyber Threats

Network Security

Threat Detection



ABSTRACT

In the era of digital transformation, organizations face an increasing range of cyber threats that directly target data and network security. This study addresses the core challenges organizations encounter in safeguarding sensitive information and network infrastructure against sophisticated cyberattacks, including ransomware, phishing, and advanced persistent threats. **Through a mixed method** approach combining surveys and case studies, this research provides a unique perspective on the current cyber threat landscape, emphasizing the growing gap in cybersecurity skills, network architecture complexity, and the rapid evolution of cyber threats. **The findings** highlight critical obstacles, such as a shortage of qualified cybersecurity professionals and the technical challenges posed by integrating IoT and cloud services in secure networks. **The practical implications** extend to specific sectors like healthcare and finance, where enhanced resilience against cyber threats is paramount. **This study** concludes by recommending advanced security solutions, including Artificial Intelligence (AI) driven threat detection and zero trust models, to bolster organizational resilience and ensure regulatory compliance.

This is an open access article under the [CC BY 4.0](https://creativecommons.org/licenses/by/4.0/) license.



DOI: <https://doi.org/10.34306/ijcitsm.v4i2.160>

This is an open-access article under the CC-BY license (<https://creativecommons.org/licenses/by/4.0/>)

©Authors retain all copyrights

1. INTRODUCTION

In the digital transformation era, organizations increasingly rely on interconnected systems and data driven operations, placing a premium on robust cybersecurity measures [1]. However, this reliance has made organizational networks and sensitive data prime targets for a range of sophisticated cyber threats, such as ransomware, phishing, Distributed Denial of Service (DDoS) attacks, and zero day exploits. These threats pose a significant risk not only to data confidentiality, integrity, and availability but also to operational continuity and regulatory compliance [2]. Despite significant research and technological advancements, a comprehensive

understanding of the challenges faced by modern organizations in securing their data and networks remains limited. Existing studies often focus on individual types of threats or technical solutions, overlooking the broader, multifaceted nature of cybersecurity challenges [3]. In particular, gaps in knowledge about the complexities of defending against rapidly evolving cyber threats, shortages of skilled cybersecurity personnel, and the increasing technical requirements of managing decentralized, cloud integrated networks remain largely unexplored. This study aims to address these gaps by offering an integrated approach that combines technical and organizational perspectives, setting it apart from previous research [4]. To achieve this goal, the study employs a mixed method approach, including surveys and case studies, to analyze the obstacles organizations face in strengthening their cyber security resilience. This approach is particularly relevant for sectors such as healthcare and finance, where data protection is critical, and the impact of security breaches can be catastrophic. Additionally, this research explores emerging solutions such as Artificial Intelligence (AI) driven threat detection and zero trust architectures that show promise in enhancing cybersecurity defenses against evolving threats [5]. By identifying and analyzing the primary challenges and effective practices in cybersecurity, this study seeks to contribute to a more secure digital landscape, equipping organizations with actionable strategies to mitigate risks. The outcomes provide insight into the technical and human factors affecting cybersecurity resilience, highlighting the practical implications of adopting advanced security models to support organizational growth in a secure, compliant, and resilient manner [6].

2. LITERATURE REVIEW

The modern cyber threat landscape has evolved significantly, with attackers leveraging increasingly sophisticated techniques and exploiting a wide range of vulnerabilities within organizational systems [7]. Among the most prevalent cyber threats today are malware, ransomware, Distributed DDoS attacks, and phishing, all of which have grown more intricate, often employing automation, machine learning, and other advanced technologies to bypass traditional security measures [8]. Malware has progressed from simple viruses to complex forms capable of stealing data, encrypting files for ransom, or establishing backdoor access within networks. Current strains of malware use advanced evasion techniques, such as polymorphism, where the code changes slightly with each execution to avoid detection by standard antivirus programs [9].

