International Transactions on Education Technology (ITEE)
Vol. 2 No. 1 November 2023

p-ISSN: 2963-6078
e-ISSN: 2963-1947

Enhancing Security Frameworks with Artificial Intelligence in Cybersecurity

Dendy Jonas[1], Natasya Aprila Yusuf[2], Achani Rahmania Az Zahra[3]

[1,2,3]Faculty of Science and Technology, University of Raharja, Indonesia
E-mail address: dendy.jonas@raharja.info[1], natasya@raharja.info[2], achani@raharja.info[3]

Author Notification
October, 01 2023
Final Revised
October, 15 2023
Published
November, 01 2023

To cite this document:
Jonas, D., Yusuf, N.A., & Zahra, A.R.A. (2023). Enhancing Security Frameworks with Artificial Intelligence in Cybersecurity. International Transactions on Education Technology (ITEE), 2(1) 83-91

Abstract

Cybersecurity, in the digital era we live in today, has become a major concern that demands innovation. Data Science and Artificial Intelligence (AI) have played a central role in changing the way we understand and address cyber threats. This research will review the important role of innovation in this technology in improving an organization's ability to detect, prevent, and respond to cyber attacks. Identifying patterns and gaining insights from security events in cyber data, while developing appropriate data-based models, is a key element in realizing automated and intelligent security systems. This research reviews needs in the cyber security domain that can be addressed through Artificial Intelligence (AI) techniques. In this study, we employed quantitative methods to assess the impact of artificial intelligence on enhancing cybersecurity by distributing questionnaires to 85 respondents, which included companies operating in the banking and IT sectors. In addition, this research will explore how data-based intelligent decision-making systems are able to protect systems from known and unknown cyber attacks. This research will conclude by considering the future potential of Artificial Intelligence and cybersecurity.

Keywords: Artificial Intelligence, Cyber Security, Innovation, Security System

1. Introduction

Cybersecurity has emerged as a significant concern in the contemporary digital era. The ongoing advancements in technology and the pervasive reach of the internet have significantly influenced business practices, communication, and our daily lives[1]. In response to the complex and continually evolving cyber threats, there is an imperative for incessant innovation to safeguard the increasingly interconnected data and systems in the digital realm. One pivotal sector at the forefront of comprehending and combatting cyber threats is Data Science and Artificial Intelligence (AI)[2]. With the swift progress of AI technology, numerous unexplored prospects exist for fortifying data and systems against cyber threats. In this dynamic landscape, it is crucial to discern how AI technology will persistently contribute to the maintenance of cybersecurity in the future[3].

p-ISSN: 2963-6078
e-ISSN: 2963-1947

Figure 1. Artificial intelligence.

This study seeks to scrutinize the pivotal role of innovation in Data Science and AI technology in enhancing an organization's capacity to identify, prevent, and respond to cyberattacks[4]. This capability has grown in significance due to the multifarious forms and origins of cyberattacks. Effectively recognizing patterns and deriving insights from security incidents in cyber data, while developing appropriate data-driven models, is an essential component in realizing an automated and intelligent security system.

A primary focus of this research is the identification of specific cybersecurity needs that can be effectively addressed through Artificial Intelligence (AI) techniques. AI technology has transcended its initial roots in Data Science and found contemporary applications in pertinent cybersecurity contexts[5]. In an era characterized by increasingly intricate and structured cyber data, the capacity to swiftly and accurately analyze and process data has become indispensable[6].

Furthermore, this research will explore how data-driven intelligent decision-making systems can be employed to shield systems from both known and unknown cyber threats[7]. Detecting unknown threats represents a significant challenge in the realm of cybersecurity, and AI innovations are poised to bridge this gap[8]. Leveraging machine learning algorithms and profound data analysis enables the system to proactively identify unusual patterns and potential threats before they can compromise system security[2][9].

2. Research Method

In this study, we employed quantitative methods to assess the impact of artificial intelligence on enhancing cybersecurity by distributing questionnaires to 85 respondents, which included companies operating in the banking and IT sectors.

