Cybersecurity: Transforming Vulnerable System to A More Secure and Hard-to-Penetrate System

Perdylasta[a], Diandra Harry Saputra[b], Muhammad Irfa'i[c], Muhammad Sayyid Azzuhdi[d], and Suciana Wijirahayu[e*]
[abcde*]Universitas Muhammadiyah Prof. Dr. HAMKA, DK Jakarta, Indonesia

*Correspondence: sucianawijirahayu@uhamka.ac.id

Protecting vulnerable systems has been a critical concern as cyberthreats continue to rapidly grow. This paper explores strategies for transforming these vulnerable systems into a more secure and hard-to-penetrate system. There are several techniques or strategies to strengthen the protection of a system including Zero-Trust Architecture (ZTA), advance authentication mechanism, and machine learning threat detection. If these techniques or strategies combined and integrated, the result would significantly enhances the system protection. Zero-trust Architecture (ZTA) reduce the attack surfaces, machine learning dynamically detect the threat, and advanced authentication mechanism reduce unauthorized access.

Article History:

Keywords:
multi-layered security, system vulnerability cybersecurity, cyberthreats

1. Introduction

The rapid advancement of the digital technology have together took us in a new era of digital age. This transformation is different from any technological revolutions we have experienced before. Advancements in things like natural language processing, machine learning, and AI have improve how we use and work with social media, Internet of Things (IoT), computer networking, etc. This massive transformation improve the operations of businesses, organizations, governments, society in general, and day to day life of an individual. This transformation also sets the current technology apart from earlier periods of technological development. These improvements have also introduced new challenges and one of them is security. The security of the new digital age is known as Cybersecurity.

Cybersecurity is a practice of protecting systems, networks or programs from cyber attack. Cybersecurity has become a critical and essential aspect of modern digital systems, where vulnerabilities can lead to severe consequences like data breaches, ransomware attacks, denial-of-service attacks, and other malicious activities. Previous studies have explored various aspects of cybersecurity. For example, Aslan et al. (2023) identified how attackers exploit weaknesses in hardware, software, and communication layers, while Kapoor et al. (2022) reviewed strategies for ransomware detection and mitigation, illustrating the evolving nature of such attacks and their impact on businesses and individuals. However, majority of these studies tend to focus on either individual solutions or specific vulnerabilities types. There is a lack of research offering a well-rounded strategy that combines different strategy to transform vulnerable systems into secure, more resilient and hard-to-penetrate system. This research aims to bridge the gap by combining these strategies into an integrated approach.

Table 1
Acronyms

Phrase	Acronym
Artificial Intelligence	AI
Internet of Things	IoT
Zero-Trust Architecture	ZTA
Machine Learning	ML
Distributed Denial of Service	DDoS
Advance Persistent Threat	APT
Multi-Factor Authentication	MFA

2. Method

This research adopts a literature study methodology to systematically analyze existing studies in cybersecurity, with a focus on strategies for transforming vulnerable systems into secure and hard-to-penetrate system. The methodology is made up of several components. First, the research design adopts a qualitative approach based on secondary data analysis. The objective is to extract, combine, and interpret insights from articles that explore vulnerabilities, threats, and mitigation strategies. A well rounded cybersecurity strategies are able to be identified by this approach, identifying best practices and how they integrate. This research paper has its insight from Aslan et al.'s (2023) review of cybersecurity vulnerabilities and solutions, Kapoor et al.'s (2022) analysis of ransomware detection and mitigation strategies, and Shaukat et al.'s (2020) exploration of machine learning techniques for cybersecurity, highlighting the potential of AI-driven approaches to strengthen the protection of a system.

The subject of this research paper is examining secondary data, that has been turned into two types, a population and a sample. The population includes academic and industry publications from 2018 to 2023, focusing on topic of cybersecurity and published in trusted journals like Electronics, Sustainability, and IEEE Access. Articles were sourced from databases like MDPI, IEEE Xplore, and SpringerLink using keywords like "cybersecurity", "system vulnerability", and "mitigation strategies". The selection criteria make sure the inclusion of journal articles from 2018 to 2023, focusing on system vulnerabilities and cybersecurity strategies while also exclude studies of unrelated to the topic.