Ransomware has also become a leading threat, shifting from individual users to large organizations and public institutions. This evolution is evident in high profile variants like WannaCry and NotPetya, which caused extensive disruptions and significant financial losses globally. These attacks underscore the impact on critical sectors, with healthcare and financial institutions being especially vulnerable due to the sensitivity and value of their data [10]. DDoS Attacks have also grown in frequency and scale, overwhelming servers or networks with traffic and causing extensive downtime for businesses. The rise of botnets has enabled attackers to conduct DDoS attacks using vast networks of infected devices, making mitigation efforts more challenging. Financial sectors often face such attacks as they can disrupt services, leading to direct financial losses [11].

Phishing has evolved from mass email scams to highly targeted spear phishing campaigns that impersonate trusted entities to gain sensitive information or install malicious software. Phishing remains one of the primary causes of security breaches, particularly when combined with social engineering tactics, affecting industries that rely heavily on sensitive client information, such as banking and healthcare [12]. The impact of these threats is profound, leading to financial losses, reputational damage, and legal liabilities. As threats evolve, organizations must adopt more advanced security strategies to protect against these increasingly complex attacks [13].

2.1. Data and Network Security Practices

Organizations have historically relied on traditional security practices like firewalls, encryption, and Intrusion Detection Systems (IDS) to counter rising cyber threats [14].

- Firewalls act as a barrier between internal and external networks. While traditional firewalls filtered traffic based on predefined rules, Next Generation Firewalls (NGFW) now incorporate features like deep packet inspection, application layer filtering, and threat intelligence integration for more robust security [15].
 - Encryption is a foundational practice, protecting data in transit and at rest. However, managing encryption keys and detecting encrypted malicious traffic pose ongoing challenges. For example, financial
-

services rely on encryption to secure transactions but face additional complexity due to regulatory requirements [16].

- IDS monitor network traffic for suspicious activity. Signature based IDS detect known attack patterns, while anomaly based IDS identify deviations from normal activity. However, IDS is often reactive and can generate false positives, which require further analysis by security teams [17].

In addition to these practices, organizations are increasingly adopting modern security models like Multi Factor Authentication (MFA), zero trust architectures, and AI driven threat detection [18]. These solutions address the complexity of modern cyber threats by requiring multiple forms of verification, assuming no user or device is trusted by default, and using AI to predict and detect anomalies. For instance, zero trust architectures have become essential in healthcare and finance, where securing each endpoint and user access is critical [19].

2.2. Challenges in Cybersecurity

Despite the adoption of advanced security measures, organizations face numerous challenges in protecting data and networks effectively. One of the most significant challenges is the shortage of skilled cybersecurity professionals, as demand for expertise continues to outpace the supply of qualified personnel, leaving organizations vulnerable to attacks [20].

- **Rapid Evolution of Threats:** Cybercriminals continuously adapt to exploit new vulnerabilities, creating an ongoing arms race. Many organizations find their security measures outdated or insufficient, particularly in sectors like finance, where real time responses are essential [21].
- **Complexity of Securing Interconnected Networks:** As organizations incorporate cloud services, mobile devices, and Internet of Things (IoT) technologies, network complexity increases, presenting new attack vectors. Securing IoT devices in healthcare, for instance, where devices are often resource constrained, introduces unique challenges [22].
- **Human Error:** A significant portion of breaches results from human error, including misconfigurations, delays in applying patches, or falling victim to phishing. Organizations are investing in cybersecurity training to reduce these risks, yet human error remains a prevalent issue across industries [23].

2.3. Case Studies

The following case studies demonstrate the real world impact of cybersecurity vulnerabilities and highlight the increasing sophistication of cyberattacks. These examples underscore critical lessons for organizations in managing risks, securing third party access points, and addressing software vulnerabilities effectively:

- **Target Data Breach:** This breach resulted in the theft of millions of credit card numbers. Attackers accessed Target network through a third party vendor, underlining the importance of securing supply chains and third party access points [24].
- **Equifax Breach:** Affecting 147 million individuals, the Equifax breach highlighted the consequences of delayed vulnerability management and underscored the necessity of timely patching, particularly in industries with sensitive data [25].
- **Solar Winds Attack:** Attackers inserted malicious code into Solar Winds Orion software, gaining access to various government and corporate networks. This attack underscored the risks inherent in third party software vulnerabilities and the need for stringent monitoring of external software [26].