2.2 Literature Review

Cybersecurity has emerged as a significant concern in the modern digital landscape[10]. This concern is driven by continuous technological advancements and the pervasive influence of the internet in our daily lives and business practices. As the digital world becomes more interconnected, the necessity for ongoing innovation to safeguard data and systems from ever-evolving cyber threats has become paramount. At the forefront of

understanding and countering these threats, Data Science and Artificial Intelligence (AI) play pivotal roles, offering uncharted possibilities for bolstering digital security[11].

a. Artificial Intelligence

The interrelationship between AI and cybersecurity is strikingly evident in the swift development of AI technology. With AI's extensive capabilities, its potential in safeguarding data and digital systems can now be harnessed. It is imperative to comprehend how AI technology will continue to contribute to upholding cybersecurity in the future[12]. AI contribution to cybersecurity is multifaceted, with a particular emphasis on enhancing an organization's capacity to identify, prevent, and respond to cyberattacks. This becomes increasingly crucial given the diverse forms and sources of cyber threats[13]. An essential aspect of these enhancements is the capability to effectively recognize patterns and extract insights from security events in cyber data, all the while constructing data-driven models to create automated and intelligent security systems[14].

b. The Influence of AI on Cybersecurity

The convergence of AI and cybersecurity is not a recent development. AI technology has evolved from its origins in Data Science to establish contemporary standards in the field of cybersecurity[15]. As cyber data becomes progressively intricate and structured, the ability to swiftly and accurately analyze and process data becomes indispensable. AI, utilizing machine learning algorithms and deep data analysis, plays a pivotal role in this process, enabling systems to proactively detect unusual patterns and potential threats before they can compromise system security[16].

c. Enhancing Cybersecurity for Artificial Intelligence

This succinct strategy provides an overview of the critical issues that emerge when striving to enhance cybersecurity and artificial awareness. Furthermore, it delves into the significant role policymakers play in tackling these challenges. With the rapid evolution of artificial intelligence technology and its widespread adoption across diverse sectors, policymakers must increasingly acknowledge the imperative of contemplating the confluence of cybersecurity and AI[17][18]. Artificial intelligence in Cybersecurity is shown in figure 2.

- Faster Discovery and Response Times:

The integration of AI with cybersecurity has ushered in significant changes in the realm of cyber threat detection and response. A crucial aspect of this transformation lies in the swifter identification of threats. Leveraging AI technology, security systems can continually analyze cyber data in real-time[19][20]. This means that when there is a potential indication of a threat, whether it's an anomalous pattern in network traffic or suspicious activity, the system can respond promptly. This empowers security teams to take immediate action, isolating or mitigating threats before they have the opportunity to inflict substantial harm.'

- Phishing Detection and Countermeasures:

Phishing attacks stand out as one of the most prevalent methods employed by cybercriminals to gain unauthorized access to sensitive data or systems[21]. The fusion of AI with cybersecurity has bolstered the capability to detect and address phishing attacks with heightened effectiveness[22]. AI-driven security systems can accurately identify counterfeit emails or messages, even when the attacker attempts to disguise the message[23]. This empowers organizations to adeptly evade phishing ploys and reduce the risk of costly data breaches. Moreover, AI can be utilized to monitor suspicious user and device behavior. In the event of a successful phishing attempt, the system can detect it based on unusual changes in behavior, such as atypical account usage. This furnishes an additional layer of defense against often financially burdensome phishing attacks.

- Behavior Analysis:

Behavioral analysis stands as a cornerstone in contemporary cybersecurity practices[24]. By harnessing AI-based behavioral analysis, security systems can continuously monitor and identify deviations from established patterns, pre-emptively identifying potential threats before they materialize as security breaches. AI's capacity to adapt and learn from behavioral data empowers it to continually refine its threat detection capabilities and proactively respond to emerging cyber risks. The significance of AI in addressing specific cybersecurity requirements is a pivotal facet of the evolving landscape[25]. Understanding how AI techniques can be effectively employed to tackle the distinct challenges posed by modern threats is of utmost importance. This encompasses the identification of both known and unknown corporate and cyber threats. Unknown threats present a significant challenge in the cybersecurity domain, and AI advancements are poised to bridge this gap by virtue of their continuous learning, adaptability, and capacity to recognize anomalies that conventional cybersecurity measures might otherwise overlook.

