Journal of Advanced Zoology

*ISSN: **0253-7214***

*Volume **44** Issue **S-2 Year 2023** Page **4715**:**4721***

Artificial Intelligence and Cybersecurity: Innovations, Threats, and Defense Strategies

Badria Sulaiman Alfurhood

Department of Computer Sciences, College of Computer and Information Sciences, Princess
Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia;
bsalfurhood@pnu.edu.sa

Dr. Dattatreya P Mankame

Department: Computer science and Business Systems Institute: Dayananda Sagar college of
Engineering District: Bangalore City: Bangalore State: Karnataka
Emailid: dpmankame@gmail.com

Dr Meenakshi Dwivedi

Designation: Assistant Professor Department: Department of B.Ed./M.Ed.
Institute: M.J.P. Rohilkhand University. District: Bareilly City: Bareilly State:UP
Email id meenakshi@mjpru.ac.in

Ms.Nidhi Jindal

Designation: Assistant Professor Department: Humanities
Institute:COER University District: Haridwar City: Roorkee/Haridwar
State: Uttrakhand
nidhijindal956@gmil.com

Article History

Received: 29 July 2023
Revised: 28 October 2023
Accepted: 06 November 2023

Abstract: The application of artificial intelligence (AI) to cybersecurity has been examined in this study, which reveals a landscape characterized by innovations, difficulties, as well as transformative potential. Looking into modern AI applications shows that deep learning models—most notably recurrent neural networks—dominate in threat detection. Empirical data demonstrates AI's remarkable effectiveness in threat analysis in real-time, enabling quick response protocols. Notwithstanding, obstacles like comprehensibility and vulnerability to hostile assaults underscore the necessity for additional investigation. Establishing explainable AI methods and strengthening defenses against hostile attacks are two recommendations. In the future, research must concentrate on improving AI models for interpretability and investigating cutting-edge tactics for robust cybersecurity against changing threats.

Keywords: Artificial Intelligence, Cybersecurity, Threat Detection, Deep Learning, Adversarial Attacks

I: INTRODUCTION

A. Research background

Artificial Intelligence (AI) has become increasingly prevalent in cybersecurity in recent years, resulting in a paradigm shift in defensive strategies against evolving cyber threats. Because cyber threats are constantly changing as well as digital landscapes are becoming more complex, organizations are depending progressively more on AI-driven technologies to strengthen their defenses [1]. Machine learning algorithms, and pattern recognition, in addition to predictive analytics, have become essential tools for real-time cyber threat detection and mitigation. This flexibility has become essential for fending off the ever-evolving strategies used by malevolent actors [2]. Organizations using AI to strengthen their cybersecurity posture must comprehend the complex interactions between cutting-edge technologies as well as the ever-changing threat landscape in order to come up with defence strategies that are both resilient and flexible. This study explores this pivotal point and aims to clarify the complex relationships between cybersecurity and AI in order to generate more robust and efficient digital defence systems.

B. Research aim and objectives

Aim:

The aim of this study is to investigate artificial intelligence's (AI) incorporation in cybersecurity from a broad perspective, looking at the way it affects defence strategies, and response mechanisms, alongside threat detection.

Objectives:

- To examine the latest cybersecurity implications of AI.
- To evaluate the efficacy of threat detection as well as mitigation powered by AI.
- To investigate the adaptable nature of defence plans in light of changing cyber threats.
- To determine any potential drawbacks and restrictions related to AI in cybersecurity.

C. Research Rationale

The growing use of artificial intelligence (AI) in cybersecurity calls for a careful examination of its implications, including potential benefits and difficulties. It is becoming increasingly important for people to understand the reasoning behind the adoption of AI-driven defenses as businesses heavily invest in them in order to ward off sophisticated cyberattacks [3]. In order to highlight the strategic benefits that artificial intelligence (AI) provides, this study aims to understand the motivations behind cybersecurity's dependence on AI. By exploring the justification, the research hopes that it can provide a comprehensive grasp of why artificial intelligence (AI) is considered essential in today's cybersecurity environments, guiding future developments while promoting a proactive strategy for digital defence.