These cases emphasize the importance of adopting a multi layered cybersecurity approach and maintaining ongoing vigilance, timely patching, and thorough security assessments to mitigate vulnerabilities.

3. RESEARCH METHODS

This study employs a mixed method approach to comprehensively assess the challenges organizations face in securing data and networks against modern cyberthreats. By combining quantitative data from structured surveys with qualitative insights gathered through case studies, the methodology provides a robust framework for understanding the complex and evolving nature of cybersecurity threats and practices [27].

The mixed method design was chosen to capture both statistical prevalence and in depth analysis of cybersecurity challenges across various organizational contexts. This dual approach not only highlights the technical and operational aspects of cybersecurity but also reflects the sector specific applications and implications of security practices. For instance, sectors like healthcare and finance, which handle highly sensitive data, require unique considerations for threat detection and incident response [28].

3.1. Data Collection

The data collection process utilized a combination of surveys, interviews, and case studies to gather comprehensive insights into cybersecurity challenges and practices [29]. Each method provided distinct perspectives, enabling a balanced understanding of both quantitative trends and qualitative experiences in addressing modern cyber threats:

- **Surveys:** Structured surveys were administered to cybersecurity professionals and IT staff across multiple industries. The survey focused on identifying common security challenges, the types of threats encountered, and the tools and protocols used to mitigate these threats. This quantitative data allowed us to assess the extent of issues like skill shortages, network complexity, and the adoption rate of advanced security solutions across sectors [30].
- **Interviews:** Semi structured interviews with cybersecurity experts provided qualitative insights into specific challenges related to data protection, network security, and the implementation of new security technologies. These experts also shared their experiences with sector specific vulnerabilities and compliance requirements, particularly in critical sectors such as finance and healthcare, where the impact of security breaches can be catastrophic [31].
- **Case Studies:** Recent high profile cybersecurity incidents, such as the Solar Winds and Equifax breaches, were examined to highlight the real world applications and limitations of current security practices. Case study analysis included an exploration of factors like the types of vulnerabilities exploited, response times, and the aftermath of each attack. The lessons drawn from these cases illustrate the effectiveness of certain security measures and underscore areas where organizations may need to bolster their defenses [32].

3.2. Analysis Techniques

The analysis techniques employed in this study combine qualitative and quantitative approaches to provide a comprehensive understanding of cybersecurity challenges and strategies [33]. Each method contributes unique insights, enhancing the overall robustness of the findings:

- **Thematic Analysis:** Qualitative data from interviews were subjected to thematic coding to identify recurring challenges, strategies, and gaps in existing security practices. Themes were also analyzed for sector specific insights, particularly within healthcare and finance, to understand how these industries address unique security concerns.
- **Statistical Analysis:** Quantitative survey data were analyzed using descriptive and inferential statistics to measure the frequency, severity, and impact of cybersecurity challenges across organizations. This analysis provided a comparative understanding of how different sectors prioritize and implement various security measures.
- **Comparative Analysis:** By comparing findings from surveys and case studies, this study assessed common vulnerabilities, threat types, and the effectiveness of various security strategies. This comparative approach generated actionable insights for improving cybersecurity frameworks, particularly for high risk sectors.

This methodology ensures a well rounded analysis of the cybersecurity landscape, combining real-world experiences with empirical data to address the key challenges in protecting networks and data from modern cyber threats.

4. RESULT AND DISCUSSION

The data collected from surveys and case studies reveal several critical challenges in securing organizational networks and data from cyber threats. Skill shortages, inadequate security measures, and network complexity emerged as the most pressing issues, impacting sectors with sensitive data, such as healthcare and finance, particularly acutely.