3. Findings

Artificial intelligence (AI) plays a crucial role in enhancing cybersecurity by facilitating swifter threat detection, executing more efficient responses to counter phishing attacks, and proactively identifying threats through behavioral analysis. Additionally, it is instrumental in mitigating both familiar and unfamiliar threat challenges.

3.1 Problem

The issue that emerges from the introduction and literature review is the importance of strong cybersecurity in today's digital landscape. This is especially important given the increasing complexity of enterprise and cyber threats, which are evolving as technology advances. Therefore, innovation in cyber security is needed to safeguard interconnected data and systems.

3.2 Research Implementation

We gather data related to the utilization of machine learning algorithms for anomaly detection, predictive analytics, and identity and access management. Anomaly Detection involves the utilization of machine learning algorithms to carry out anomaly detection, meaning that algorithms will be used to analyze cyber data and search for unusual patterns or behaviors, which could indicate potential security threats. The objective is to gauge the effectiveness of this method in increasing threat detection rates in an objective and measurable manner.

p-ISSN: xxxx-xxxx
e-ISSN: xxxx-xxxx

Figure 2. The Role of Artificial Intelligence in Cybersecurity.

Machine learning algorithms will be employed to create predictive models. The research will measure the extent to which these models can assist in forecasting threats and evaluate their success. The research will also encompass the use of artificial intelligence for identity and access management. This implies that the system will use machine learning algorithms to analyze user behavior and manage access based on risk. The aim is to assess the efficiency and success of this method in reducing the risk of unauthorized access and safeguarding systems and data.

This data is subsequently analyzed quantitatively to measure increased threat detection levels, security system efficiency, and reduced risk of unauthorized access. Additionally, we also assess the effectiveness of using artificial intelligence in improving data encryption and protection. The outcomes of this quantitative analysis will offer a deeper comprehension of the role of artificial intelligence in reinforcing the security framework within the realm of cybersecurity in an objective and measurable manner.

Table 1. Quantitative Interviews

No	Question
1.	What is your perspective on the use of artificial intelligence in the context of cybersecurity?
2.	Have you or your company implemented artificial intelligence, particularly in the context of cybersecurity?
3.	To what extent has your company experienced improvements in threat detection since adopting artificial intelligence?
4.	What percentage increase in threat detection rates has been achieved after using machine learning algorithms for anomaly detection?
5.	What is the accuracy level of predictive models in forecasting security threats since the adoption of artificial intelligence?
6.	How much has the response time to threats been accelerated since

	implementing artificial intelligence in the security system?
7.	How has the acceleration of decision-making in cybersecurity been since implementing artificial intelligence in your company?
8.	How significant has the increase in threat detection been after applying artificial intelligence in cybersecurity analysis?
9.	To what extent has your company improved the protection of sensitive data and critical information since the implementation of artificial intelligence?
10.	How confident is your company that artificial intelligence has enhanced overall cybersecurity levels?

Table 2. The Value of the Response Given by the Respondent.

No	Excellent	Good	Neutral	Not Good	Very Poor
1.	46	16	15	4	4
2.	32	12	14	5	22
3.	38	14	23	7	3
4.	53	8	10	8	6
5.	37	8	26	8	6
6.	30	25	22	3	5
7.	28	24	17	9	7
8.	18	25	18	20	4
9.	27	18	25	7	8
10.	50	11	15	5	4