The data were analyzed using thematic and comparative qualitative methods. Thematic analysis categorized findings into areas like system vulnerabilities (for example: software misconfigurations) and mitigation strategies (for example: zero-trust architecture and machine learning-based detection). Comparative analysis identify consistencies, research gaps, and innovative practices from different sources. This methodology supports the development of a well-rounded approach to addressing evolving cybersecurity challenges.

3. Results and Discussion

3.1 Results

The literature review conducted for this research revealed several key findings regarding the state of cybersecurity and the strategies for transforming vulnerable systems into secure infrastructure. One of the findings from the review is that adopting a multi-layered protection model can increase and strengthen the protection of a system by combining and integrating various cybersecurity strategies and approaches to handle different threats.

In recent studies, the use of zero-trust architecture (ZTA) has become an essential strategies of modern cybersecurity. Unlike traditional network defenses that focus solely on perimeter security, zero-trust architecture (ZTA) assumes that all systems and users, both inside and outside of the network

should be continuously verified and monitored. This approach prove that zero-trust architecture (ZTA) is very effective in limiting the attack surface and improving detection capabilities for external and internal threats. Research by Aslan et al. (2023) highlights that zero-trust architecture (ZTA) can provide a more effective and better cybersecurity setup compared to previous models like firewall which focused on perimeter defenses only.

The importance of machine learning (ML) and artificial intelligence (AI) techniques in cybersecurity has become a key focus in cybersecurity. Machine Learning and AI-driven system is being used to strengthen threat detection, prediction, and response capabilities. For example machine learning algorithms can be trained to detect unusual activities, patterns, and behaviors that indicate malicious activities, such as ransomware attack, data breaches, or DDoS. Studies conducted by Kapoor et al. (2022) and Shaukat et al. (2020) shows that machine learning and AI-based detection systems can improve the efficiency and accuracy of threat detection while reducing false positives. Another finding from the review is integration of continuous monitoring systems that can help to identify and respond to threats in real-time. Continuous monitoring proved to be effective to identify new and advanced cyber attacks like advanced persistent threat (APT) that is designed to evade detection.

Those findings shows that integrated model has been a trending practice in cybersecurity and still continue to be researched. The traditional model of relying on spesific security solutions like firewalls or intrusion detection systems is being replaced gradually by a more compact strategy that include real-time monitoring, artificial intelligence (AI), and zero-trust architecture (ZTA). This transformation reflects the rapidly growing nature of cyber threats and the need to always adapt to a more innovative and multi-layered protection. These results offer a foundation for further research and practical implementations in the field of cybersecurity, as it highlight the limitations of existing systems and suggest more effective strategies for transforming vulnerable systems into a more secure systems.

3.2 Discussion

This study found that combining zero-trust architecture (ZTA), machine learning, and advanced authentication mechanism can reduce system vulnerabilities and improve protection capabilities. This is consistent with existing literature, such as the studies by Aslan et al. (2023) that emphasize the importance of multi-layered defenses. However, the uniqueness of this research lies in proposing an integrated model that combines diverse cybersecurity strategies, not only focusing on spesific solutions. Additionally, the role of machine learning in identify, predict, and response to threats, as discussed by Shaukat et al. (2020), illustrates how AI-driven detection system offer stronger capabilities that enhance the security and protection of vulnerable systems.

The reason to integrate these strategies stems from the increasing complexity of cyberattacks. As the variety and advancement of threats continue to grow, relying on a single mitigation method like traditional intrusion detection or encryption alone is not effective. This study demonstrates that a multi-layered approach, using continuous monitoring, anomaly detection through machine learning, and zero-trust achitecture (ZTA), helps to improve the detection of unique threats and reduces the potential attack surface. Machine learning's ability to anticipate threats and identify abnormal patterns (known as anomaly) in real-time as discussed by Kapoor et al. (2022), adds another layer of predictive defense that increase the protection and making it able to anticipate advanced persistent threats (APTs).