4.1. Analysis of Survey and Case Study Findings

Skill Shortages Approximately 65% of surveyed organizations reported a shortage of qualified cybersecurity staff, impacting their ability to monitor and respond to threats effectively. This gap poses a significant risk, as it leaves organizations vulnerable to undetected attacks. In finance, this shortage translates to higher risks in transactional security, while in healthcare, it impacts patient data protection. **Inadequate Security Measures:** While traditional security tools like firewalls and IDS are widely implemented, they are increasingly insufficient against sophisticated attacks. AI driven threat detection and zero trust architectures, adopted by only 40% of organizations, were linked with a 35% reduction in detected security incidents. This finding highlights the necessity of advanced security measures, particularly for sectors like finance, where realtime threat identification can prevent significant monetary losses, and healthcare, where patient data integrity is critical.

Table 1. Common Challenges in Cybersecurity and the Percentage of Organizations Affected

Challenges in Cybersecurity	Percentage of Organizations Affected
Skill Shortages	65%
Inadequate Security Measures	58%
Network Complexity	72%
Rapidly Evolving Threats	48%

The study findings underscore that traditional security measures, though still valuable, require continuous enhancement to keep up with modern threats. Table 1 presents a comparative analysis of traditional and advanced security solutions, showing that AI driven detection systems and zero trust models are statistically more effective in reducing security incidents. This supports the argument for adopting advanced models, especially in high risk sectors.

4.2. Evaluation of Current Security Practices

In the case study analysis, organizations affected by ransomware attacks and DDoS attacks highlighted the vulnerabilities in their perimeter defenses, particularly the insufficient implementation of MFA and lack of real time monitoring systems.

Table 2. Effectiveness of Various Security Solutions Implemented

Security Solutions Implemented	Effectiveness (%)
Traditional Firewalls and IDS	55%
AI Driven Threat Detection Systems	78%
Zero Trust Architecture	72%
Multi Factor Authentication (MFA)	65%

Table 2 shows the effectiveness of various security solutions implemented, measured in percentage. AI driven threat detection systems have the highest effectiveness at 78%, followed by Zero Trust Architecture at 72%, MFA at 65%, and Traditional Firewalls and IDS at 55%.

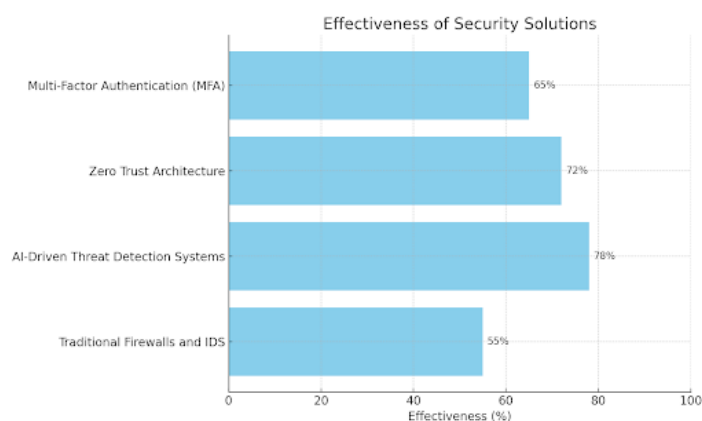


Figure 1. Comparative Performance of AI and Traditional Models

Figure 1 Effectiveness of Security Solutions, which compares the effectiveness of various security measures based on the data collected. This visual representation highlights the higher effectiveness of AI driven threat detection systems and zero trust architectures in mitigating modern cyber threats.

4.3. Implications for Organizations

The challenges identified have significant implications for organizations. The shortage of skilled professionals and inadequate security measures can lead to financial losses, as organizations become more susceptible to breaches. Additionally, reputational damage and regulatory penalties are common outcomes when customer data is compromised. The case studies showed that organizations failing to implement adequate security measures faced an average recovery cost of \$3.8 million following a breach. Moreover, non compliance with regulations such as General Data Protection Regulation (GDPR) resulted in fines for several companies, further emphasizing the need for enhanced security protocols.