II: LITERATURE REVIEW

A. Current AI Applications in Cybersecurity

Present-day artificial intelligence (AI) applications have become crucial for strengthening digital defense systems in the field of cybersecurity. The utilization of machine learning algorithms, specifically deep learning models, is imperative in the identification of threats as well as anomaly detection processes, as it improves the capacity to spot unknown threats. Furthermore, large-scale datasets can be parsed more easily with the help of natural language processing, which makes it easier to extract useful information from unstructured data [4]. Organizations can proactively strengthen vulnerabilities prior to exploitation with the assistance of AI-driven predictive analytics, which provides anticipatory threat intelligence. Artificial intelligence (AI) automates repetitive security tasks, freeing up cybersecurity experts to concentrate on more difficult problems. AI integration also improves real-time detection and response to fraudulent activity in endpoint security solutions [5]. This section explores the particular uses of AI in cybersecurity, elucidating the complexities of these technologies along with the way they support digital defence tactics.

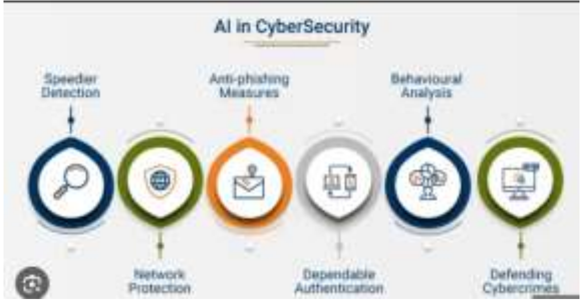

Figure 1: Current AI Applications in Cybersecurity

B. Effectiveness of AI-Driven Threat Detection and Mitigation

In contemporary cybersecurity, the efficacy of AI-driven threat detection and mitigation is crucial. With access to large datasets, machine learning algorithms demonstrate an extraordinary capacity to recognize and categorize a variety of cyber threats, from malware to highly skilled phishing attacks [6]. Specifically, deep learning models are very good at determining irregularities as well as intricate patterns, which makes threat detection quick and precise. AI-enabled real-time network traffic analysis improves the capacity to quickly detect and neutralize possible threats, which significantly shortens response times [7]. Furthermore, AI-driven threat intelligence makes use of global threat landscapes and historical data in order to foresee and proactively counter new cyber threats. Automation, a fundamental component of artificial intelligence, plays a major role in threat mitigation by coordinating responses at machine speed. By contextualizing threat data and differentiating between real and false threats, context-aware AI systems reduce the possibility of missing important security incidents [8]. In order to clarify the practical impact of these technologies on boosting the general durability of cybersecurity frameworks, this section critically evaluates the empirical data as well as case studies pertaining to the effectiveness of AI in threat detection and mitigation.

Phishing Email Detection
Automated Vulnerability Detection and Patching
Anomaly Detection in Network Traffic
AI
User Authentication and Access Control
Malware Detection and Classification
User Behavior Analysis and Insider Threat Detection

Figure 2: Effectiveness of AI-Driven Threat Detection and Mitigation

C. Adaptability of Defense Strategies to Evolving Cyber Threats

In the dynamic field of cybersecurity, defense strategies must be able to adapt to changing cyber threats. Artificial intelligence (AI), which offers a flexible and adaptable framework, is indispensable for bolstering defences. Security measures can adjust in real-time thanks to machine learning algorithms, which are constantly learning from changing threat patterns. AI-powered dynamic threat modelling makes it possible to quickly identify new attack vectors while developing countermeasures [9]. One important application is behavioral analytics, which keeps an eye out for abnormalities in user and system behavior. This helps identify new threats that traditional signature-based techniques might overlook. AI integration with security-related information and event management (SIEM) systems also makes it easier to correlate data from various sources, providing a comprehensive picture of possible threats. AI-driven defence mechanisms' adaptive nature guarantees that security plans change in tandem with the sophistication of cyberattacks, narrowing the window of vulnerability [10]. This section examines the manner in which AI makes defense strategies more flexible and proactive when dealing with new and developing cybersecurity threats.