The findings support previous calls in the literature for a more integrated approach to cybersecurity as seen in the work of Kapoor et al. (2022) and Shaukat et al. (2020), who emphasize that using both AI and traditional defense mechanism is important to strengthen the protection of a system. While zero-trust architectures and multi-factor authentication (MFA) have been shown to significantly strengthen security, this study demonstrates that their integration with machine learning and continuous monitoring systems provides a more dynamic and adaptive protection. These combined solutions offer a more quick and strong response to the complex and rapidly growing of cybersecurity threats.

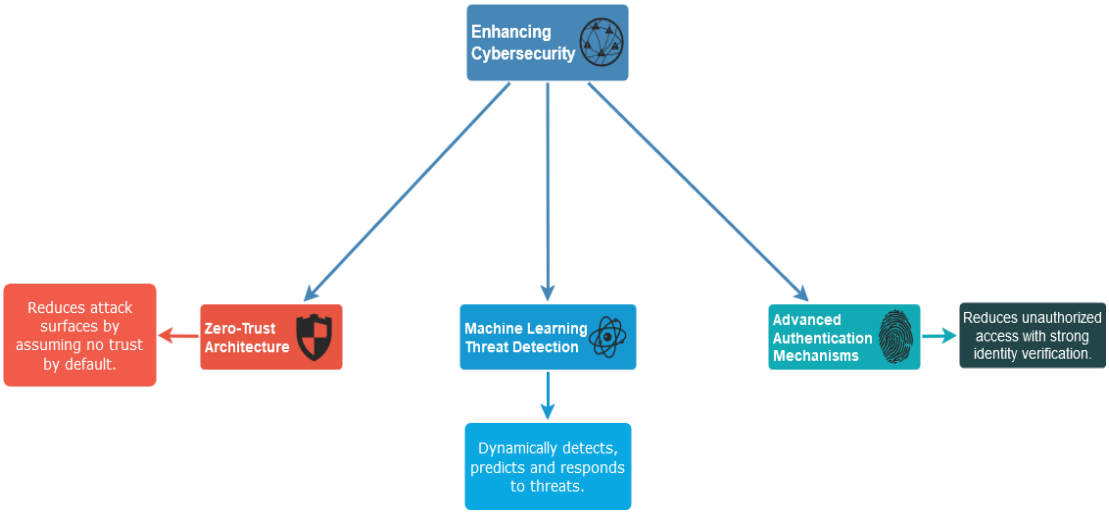

Figure 1
Key Strategies to Enhance Cybersecurity.

This research also identifies a gap in current cybersecurity practices, as many studies and frameworks focus on spesific security strategies. The lack of research on integrated defense models suggests an opportunity for innovation in cybersecurity. By integrating different protection strategies into a comprehensie and multi-layered approach, organizations can better protect themselves against a broader range of cyber attacks, including those that use advanced techniques like AI-driven exploitation or social engineering attacks.

4. Conclusion

This research aimed to explore strategies to transform vulnerable systems into secure, hard-to-penetrate infrastructure by integrating multiple cybersecurity strategies. The goal of the study was to propose a comprehensive and multi-layered approach that combines zero-trust architecture (ZTA), machine learning, and advanced authentication mechanism to enhance and strengthen protection against growing cyber threats.

The study contributes to the existing body of knowledge by bridging the gap between spesific cybersecurity solutions so it becomes one integrated strategies. While previous research has focused on specific security strategy or vulnerabilities, this work demonstrates that combining these diverse strategies into an integrated system can lead to a more resilient protection model. Specifically, the findings suggest that zero-trust architecture can reduce the attack surface, machine learning threat detection can detect, predict and respond to cyber threats and multi-factor authentication ensures that unauthorized access is effectively prevented.