In conclusion, while traditional security measures are still widely used, there is a growing need for more advanced solutions to counter the complexity and evolving nature of cyber threats. By adopting technologies such as AI driven detection and zero trust, organizations can better protect their assets and mitigate the risk of cyberattacks.

4.4. Sector Specific Implications for Healthcare and Finance

The implications of these findings are particularly relevant for sectors that handle critical data. In healthcare, the increasing use of IoT devices has created new vulnerabilities, requiring organizations to implement secure IoT frameworks. Meanwhile, the finance sector is highly susceptible to phishing and ransomware due to the value of financial data. The study recommends sector specific strategies, such as enhanced training for healthcare staff on IoT security and zero trust implementation for financial services to control access more effectively.

4.5. Practical Recommendations

The findings indicate that organizations need to adopt a multi layered cybersecurity approach, combining traditional and advanced methods. AI driven threat detection, multifactor authentication, and zero trust models are particularly recommended, as they address gaps in both network complexity and skill shortages. The results also suggest the need for ongoing cybersecurity training programs to mitigate human error, which remains a significant vulnerability.

5. MANAGERIAL IMPLICATION

Organizations must recognize that traditional cybersecurity measures are no longer sufficient to address the complexity of modern threats. Managers should prioritize the adoption of advanced technologies, such as AI driven threat detection and zero trust architectures, to enhance security, especially in high risk sectors like healthcare and finance. Furthermore, continuous employee training programs are essential to minimize human error, a critical factor in security breaches. By integrating advanced solutions with sector specific

frameworks, managers can build a resilient and adaptive cybersecurity strategy to protect their organizations in an increasingly digital and interconnected environment.


6. CONCLUSION

This study identifies critical challenges in organizational cybersecurity, such as skill shortages, inadequate security measures, and increasing network complexity, which collectively undermine resilience against evolving cyber threats. By employing a mixed method approach, this research bridges quantitative IDS, in countering sophisticated threats. Advanced solutions like AI driven threat detection systems and zero trust architectures demonstrate greater effectiveness in high risk sectors. For instance, secure IoT frameworks are vital for safeguarding connected medical devices in healthcare, while real time threat detection systems are crucial for the finance sector to combat phishing and ransomware attacks. These findings emphasize the need for organizations to prioritize innovative technologies and tailor their cybersecurity strategies to sector specific risks.

Despite these advancements, cybersecurity is not solely a technological challenge but also a human one. Organizations must adopt a multi layered approach that combines cutting edge technology with continuous cybersecurity training to reduce human error, which remains a significant factor in breaches. This study acknowledges its limitation in focusing on existing technologies and recommends future research to explore the implications of emerging innovations like quantum computing on cybersecurity. Additionally, developing sector specific frameworks to address unique industry challenges will further enhance resilience. An integrated approach combining technology, human expertise, and sector specific adaptations will be indispensable for building a secure and adaptable cybersecurity posture in today's rapidly evolving digital landscape.


7. DECLARATIONS


7.1. About Authors


Irma Shantilawati (IS)  <https://orcid.org/0009-0009-5056-0480>

Jihan Zanubiya (JZ)  <https://orcid.org/0009-0009-3661-0824>

Fajriannoor Fanan (FF)  <https://orcid.org/0000-0002-5621-7802>

Henrik Jensen (HJ)  -

Shofiyul Millah (SM)  <https://orcid.org/0000-0002-6696-9450>

Ninda Lutfiani (NL)  <https://orcid.org/0000-0001-7019-0020>

7.2. Author Contributions

Conceptualization: IS; Methodology: JZ; Software: HJ; Validation: SM and NL; Formal Analysis: IS and NL; Investigation: SM; Resources: JZ; Data Curation: HJ; Writing Original Draft Preparation: JZ and SM; Writing Review and Editing: IS and NL; Visualization: HJ; All authors, IS, JZ, HJ, SM, NL have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Declaration of Conflicting Interest

The authors declare that they have no conflicts of interest, known competing financial interests, or personal relationships that could have influenced the work reported in this paper.