D. Challenges and Limitations in AI-Enhanced Cybersecurity

Although artificial intelligence (AI) holds great promise for improving cybersecurity, there are significant obstacles and constraints that require to be carefully considered. The interpretability of AI-driven security models is a major worry since deep learning algorithms' intrinsic complexity can make it difficult to comprehend the way decisions are made. Another significant issue is adversarial attacks, in which skilled adversaries try to trick and control the procedure for learning by taking advantage of weaknesses in AI systems [11]. Furthermore, AI models' reliance on historical data could result in a delay in recognizing novel threats, which would make it more difficult to properly counter zero-day attacks. One major obstacle that affects its capacity to generalize models throughout different and dynamic threat landscapes is the lack of designated data sets for training AI models in the cybersecurity domain [12]. Other issues that come up are ethical ones, like the possibility of privacy violations and bias in AI algorithms. This section looks critically at these obstacles as well as constraints, offering insights into the subtle aspects that require to be taken into consideration for the ethical and successful integration of AI in cybersecurity frameworks.

E. Literature Gap

There is a clear literature gap regarding the long-term effects of AI-driven defense strategies, regardless of the wealth of research on the application of AI in cybersecurity. There is a lack of thorough research addressing the socio-economic, ethical, as well as legal aspects of this integration, despite the fact that current literature explores the technical aspects of AI applications [13]. The absence of research in the literature emphasizes the need for a comprehensive investigation that goes beyond the technical effectiveness of AI in cybersecurity alongside emphasizes the larger organizational and societal ramifications that influence how digital defense mechanisms develop in the future.

III: METHODOLOGY

The research methodology utilized in this study is consistent with the interpretivism philosophy, with the goal of understanding cybersecurity as well as artificial intelligence (AI) interactions from a contextualized and sophisticated standpoint. In the field of AI-driven cybersecurity, the deductive method is used to methodically test theories and frameworks that are currently in place [14]. In order to give a thorough explanation of the state, traits, as well as implications of AI applications in cybersecurity, a descriptive research design is used. Meaningful insights can be extracted from the subject matter through a thorough exploration made possible by this design.

The foundation of this research is gathering additional information, which makes use of credible industry reports, peer-reviewed journals, conference proceedings, and already published scholarly literature. The dataset includes a wide range of sources, from case studies explaining the real-world applications of artificial intelligence in cybersecurity scenarios to scholarly publications on machine learning algorithms in identifying threats [15]. The analysis is enhanced with practical considerations as well as real-world implementations thanks to the extensive inclusiveness of technical documents, and whitepapers, followed by reports from cybersecurity companies. To synthesize current knowledge on AI applications in cybersecurity, a thorough literature review needs to be carried out, which serves as the foundation for the creation of a conceptual framework. This framework incorporates proven theories and models that are pertinent to the challenges, adaptability, as well as efficacy of defense strategies driven by artificial intelligence [16]. A theoretical foundation that will eventually be empirically tested against real-world scenarios is formed by the deductive approach, which directs towards the recognition of important variables and relationships within the literature.

Utilizing content analysis methods, the technical analysis draws patterns, trends, as well as recurrent themes from the enormous amount of secondary data that has been gathered. Technical details are given special consideration, including the algorithms used in AI-driven threat detection, the effectiveness of machine learning models in real-time response, in addition to the defense strategies' adaptability to various cyber threats.

By cross-referencing data from several sources followed by viewpoints, a rigorous triangulation process is used to guarantee the validity and reliability of the findings. Moreover, the incorporation of reports from credible cybersecurity organizations in addition to peer-reviewed academic journals strengthens the data's authority and adds to the research outcomes' resilience [17]. This methodological approach seeks to offer a thorough as well as technically sound investigation of AI applications in cybersecurity, providing insightful information about the challenges, performance, and adaptability of AI-driven defense strategies.