p-ISSN: xxxx-xxxx
e-ISSN: xxxx-xxxx

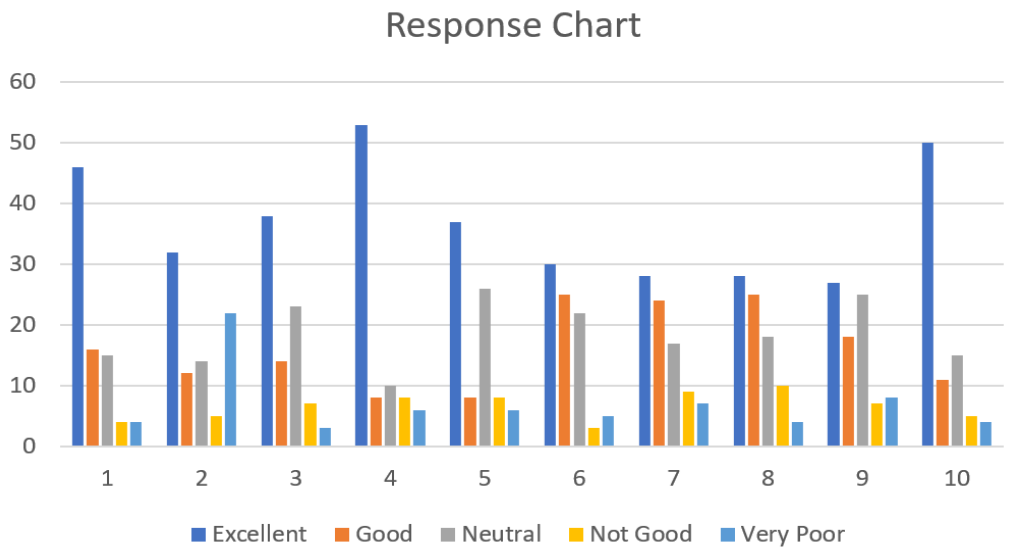

Figure 3. Quantitative Response Chart

Table 3. Percentage Value of Respondents

	1	2	3	4	5	6	7	8	9	10
E	54.12	37.65	44.71	62.35	43.53	35.29	32.94	32.94	31.76	58.82
G	18.82	14.12	16.47	9.41	9.41	29.41	28.24	29.41	21.18	12.94
N	17.65	16.47	27.06	11.76	30.59	25.88	20.00	21.18	29.41	17.65
NG	4.71	5.88	8.24	9.41	9.41	3.53	10.59	11.76	8.24	5.88
VP	4.71	25.88	3.53	7.06	7.06	5.88	8.24	4.71	9.41	4.71

For item 1, 46 people (54.12%) responded strongly agree, while 16 people (18.82%) responded agreeably regarding the use of artificial intelligence in the context of cyber security. There were 32 respondents or around 37.65% of the total 85 respondents, who indicated that their companies had implemented artificial intelligence in cyber security efforts. On the other hand, 22 responses, or around 25.88%, indicate that there are still companies that have not implemented artificial intelligence in the context of cyber security.

4. Conclusion

Based on previous analysis, researchers have discovered that 58.82% of the 85 total respondents firmly believe that the integration of artificial intelligence (AI) into a company's cybersecurity measures can have a positive impact on enhancing security levels. The presence of AI in the realm of cybersecurity also exerts a notable influence on enhancing threat detection, thereby fortifying the safeguarding of sensitive data and vital information. Furthermore, AI-empowered cybersecurity significantly heightens the precision of predictive and anomaly threat detection, as evidenced by survey results displaying approval rates of 44.71% and 62.35%. This, overall, has the potential to speed up decision making in company operations.