REFERENCES

- [1] S. AlDaajeh, H. Saleous, S. Alrabaae, E. Barka, F. Breitingner, and K.-K. R. Choo, "The role of national cybersecurity strategies on the improvement of cybersecurity education," *Computers & Security*, vol. 119, p. 102754, 2022.
- [2] Y. Shino, F. Utami, and S. Sukmaningsih, "Economic preneur's innovative strategy in facing the economic crisis," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 5, no. 2, pp. 117–126, 2024.
- [3] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, "A systematic literature review on cloud computing security: threats and mitigation strategies," *Ieee Access*, vol. 9, pp. 57 792–57 807, 2021.
- [4] M. Macas, C. Wu, and W. Fuertes, "A survey on deep learning for cybersecurity: Progress, challenges, and opportunities," *Computer Networks*, vol. 212, p. 109032, 2022.
- [5] J. van der Merwe, S. M. Wahid, G. P. Cesna, D. A. Prabowo *et al.*, "Improving natural resource management through ai: Quantitative analysis using smartpls," *International Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 135–142, 2024.
- [6] Q. Li, Z. Wen, Z. Wu, S. Hu, N. Wang, Y. Li, X. Liu, and B. He, "A survey on federated learning systems: Vision, hype and reality for data privacy and protection," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 4, pp. 3347–3366, 2021.
- [7] W. Sejati, A. N. Pusoko, E. V. Aryadi, S. Andajani, D. P. A. Hidayat, E. Kurniyaningrum, and N. Z. O'Connor, "Flood routing and dam breach parameter calculation on sepaku semoi dam," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 1, pp. 136–148, 2024.
- [8] P. B. Prince and S. J. Lovesum, "Privacy enforced access control model for secured data handling in cloud-based pervasive health care system," *SN Computer Science*, vol. 1, no. 5, p. 239, 2020.
- [9] T. Winarti, E. Widodo, S. Handayni, and A. Nugroho, "Utilizing pearson correlation matrix to identify negative correlations among cryptocurrencies," in *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCICT)*. IEEE, 2024, pp. 1–7.
- [10] A. K. Jain, S. R. Sahoo, and J. Kaubiyal, "Online social networks security and privacy: comprehensive review and analysis," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2157–2177, 2021.
- [11] J. Manurung, E. Anom *et al.*, "Strategi pemanfaatan media sosial sebagai sarana promosi sekolah musik di dotodo music edutainment," *Technomedia Journal*, vol. 8, no. 2 Oktober, pp. 248–260, 2023.
- [12] R. Ferdiana *et al.*, "A systematic literature review of intrusion detection system for network security: Research trends, datasets and methods," in *2020 4th International Conference on Informatics and Computational Sciences (ICICoS)*. IEEE, 2020, pp. 1–6.
- [13] L. Honesti, Q. Aini, M. I. Setiawan, N. P. L. Santoso, and W. Y. Prihastiwi, "Smart contract-based gamification scheme for college in higher education," *APTISI Transactions on Management*, vol. 6, no. 2, pp. 102–111, 2022.
- [14] D. Ghelani, "Cyber security, cyber threats, implications and future perspectives: A review," *Authorea Preprints*, 2022.
- [15] S. Rahayu, H. Haris, and Y. Candrah, "Web-based classification information system for web-based at pt. sintech berkah abadi," *ADI Journal on Recent Innovation*, vol. 2, no. 2, pp. 208–215, 2021.
- [16] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity threats and their mitigation approaches using machine learning—a review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 527–555, 2022.
- [17] A. Bagaskara, R. Mulyana, and T. Kurniawan, "Memanfaatkan teknologi dalam administrasi komunikasi bisnis," *ADI Bisnis Digital Interdisiplin Jurnal*, vol. 4, no. 2, pp. 122–126, 2023.
- [18] K. Albulayhi and Q. A. Al-Haija, "Early-stage malware and ransomware forecasting in the short-term future using regression-based neural network technique," in *2022 14th International Conference on Computational Intelligence and Communication Networks (CICN)*. IEEE, 2022, pp. 735–742.
- [19] D. Zegzhda, D. Lavrova, E. Pavlenko, and A. Shtyrkina, "Cyber attack prevention based on evolutionary cybernetics approach," *Symmetry*, vol. 12, no. 11, p. 1931, 2020.
- [20] S. Watini *et al.*, "Development of java hands startup business idea model by lean startup approach," *Startupreneur Business Digital (SABDA Journal)*, vol. 2, no. 1, pp. 43–50, 2023.
- [21] I. Magomedov, H. Murzaev, A. Zolkin *et al.*, "Cyber literacy as one of the main discipline necessary in modern time," *European Proceedings of Social and Behavioural Sciences*, 2020.
- [22] D. Hernandez, L. Pasha, D. A. Yusuf, R. Nurfaizi, and D. Julianingsih, "The role of artificial intelligence