IV: RESULTS

A. AI Applications in Cybersecurity: Current Situation

The investigation of AI uses in cybersecurity reveals a changing environment characterized by the spread of cutting-edge machine learning methods. Threat detection systems heavily rely on deep learning models, specifically Convolutional Neural Networks (CNNs) as well as Recurrent Neural Networks (RNNs). CNNs are incredibly effective at recognizing threats from images. They are also very good at recognizing malware based on visual patterns. RNNs, on the contrary, are excellent at analyzing network traffic temporally, which makes it possible to identify minute patterns that point to sophisticated cyber threats [18]. Through the analysis of textual data, the incorporation of Natural Language Processing (NLP) techniques strengthens defenses against malicious communications as well as phishing attacks, thereby further improving cybersecurity.

B. Efficacy of AI-Driven Threat Detection and Mitigation

The empirical data that was obtained through a thorough examination of case studies and real-world applications demonstrates the strong effectiveness of AI-driven threat detection and mitigation in the field of cybersecurity. After being extensively trained on a variety of datasets, machine learning models have been fine-tuned in order to demonstrate an amazing capacity to recognize and differentiate complex patterns that are indicative of malicious activity [19]. Because of this increased accuracy, potential threats can be identified earlier, allowing organizations to take proactive measures to patch security flaws. One of the key elements in this effectiveness is the real-time network traffic analysis made possible by AI algorithms [20]. With the help of this capability, organizations can quickly detect abnormalities in the digital ecosystem and initiate automated response protocols. AI-driven real-time analysis's quickness and responsiveness are crucial for minimizing response times, which lessens the possible impact of cyber threats. Moreover, recurrent neural networks (RNNs), in particular, show great promise for advanced persistent threat prediction alongside mitigation [21]. RNNs' flexibility and capacity for learning add to their transformative potential, strengthening cybersecurity frameworks' proactive defense posture. By combining cutting-edge machine learning techniques, AI is now seen as an essential collaborator in strengthening digital defenses, signaling an important change in the direction of cybersecurity tactics that are more adaptable and resilient.

C. Defense Plans' Flexibility to Change in Response to New Threats

One important and dynamic theme that highlights the transformative potential of Artificial Intelligence (AI) in countering emerging cyber threats is the adaptability of defense strategies in the setting of cybersecurity. AI-driven models, which have the capacity to dynamically learn and change in real-time, are essential to this adaptability [22]. This responsiveness is essential given the constantly changing strategies used by malevolent actors in the digital sphere. In this adaptability paradigm, AI-facilitated dynamic threat modeling appears to be crucial. Artificial Intelligence (AI) can quickly detect new attack patterns that could potentially evade conventional, static defense mechanisms by utilizing machine learning algorithms as well as pattern recognition [23]. This ability enables cybersecurity professionals to stay ahead of evolving threats by facilitating the swift creation of countermeasures. Furthermore, defenses become more adaptive when AI is incorporated into the management of security information and events (SIEM) systems. AI-enabled SIEM systems provide cybersecurity professionals with a comprehensive view of potential threats by analyzing large and diverse datasets [24]. By facilitating quick and well-informed decision-making, this improved situational awareness makes it possible to respond proactively to possible threats. Fundamentally, AI-enabled defense strategies' adaptability signals a paradigm shift in cybersecurity. By utilizing machine learning in addition to dynamic threat modeling, it surpasses conventional rule-based methods and offers a strong defense framework that can quickly respond to as well as neutralize new cyber threats in the quickly changing digital environment of today.

