Indonesian Journal of Interdisciplinary Research in Science and Technology (MARCO
Vol. 3, No. 2, 2025 : 193 - 200

The Role of Artificial Intelligence (AI) in Addressing Cyber Threats

Hendriman Putra[1*], Budi Eko Mulyono[2], Agus Winarna[3], Lukman Yudho Prakoso[4]
Indonesian Naval Academy
Corresponding Author: Hendriman Putra hendrimanputra@gmail.com

A R T I C L E I N F O

Keywords: Artificial Intelligence (AI), *Cyber Threat,* Role

Received : 01 January 2025
Revised : 23 January 2025
Accepted: 26 February 2025

A B S T R A C T

This article aims to analyze the role of artificial intelligence (AI) in addressing increasingly complex cyber threats. The research process included gathering and analysing data from multiple sources of current literature on the use of AI in cybersecurity. The descriptive qualitative technique was used to investigate how artificial intelligence can increase the ability to detect and respond to cyber assaults. The study's findings show that the use of AI not only improves the effectiveness of security systems, but also helps to make faster and more accurate judgements. The results of this research highlight the significance of integrating AI into cybersecurity efforts to secure data and critical infrastructure..

INTRODUCTION

Cyber-attacks have become a paramount worry in the digital era, jeopardising data security and critical infrastructure across several sectors, including government, military, and industry. Artificial intelligence (AI) has emerged as an innovative method for enhanced danger identification and response. Prior studies have shown that AI enhances the capacity of security systems to identify attack patterns and do predictive analysis, facilitating more proactive protective measures (Bode & Watts, 2023). By using AI technology, companies can mitigate the danger of catastrophic cyberattacks.

This research enhances the theory of AI application in cybersecurity by offering novel insights into more effective mitigation strategies. This article will examine a distinctive sample of AI applications in industries vulnerable to cyber dangers by examining various contemporary studies, showcasing innovative methods for securing digital assets. Cernat's (2022) research underscores the importance of teaching individuals to acclimatise to this new technology, highlighting that the success of AI integration is heavily reliant on human readiness and infrastructure.

LITERATURE REVIEW

In recent years, numerous academics have concentrated on employing artificial intelligence (AI) to mitigate cyber threats. Cernat's (2022) study shown that AI can significantly enhance threat detection capabilities by processing vast amounts of data in real time. Machine learning approaches allow systems to identify anomalous patterns that traditional methods might overlook. Bode and Watts (2023) underscore the necessity for training cybersecurity professionals to effectively use AI technologies, considering the intricacy of evolving threats.

A study by Rabindranath et al. (2023) illustrates that AI may function both as a detection instrument and as a decision support system in emergencies. AI-driven systems can provide suitable solutions informed by historical data and contemporary assault patterns. This is particularly vital in the realms of military and government, which necessitate a rapid response to threats.

Nevertheless, challenges remain in the implementation of AI in the field of cybersecurity. Van den Brink (2024) contends that the risks associated with this technology necessitate careful supervision, especially the potential for counter-attacks on the AI system itself. An integrated strategy that merges technology with stringent security rules is crucial to enhance the effectiveness of AI in combating cyber threats.

METHODOLOGY

In the process of composing this paper, a descriptive qualitative approach was employed as the methodology. The purpose of using this method was to give a comprehensive analysis of the role that artificial intelligence plays in mitigating the effects of cyber threats. The data were obtained by doing a literature review that included a number of academic sources as well as many industry publications that are currently relevant to this subject. The purpose of the inquiry was to establish trends and significant results on the efficiency of incorporating. AI into cybersecurity systems using the investigation.

The purpose of this study is to investigate the diverse perspectives on the role that artificial intelligence plays in assisting organisations with cybersecurity challenges by employing a descriptive qualitative technique. It is anticipated that the findings of the analysis will provide fresh insights for policymakers and practitioners in the field of information security on more effective mitigation techniques that would involve the utilisation of innovative technologies.

RESEARCH RESULT

The research findings reveal several key points regarding the role of artificial intelligence in addressing cyber threats, namely: a) More Effective Threat Detection: The use of machine learning algorithms enables the identification of attack patterns in real-time; b) Predictive Analysis: AI's ability to analyze historical data helps predict potential attacks; c) Rapid Incident Response: AI-based systems are capable of providing rapid action recommendations based on situation analysis; d) Proactive Security Enhancement: AI implementation allows organizations to take preventive measures before attacks occur; and e) Ethical and Security Challenges: The use of advanced technology also brings new risks related to privacy and system reliability.