- in sustainable agriculture and waste management: Towards a green future,” *International Transactions on Artificial Intelligence*, vol. 2, no. 2, pp. 150–157, 2024.
- [23] M. Jangjou and M. K. Sohrabi, “A comprehensive survey on security challenges in different network layers in cloud computing,” *Archives of Computational Methods in Engineering*, vol. 29, no. 6, pp. 3587–3608, 2022.
- [24] H. Tabrizchi and M. Kuchaki Rafsanjani, “A survey on security challenges in cloud computing: issues, threats, and solutions,” *The journal of supercomputing*, vol. 76, no. 12, pp. 9493–9532, 2020.
- [25] N. Daswani, M. Elbayadi, N. Daswani, and M. Elbayadi, “The equifax breach,” *Big Breaches: Cybersecurity Lessons for Everyone*, pp. 75–95, 2021.
- [26] E. D. Wolff, K. M. GroWIEy, M. O. Lerner, M. B. Welling, M. G. Gruden, and J. Canter, “Navigating the solarwinds supply chain attack,” *Procurement Law.*, vol. 56, p. 3, 2021.
- [27] D. Indiyati, U. Rahardja, U. Rusilowati, S. Millah, A. Faturahman, and A. Fitriani, “Enhancing human resources management with blockchain technology: A case study approach,” in *2024 3rd International Conference on Creative Communication and Innovative Technology (ICCICT)*. IEEE, 2024, pp. 1–6.
- [28] S. Maesaroh, H. Gunawan, A. Lestari, M. S. A. Tsaurie, and M. Fauji, “Query optimization in mysql database using index,” *International Journal of Cyber and IT Service Management*, vol. 2, no. 2, pp. 104–110, 2022.
- [29] V. Schlatt, T. Guggenberger, J. Schmid, and N. Urbach, “Attacking the trust machine: Developing an information systems research agenda for blockchain cybersecurity,” *International journal of information management*, vol. 68, p. 102470, 2023.
- [30] K. Zhao, J. Hu, H. Shao, and J. Hu, “Federated multi-source domain adversarial adaptation framework for machinery fault diagnosis with data privacy,” *Reliability Engineering & System Safety*, vol. 236, p. 109246, 2023.
- [31] M. Khan and L. Ghafoor, “Adversarial machine learning in the context of network security: Challenges and solutions,” *Journal of Computational Intelligence and Robotics*, vol. 4, no. 1, pp. 51–63, 2024.
- [32] M. Sewak, S. K. Sahay, and H. Rathore, “Deep reinforcement learning in the advanced cybersecurity threat detection and protection,” *Information Systems Frontiers*, vol. 25, no. 2, pp. 589–611, 2023.
- [33] M. S. Islam, M. A. Rahman, M. A. Bin Ameedeen, H. Ajra, Z. B. Ismail, and J. M. Zain, “Blockchain-enabled cybersecurity provision for scalable heterogeneous network: A comprehensive survey.” *CMES-Computer Modeling in Engineering & Sciences*, vol. 138, no. 1, 2024.