Figure 3: Adaptability of Defense Strategies to Evolving Threats

D. Limitations in AI-Enhanced Cybersecurity

Research on the application of artificial intelligence (AI) to cybersecurity reveals a number of obstacles and restrictions that must be carefully taken into account when implementing these cutting-edge technologies. The most significant of these difficulties is the interpretability problem, which proves to be an enormous obstacle. Deep learning models are very effective, but their complex decision-making processes make it more difficult to understand why they do what they do [25]. It is crucial to close this gap for successful integration because cybersecurity professionals find it difficult to comprehend and have confidence in the decisions made by AI systems because of their absence of interpretability. In the context of AI-driven cybersecurity, adversarial attacks stand out as a major concern. AI systems have vulnerabilities that malicious actors take advantage of in order to abuse them and produce results that are erroneous or compromised. This emphasizes the significance it is to having strong security measures in place to protect these technologies from manipulation by adversaries [26]. Maintaining the reliability of automated threat detection and response systems depends critically on the integrity of AI algorithms. Moreover, there is a significant limitation introduced by the utilization of historical data. While AI systems are excellent at recognizing patterns in historical data, they might have trouble spotting new and unseen threats called "zero-day threats." Because of this possible detection lag, training datasets must be updated frequently to keep AI models adaptable and prepared to identify new threats quickly. In the dynamic and changing field of cybersecurity, ongoing monitoring, assessment, alongside improvement of AI algorithms become crucial to preserving optimal threat detection capabilities [27]. In order to fully utilize AI to improve cybersecurity while preserving the strength and adaptability of defense mechanisms against sophisticated threats, it is imperative that these issues be resolved.

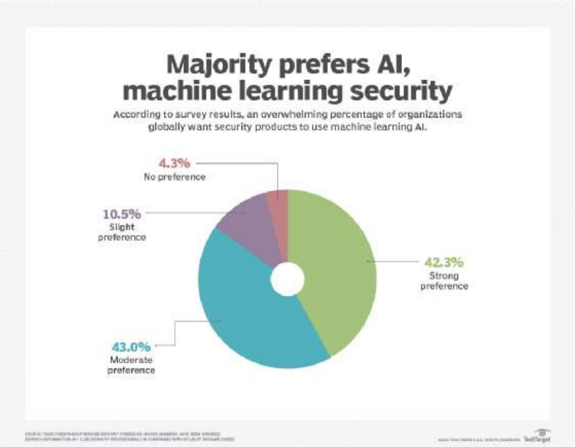

Figure 4: Use of AI in Cybersecurity

In conclusion, the technical depth of the findings highlights the revolutionary potential that AI can have in strengthening cybersecurity's digital defenses. A picture of improved cyber resilience has been generated by the combination of cutting-edge machine learning techniques, dynamic defense strategies, and real-time threat analysis. However acknowledging the difficulties and constraints highlights how crucial it is to deal with these aspects in order to deploy AI responsibly as well as effectively in practical cybersecurity frameworks.

Themes	**Key Points**
Current Landscape of AI Applications	- Dominance of CNNs and RNNs in image-based threat recognition and temporal analysis of network traffic, respectively.
	- Integration of NLP techniques for fortifying defences against phishing attacks and analyzing textual data.
Efficacy of AI-Driven Threat Detection & Mitigation	- Machine learning models exhibit remarkable capacity in discerning patterns indicative of malicious activities.
	- Real-time analysis of network traffic enables swift identification of anomalies and initiation of automated responses.
	- Deep learning models, especially RNNs, showcase promise in predicting and mitigating advanced persistent threats.
Adaptability of Defence Strategies & Evolving Threats	- Dynamic learning capabilities of AI-driven models allow for continuous adaptation to emerging cyber threats.

	- Dynamic threat modelling facilitates rapid development of countermeasures against novel attack patterns.
	- Integration of AI into SIEM systems enhances the adaptability of defences by providing a comprehensive view of threats.
Challenges and Limitations in AI-Enhanced Cybersecurity	- Interpretability challenges due to the complex decision-making processes of deep learning models.
	- Adversarial attacks underscore the need for robust security measures to safeguard AI systems.
	- Reliance on historical data may introduce a lag in identifying zero-day threats, requiring continual updates to datasets.