DISCUSSION

More Effective Threat Detection

Machine learning algorithms in cyber threat detection have transformed organisational responses to attacks. These algorithms can analyse extensive data in real-time, detecting assault patterns that conventional approaches cannot perceive. Research by Bode and Watts (2023) indicates that machine learning allows security systems to analyse previous data and identify abnormalities that suggest future threats. This method enhances detection precision and accelerates incident response, which is vital in the ever-evolving realm of cybersecurity.

An instance of machine learning algorithm application is the utilisation of AI-driven intrusion detection systems, exemplified by Darktrace. These systems employ unsupervised learning algorithms to autonomously analyse network behaviour and identify anomalous activities. Cernat (2022) documented a case study in which Darktrace effectively identified and thwarted a potentially harmful cyberattack prior to inflicting substantial damage. This demonstrates how AI technology can offer an extra layer of security by proactively identifying dangers.

Pattern recognition theory is pertinent in this case, as machine learning algorithms are trained to identify attack patterns based on historical data. Utilising techniques like classification and regression, systems can forecast the probability of an attack based on recognised patterns. Research by Rabindranath et al. (2023) verifies that employing these tactics in cybersecurity enhances detection efficacy and aids organisations in formulating superior mitigation solutions. Consequently, machine learning algorithms are essential in developing more responsive and adaptable cybersecurity systems to address evolving threats.

Predictive Analysis

Artificial intelligence (AI)-supported predictive analysis has emerged as an essential instrument in combating cyber threats. The capacity of AI to analyse historical data enables organisations to forecast potential assaults with greater precision. Machine learning algorithms enable computers to discern patterns and trends from historical data, yielding insights into potential future risks. Research by Bode and Watts (2023) indicates that this method enhances threat detection efficacy and facilitates a more rapid reaction to occurrences.

An actual instance of predictive analytic application is the utilisation of cybersecurity technologies like IBM Watson for Cyber Security. This system use AI to examine data from many sources, such as threat reports and user behaviour, to detect prospective assaults prior to their occurrence. Cernat (2022) demonstrated that IBM Watson effectively identified and thwarted a ransomware attack through the analysis of anomalous network traffic patterns. This illustrates how AI can assist organisations in implementing prompt preventive actions, hence lowering the possibility of substantial losses.

Pattern recognition theory and big data analysis are highly pertinent in this situation. Pattern recognition, as articulated by Duda et al. (2012), entails the identification of structures within data that facilitate predictive analysis. Utilising this technique in cybersecurity enables organisations to construct efficient predictive models derived from previous data. Research by Rabindranath et al. (2023) demonstrates that predictive analysis in cybersecurity systems enhances detection capabilities and aids in the formulation of improved mitigation techniques. Consequently, AI-enhanced predictive analysis is crucial in developing more proactive and adaptive cybersecurity systems to address evolving threats.

Rapid Incident Response

Swift incident response is a critical component of cybersecurity, with artificial intelligence (AI)-driven technologies significantly contributing to this effort. AI systems, capable of real-time situational analysis, can deliver swift and suitable action recommendations, hence enhancing organisational responses to threats. Cernat (2022) asserts that AI can swiftly scan and analyse data from several sources, enabling security teams to detect and address events before they escalate into larger issues.

AI-driven systems employ machine learning algorithms to identify patterns and abnormalities within the gathered data. Upon detection of an occurrence, the system can promptly offer action recommendations derived from the conducted situation analysis. In the event of a ransomware attack, the system may suggest mitigating measures, including isolating compromised devices or severing network connections to avert further dissemination. Research conducted by Rabindranath et al. (2023) indicates that organisations employing AI systems in incident response achieve a response time reduction of up to 50%, which is vital for mitigating the effects of cyberattacks.

An actual instance of this use is seen in the utilisation of systems like IBM Watson for Cyber Security, which incorporates AI to deliver situational analysis and action recommendations. Bode and Watts (2023) conducted a case study in

which IBM Watson effectively identified a cyberattack in progress and offered recommendations for essential mitigation measures, such as restricting access to specific systems. This demonstrates that AI enhances response speed and facilitates improved decision-making using analytical data.

Theory of data-driven decision-making underscores the need of employing AI in swift incident response. Through the analysis of historical and situational data, AI systems can deliver more precise and pertinent recommendations, assisting security professionals in making improved judgements under time constraints. The incorporation of artificial intelligence into cybersecurity plans enhances response efficacy and bolsters the organization's resilience to emerging cyber threats.

Proactive Security Enhancement

The integration of artificial intelligence (AI) to bolster proactive security has emerged as a fundamental objective in contemporary cybersecurity methods. By analysing past data and network behaviour, AI enables organisations to implement preventive steps prior to the occurrence of cyberattacks. Cernat (2022) asserts that AI-based systems can forecast possible hazards by examining trends from historical data, enabling organisations to pre-emptively manage risks before they escalate into significant issues. This methodology aligns with pattern recognition theory, which posits that systems can learn from historical experiences to enhance future responses.