The proposed strategy is more advance than current model because it provides a well-rounded protection against a wide range of threats. By integrating these strategies, organizations can improve their security setup and better defend against advance attacks like advanced persistent threats (APTs) or social engineering attacks, which often can bypass traditional defense and protection strategy.

For practical implementation, this integrated strategies can be used across different sectors where security is important like data center, server, healthcare, finance, etc. Future research could focus on innovating the implementation of this strategies in the real world, exploring its adaptability to different sectors and evaluating effectivity in handling cyber attacks. Experiments on combining and integrating other developing technologies like blockchain to secure data sharing or quantum computing for advanced encryption can further enhance the strength of cybersecurity protection.

5. References

Alsamiri, J., & Alsubhi, K. (2019). Internet of Things Cyber Attacks Detection using Machine Learning. *International Journal of Advanced Computer Science and Applications*, *10*(12). https://doi.org/10.14569/IJACSA.2019.0101280

Alsharif, M., Mishra, S., & AlShehri, M. (2021). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering*, *40*(3), 1153–1166. https://doi.org/10.32604/CSSE.2022.019938

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(6), 1333. https://doi.org/10.3390/electronics12061333

Barik, K., Misra, S., Konar, K., Fernandez-Sanz, L., & Koyuncu, M. (2022). Cybersecurity Deep: Approaches, Attacks Dataset, and Comparative Study. *Applied Artificial Intelligence*, *36*(1). https://doi.org/10.1080/08839514.2022.2055399

Dokur, N. B. (2023). *Artificial Intelligence (AI) Applications in Cyber Security*. *January*. https://www.researchgate.net/publication/367253331_Artificial_Intelligence_AI_Applications_in_Cyber_Security

Dwyer, A. C., Stevens, C., Muller, L. P., Cavelty, M. D., Coles-Kemp, L., & Thornton, P. (2022). What Can a Critical Cybersecurity Do? *International Political Sociology*, *16*(3), 1–26. https://doi.org/10.1093/ips/olac013

Esther Jyothi, V., Prasad, B. D. C. N., & Mojjada, R. K. (2020). Analysis of Cryptography Encryption for Network Security. *IOP Conference Series: Materials Science and Engineering*, *981*(2). https://doi.org/10.1088/1757-899X/981/2/022028

Gawand, S. P., & Kumar, M. S. (2023). *A Comparative Study of Cyber Attack Detection & Prediction Using Machine Learning Algorithms*. https://doi.org/10.21203/rs.3.rs-3238552/v1

Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2021). Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. *Sustainability*, *14*(1), 8. https://doi.org/10.3390/su14010008

MalathiEswaran, S.Hamsanandhini, & IlakiyaLakshmi, K. (2021). Survey of Cyber security approaches for Attack Detection and Prevention. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(2), 3436–3441. https://doi.org/10.17762/turcomat.v12i2.2406

Mantha, B. R. K., & de Soto, B. G. (2019). Cyber security challenges and vulnerability assessment in the construction industry. *Proceedings of the Creative Construction Conference 2019*, *June*, 29–37. https://doi.org/10.3311/CCC2019-005

Perwej, D. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, D. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Rauf, U., Mohsen, F., & Wei, Z. (2023). A Taxonomic Classification of Insider Threats: Existing Techniques, Future Directions & Recommendations. *Journal of Cyber Security and Mobility*, *12*(2), 221–252. https://doi.org/10.13052/jcsm2245-1439.1225

Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1), 105. https://doi.org/10.1186/s40537-024-00957-y

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A Survey on Machine Learning Techniques for Cyber Security in the Last Decade. *IEEE Access*, *8*, 222310–222354. https://doi.org/10.1109/ACCESS.2020.3041951

Veale, M., & Ian Bro. (2020). *Cybersecurity Cybersecurity*. 0–22.

Welukar, J. N., & Bajoria, G. P. (2021). Artificial Intelligence in Cyber Security - A Review. *International Journal of Scientific Research in Science and Technology*, 488–491. https://doi.org/10.32628/IJSRST218675