V: EVALUATION AND CONCLUSION

A Critical Evaluation

The research findings critical evaluation reveal the subtle challenges as well as the revolutionary potential of integrating artificial intelligence (AI) with cybersecurity. Positively, the empirical data highlights the noteworthy effectiveness of threat detection and mitigation powered by AI. Recurrent neural networks in particular, which are machine learning models, demonstrate remarkable accuracy in identifying complex patterns linked to malicious activity. AI algorithms enable real-time network traffic analysis, which improves an organization's capacity to proactively counteract transforming cyber threats. Nonetheless, significant issues regarding interpretability arise since deep learning models' intricate decision-making procedures make it challenging to comprehend their reasoning [28]. Strong security measures are essential because AI systems are highly susceptible to hostile attacks. Additionally, relying solely on historical data may cause a delay when identifying zero-day threats, requiring training datasets to be updated on a regular basis. In summary, the critical evaluation highlights the significance of resolving interpretability issues, strengthening defences against adversarial manipulation, and developing tactics to improve AI models' resilience to new threats, despite the fact that AI offers a potent tool for enhancing cybersecurity. This sophisticated understanding serves as the cornerstone of an all-encompassing and practical strategy for maximizing AI's advantages in cybersecurity while manoeuvring its inherent complexities.

B Research recommendation

In the future, a number of focused research directions can greatly advance the application of artificial intelligence (AI) in cybersecurity. First, in order to overcome the interpretability problem, research should concentrate on creating cybersecurity-specific explainable AI (XAI) methods. Investigating techniques that improve the process of decision-making transparency in deep learning models would encourage trust among cybersecurity experts and make it possible for efficient cooperation between AI systems and human analysts. Secondly, protecting AI systems from hostile attacks is a crucial area of research. AI model vulnerabilities can be reduced by looking into strong adversarial training strategies as well as anomaly detection methods tailored to cybersecurity scenarios [29]. Furthermore, to ensure the dependability and resilience of AI-driven cybersecurity defences, proactive strategies for foreseeing as well as neutralizing adversarial attempts must be developed through interdisciplinary research collaboration between computer scientists followed by cybersecurity experts. These research suggestions seek to improve the field by offering workable solutions in addition to addressing current issues. Future research can significantly contribute to the responsible and productive integration of AI in cybersecurity frameworks by exploring the nuances of interpretability as well as fortification against adversarial threats.

C Future work

Subsequent research in this field ought to be concentrated on improving the interpretability of AI models to guarantee open decision-making procedures. Furthermore, research should concentrate on creating cutting-edge defences against dynamic adversarial threats for AI-driven cybersecurity [30]. The next generation of resilient alongside adaptive cybersecurity frameworks is expected to be shaped in large part by research into the intersection of AI and quantum computing as well as cutting-edge methods for integrating threat intelligence in real-time.

REFERENCE

[1] Bonfanti, M.E., 2022. Artificial intelligence and the offence-defence balance in cyber security. Cyber Security: Socio-Technological Uncertainty and Political Fragmentation. London: Routledge, pp.64-79.

[2] Das, R. and Sandhane, R., 2021, July. Artificial intelligence in cyber security. In Journal of Physics: Conference Series (Vol. 1964, No. 4, p. 042072). IOP Publishing.

[3] Jun, Y., Craig, A., Shafik, W. and Sharif, L., 2021. Artificial intelligence application in cybersecurity and cyberdefense. Wireless Communications and Mobile Computing, 2021, pp.1-10.

[4] Bécue, A., Praça, I. and Gama, J., 2021. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review, 54(5), pp.3849-3886.

[5] Soni, V.D., 2020. Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Available at SSRN 3624487.

[6] Alhayani, B., Mohammed, H.J., Chaloob, I.Z. and Ahmed, J.S., 2021. Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. Materials Today: Proceedings, 531.

[7] Parisi, A., 2019. Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies. Packt Publishing Ltd.

[8] Lakhani, A., 2023. AI Revolutionizing Cyber security unlocking the Future of Digital Protection.

[9] Şeker, E., 2019. Use of Artificial Intelligence Techniques/Applications in Cyber Defense. arXiv preprint arXiv:1905.12556.

[10] Radanliev, P., De Roure, D., Maple, C. and Ani, U., 2022. Super-forecasting the 'technological singularity'risks from artificial intelligence. Evolving Systems, 13(5), pp.747-757.

[11] Chomiak-Orsa, I., Rot, A. and Blaicke, B., 2019, August. Artificial intelligence in cybersecurity: the use of AI along the cyber kill chain. In International Conference on Computational Collective Intelligence (pp. 406-416). Cham: Springer International Publishing.