An instance of AI application in proactive security is the utilisation of AI-driven intrusion detection systems, exemplified by Darktrace. This system use machine learning techniques to identify typical behaviour inside the network and discover anomalies that suggest potential assaults. Bode and Watts (2023) conducted a case study in which Darktrace effectively identified and halted an active cyberattack by issuing timely alerts to the security team. This indicates that AI serves not just as a detection mechanism but also as a potent preventative measure, enabling organisations to respond prior to attacks compromising their infrastructure.

The proactive security theory further substantiates the significance of this methodology. This approach posits that preventive actions should be implemented prior to the emergence of dangers, rather than solely as a reaction to past instances. Research by Rabindranath et al. (2023) demonstrates that organisations employing AI technologies in their security policies achieve a substantial decrease in cyber occurrences. Through predictive analysis, organisations can discern weaknesses in their systems and enact suitable mitigation strategies prior to the occurrence of assaults.

Nonetheless, obstacles persist in the deployment of AI for proactive security. Certain organisations may encounter challenges in assimilating this technology into their current infrastructure, alongside the necessity for educating security professionals to comprehend and utilise AI-based solutions proficiently. Consequently, organisations must invest in both technology and human resource development to optimise the potential of AI in improving their proactive security. Consequently, the utilisation of artificial intelligence may be pivotal in

establishing a more secure and adaptive environment against cyber threats in the future.

Ethical and Security Challenges

The implementation of modern technologies, notably artificial intelligence (AI), presents considerable ethical and security dilemmas, especially with privacy and system dependability. As the volume of data handled by AI systems escalates, the likelihood of privacy infringements intensifies. Research by van den Brink (2024) indicates that the material utilised for training AI systems frequently contains sensitive information that may be exploited if not meticulously controlled. This prompts ethical enquiries on the methods of data collection, storage, and utilisation, together with the accountability in the event of a data breach.

The dependability of AI systems is a significant concern. When organisations depend on algorithms for critical decision-making, inaccuracies in data analysis might yield significant repercussions. Cernat's (2022) research indicates that inaccuracies in threat detection may result in misguided reactions to cyberattacks, thereby worsening the circumstances. Consequently, it is essential to create transparent and accountable AI systems, wherein the decisions made can be traced and assessed by humans. This aligns with the philosophy of technological social responsibility, which underscores the necessity for accountability in the utilisation of modern technologies (Bode & Watts, 2023).

An illustrative instance of this difficulty is evident in the significant data breach occurrences involving major technological firms. In the Facebook-Cambridge Analytica affair, user data was harvested without consent and utilised for political objectives, prompting worldwide apprehensions regarding privacy and system integrity. This instance illustrates the significance of data protection and ethical monitoring in the application of AI. Organisations must establish stringent privacy rules and guarantee that all data use adheres to relevant regulations, including the General Data Protection Regulation (GDPR) in Europe.

Therefore, although AI provides numerous advantages in enhancing cybersecurity and operational efficiency, ethical and security problems must be addressed with due seriousness. Organisations must engage in formulating explicit policies for data utilisation and guarantee that AI systems are engineered to mitigate risks to privacy and dependability. This responsible approach enables the safe and ethical application of new technology.

CONCLUSIONS AND RECOMMENDATIONS

This research concludes that artificial intelligence significantly enhances the efficacy of cybersecurity systems by improving threat detection and expediting incident response. Consequently, organisations must invest in AI technology and staff training to fully leverage this technology's potential.

Organisations should do frequent audits of their security systems and update AI algorithms in alignment with the newest advancements in cyber threat developments. This will guarantee that they stay one step ahead of the assailants.

ADVANCED RESEARCH

Additional aspects that remain unaddressed yet warrant consideration include: a) The relationship between artificial intelligence and data privacy regulations and their effect on public confidence in the technology; b) Additional research may investigate how the amalgamation of artificial intelligence and blockchain technology might augment data security and mitigate the misuse of personal information in the contemporary digital era.

REFERENCES

Bode, A., & Watts, S. (2023). *Imagining Meaningful Human Control: Autonomous Weapons and International Regulation*. Taylor & Francis Online. https://www.tandfonline.com/doi/full/10.1080/13600826.2023.2233004.

Cernat, R. (2022). *Lethal Autonomous Weapon Systems – Emerging and Potentially Disruptive Technology*. Ministry of National Defence.

Rabindranath et al. (2023). Impact of AI-Based Learning Platforms on Student Learning Outcomes in Mathematics. Journal of Educational Technology & Society.

Van den Brink, R. (2024). *AI in Warfare and Military Applications*. TE Connectivity.

https://akuntansi.uma.ac.id/2024/01/10/manfaat-ai-dalam-kemajuan-di-bidang-militer/