References

[1] A. Elliott, *The culture of AI: Everyday life and the digital revolution*. Routledge, 2019.
[2] A. Ibrahim, D. Thiruvady, J.-G. Schneider, and M. Abdelrazek, “The challenges of leveraging threat intelligence to stop data breaches,” *Front. Comput. Sci.*, vol. 2, p. 36, 2020.
[3] I. H. Sarker, M. H. Furhad, and R. Nowrozy, “Ai-driven cybersecurity: an overview, security intelligence modeling and research directions,” *SN Comput. Sci.*, vol. 2, pp. 1–18, 2021.
[4] A. Parisi, *Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies*. Packt Publishing Ltd, 2019.
[5] M. Dunn Cavelty and A. Wenger, “Cyber security meets security politics: Complex technology, fragmented politics, and networked science,” *Contemp. Secur. Policy*, vol. 41, no. 1, pp. 5–32, 2020.
[6] D. B. Rawat, R. Doku, and M. Garuba, “Cybersecurity in big data era: From securing big data to data-driven security,” *IEEE Trans. Serv. Comput.*, vol. 14, no. 6, pp. 2055–2072, 2019.
[7] N. Kharlamova, S. Hashemi, and C. Træholt, “Data-driven approaches for cyber defense of battery energy storage systems,” *Energy AI*, vol. 5, p. 100095, 2021.
[8] N. Kaloudi and J. Li, “The ai-based cyber threat landscape: A survey,” *ACM Comput. Surv.*, vol. 53, no. 1, pp. 1–34, 2020.
[9] I. H. Sarker, “Machine learning for intelligent data analysis and automation in cybersecurity: current and future prospects,” *Ann. Data Sci.*, pp. 1–26, 2022.
[10] R. Ali, “Looking to the future of the cyber security landscape,” *Netw. Secur.*, vol. 2021, no. 3, pp. 8–10, 2021.
[11] S. Kumar, U. Gupta, A. K. Singh, and A. K. Singh, “Artificial Intelligence: Revolutionizing cyber security in the Digital Era,” *J. Comput. Mech. Manag.*, vol. 2, no. 3, pp. 31–42, 2023.
[12] T. Sobb, B. Turnbull, and N. Moustafa, “Supply chain 4.0: A survey of cyber security challenges, solutions and future directions,” *Electronics*, vol. 9, no. 11, p. 1864, 2020.
[13] S. Sharma, “Role of artificial intelligence in cyber security and security framework,” *Artif. Intell. Data Min. Approaches Secur. Fram.*, pp. 33–63, 2021.
[14] R. Coulter, Q.-L. Han, L. Pan, J. Zhang, and Y. Xiang, “Data-driven cyber security in perspective—Intelligent traffic analysis,” *IEEE Trans. Cybern.*, vol. 50, no. 7, pp. 3081–3093, 2019.
[15] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, “Cybersecurity data science: an overview from machine learning perspective,” *J. Big data*, vol. 7, pp. 1–29, 2020.
[16] L. Balyen and T. Peto, “Promising artificial intelligence-machine learning-deep learning algorithms in ophthalmology,” *Asia-Pacific J. Ophthalmol.*, vol. 8, no. 3, pp. 264–272, 2019.
[17] Y. K. Dwivedi *et al.*, “Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy,” *Int. J. Inf. Manage.*, vol. 57, p. 101994, 2021.
[18] M. G. Jacobides, S. Brusoni, and F. Candelon, “The evolutionary dynamics of the artificial intelligence ecosystem,” *Strateg. Sci.*, vol. 6, no. 4, pp. 412–435, 2021.
[19] G. Nguyen *et al.*, “Machine learning and deep learning frameworks and libraries for large-scale data mining: a survey,” *Artif. Intell. Rev.*, vol. 52, pp. 77–124, 2019.
[20] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan, “Harnessing artificial intelligence capabilities to improve cybersecurity,” *Ieee Access*, vol. 8, pp. 23817–23837, 2020.
[21] M. Jaiswal, “CYBERCRIME CATEGORIES AND PREVENTION,” *Manishaben Jaiswal," CYBERCRIME Categ. Prev. Int. J. Creat. Res. Thoughts (IJCRT), ISSN*, pp. 2320–2882, 2019.

[22] J. Bharadiya, "Machine Learning in Cybersecurity: Techniques and Challenges," *Eur. J. Technol.*, vol. 7, no. 2, pp. 1–14, 2023.
[23] S. K. Hassan and A. Ibrahim, "The role of Artificial Intelligence in Cyber Security and Incident Response," *Int. J. Electron. Crime Investig.*, vol. 7, no. 2, 2023.
[24] R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3, no. 1, pp. 1–18, 2020.
[25] J. N. Paredes, J. C. L. Teze, G. I. Simari, and M. V. Martinez, "On the importance of domain-specific explanations in AI-based cybersecurity systems (technical report)," *arXiv Prepr. arXiv2108.02006*, 2021.