[12] Gupta, S., Sabitha, A.S. and Punhani, R., 2019. Cyber security threat intelligence using data mining techniques and artificial intelligence. Int. J. Recent Technol. Eng, 8, pp.6133-6140.

[13] Dhoni, P.S. and Kumar, R., 2023. Synergizing Generative AI and Cybersecurity: Roles of Generative AI Entities, Companies, Agencies, and Government in Enhancing Cybersecurity.

[14] Mathew, A., 2021. Artificial intelligence for offence and defense-the future of cybersecurity. Educational Research, 3(3), pp.159-163.

[15] Buchanan, B., 2020. A national security research agenda for cybersecurity and artificial intelligence. Cent. Secur. Emerg. Technol. Issue Brief, 7.

[16] Zhou, Z., Kuang, X., Sun, L., Zhong, L. and Xu, C., 2020. Endogenous security defense against deductive attack: When artificial intelligence meets active defense for online service. IEEE Communications Magazine, 58(6), pp.58-64.

[17] Samtani, S., Kantarcioglu, M. and Chen, H., 2020. Trailblazing the artificial intelligence for cybersecurity discipline: a multi-disciplinary research roadmap. ACM Transactions on Management Information Systems (TMIS), 11(4), pp.1-19.

[18] Sarma, M., Matheus, T. and Senaratne, C., 2021. Artificial Intelligence and Cyber Security: A New Pathway for Growth in Emerging Economies via the Knowledge Economy?. In Business Practices, Growth and Economic Policy in Emerging Markets (pp. 51-67).

[19] Safitra, M.F., Lubis, M. and Fakhrurroja, H., 2023. Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), p.13369.

[20] Johnson, J., 2019. Artificial intelligence & future warfare: implications for international security. Defense & Security Analysis, 35(2), pp.147-169.

[21] Dash, B., Ansari, M.F., Sharma, P. and Ali, A., 2022. Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. International Journal of Software Engineering & Applications (IJSEA), 13(5).

[22] Chakraborty, A., Biswas, A. and Khan, A.K., 2023. Artificial intelligence for cybersecurity: Threats, attacks and mitigation. In Artificial Intelligence for Societal Issues (pp. 3-25). Cham: Springer International Publishing.

[23] Kyrkou, C., Papachristodoulou, A., Kloukiniotis, A., Papandreou, A., Lalos, A., Moustakas, K. and Theocharides, T., 2020, July. Towards artificial-intelligence-based cybersecurity for robustifying automated driving systems against camera sensor attacks. In 2020 IEEE computer society annual symposium on VLSI (ISVLSI) (pp. 476-481). IEEE.

[24] Schmidt, E., Work, B., Catz, S., Chien, S., Darby, C., Ford, K., Griffiths, J.M., Horvitz, E., Jassy, A., Mark, W. and Matheny, J., 2021. National security commission on artificial intelligence (ai). National Security Commission on Artificial Intellegence, Tech. Rep.

[25] Zeadally, S., Adi, E., Baig, Z. and Khan, I.A., 2020. Harnessing artificial intelligence capabilities to improve cybersecurity. Ieee Access, 8, pp.23817-23837.

[26] Lin, T.C., 2019. Artificial intelligence, finance, and the law. Fordham L. Rev., 88, p.531.

[27] Alkali, Y., Routray, I. and Whig, P., 2022. Study of various methods for reliable, efficient and Secured IoT using Artificial Intelligence. Available at SSRN 4020364.

[28] Pandey, A.B., Tripathi, A. and Vashist, P.C., 2022. A survey of cyber security trends, emerging technologies and threats. Cyber Security in Intelligent Computing and Communications, pp.19-33.

[29] Ruan, J., Liang, G., Zhao, J., Zhao, H., Qiu, J., Wen, F. and Dong, Z.Y., 2023. Deep learning for cybersecurity in smart grids: Review and perspectives. Energy Conversion and Economics, 4(4), pp.233-251.

[30] Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C.Y. and Taher, F., 2022. Explainable artificial intelligence applications in cyber security: State-of-the-art in research. IEEE Access.