Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

AI-Driven Cybersecurity: Balancing Advancements and Safeguards

Atia Shahana[1], Rakibul Hasan[2], Sayeda Farjana Farabi[2], Jahanara Akter[2], Md Abdullah Al Mahmud[3], Fatema Tuz Johora[2], Gurkan Suzer[2]
[1]Department of Business Administration, National University, Dhaka 1230, Bangladesh
[2]Department of Business Administration, Westcliff University, California 90020, USA
[3]Department of Business Administration, International American University, California 90004, USA

Corresponding Author: Rakibul Hasan, **E-mail**: r.hasan.179@westcliff.edu

| ABSTRACT
As Artificial Intelligence (AI) continues its rapid evolution, its profound influence on cybersecurity becomes increasingly evident. This study delves into the pivotal role of AI in fortifying cybersecurity measures, emphasizing its capacity for enhanced threat detection, automated response mechanisms, and the development of resilient security frameworks. However, alongside its promise, recognition of AI's susceptibility to exploitation in sophisticated cyber-attacks exists, underscoring the imperative for continual advancements in AI-driven security solutions. This research offers a nuanced perspective on AI's impact on cybersecurity, advocating for the proactive integration of AI strategies, sustained research efforts, and formulating ethical guidelines. Adopting supervised machine learning (ML) algorithms like decision trees, support vector machines, and neural networks aims to harness AI's potential to bolster cybersecurity while concurrently addressing associated risks, paving the way for a secure digital landscape. Regarding accuracy, the neural network outperforms other models by 98%.

| KEYWORDS

Artificial Intelligence; Cybersecurity; Threat Detection; Decision Trees, Support Vector Machines, Neural Networks.

| ARTICLE INFORMATION

ACCEPTED: 15 April 2024 **PUBLISHED:** 10 May 2024 **DOI:** 10.32996/jcsts.2024.6.2.9

1. Introduction

In the contemporary era, the pervasive integration of digital technologies has revolutionized nearly every facet of human society. From the seamless connectivity enabled by cloud computing to the intricate network of interconnected devices forming the Internet of Things (IoT) (Lacka & Wong, 2021), our dependence on digital infrastructure has become intrinsic to modern life. These advancements have brought about unparalleled efficiency, productivity, and interconnectedness, fundamentally altering how business, communication, and engagement can be conducted worldwide (Urbinati et al., 2020). However, within this digital transformation lurks a shadowy underbelly marked by the looming specter of cyber threats (Couretas, 2022). With each stride in technology, malicious actors - ranging from lone hackers to sophisticated cybercriminal syndicates and even nation-state adversaries - exploit vulnerabilities within our digital ecosystem to perpetrate various nefarious activities (Mahjabin et al., 2017; Zou et al., 2002). These threats manifest in diverse forms, encompassing ransomware attacks that hold critical data hostage for exorbitant ransoms to intricate phishing schemes aimed at stealing sensitive information or infiltrating networks for espionage purposes. The repercussions of these cyber incursions can be profound and far-reaching, extending beyond mere financial losses to include reputational harm, operational disruptions, and even jeopardizing national security.

In critical sectors such as energy, healthcare, and transportation, the potential ramifications of cyber-attacks on public safety and essential services cannot be overstated (Iyamu et al., 2021). Furthermore, the evolving nature of cyber threats poses a formidable

challenge for defenders, as attackers continuously adapt their tactics to evade existing security measures. Rapid technological innovation exacerbates this challenge, as fresh vulnerabilities surface with each advancement, providing fertile ground for exploitation by malicious entities (Marres, 2012). Consequently, the imperative for robust cybersecurity measures has never been more urgent. Organizations across all sectors must proactively bolster their defenses against cyber threats, employing a multi-layered approach encompassing robust perimeter defenses, continuous monitoring and detection capabilities, and swift incident response protocols. Moreover, cultivating a culture of cybersecurity awareness and resilience among employees and stakeholders is crucial in mitigating the human element in cyber risk.

Anyway, the advent of Artificial Intelligence (AI) signifies a transformative juncture in cybersecurity, heralding a fundamental change in how we combat and address cyber threats (Kaur et al., 2023). Previously confined to science fiction and speculative futurism, AI has transcended its conceptual boundaries to emerge as a tangible and impactful force with deep implications for cybersecurity. In contrast to conventional cybersecurity methods that heavily depend on manual oversight and predetermined rule sets, the advent of AI heralds a new epoch of automated and intelligence-infused defense mechanisms. Central to this paradigm shift are methodologies like Machine Learning (ML) and Deep Learning (DL) (Kaur et al., 2023; Singh & Gupta, 2022), which equip AI systems with the capability to swiftly and comprehensively analyze enormous volumes of data with unparalleled speed and intricacy.

Machine learning algorithms exhibit remarkable proficiency in identifying patterns and correlations within datasets, thereby effectively detecting subtle anomalies that might escape traditional rule-based detection methods (Kaur et al., 2023). Through continuous learning from historical data and adeptness at adapting to evolving threat landscapes, systems powered by machine learning can pinpoint emerging threats with remarkable precision, even without explicit instructions or predefined rules.

Similarly, deep learning, a branch of machine learning inspired by the human brain's neural networks (Borode & Olubambi, 2024), significantly bolsters the capabilities of artificial intelligence in cybersecurity. With intricate neural architectures capable of hierarchical feature extraction and representation learning, deep learning models autonomously discern complex features from raw data (Singh & Gupta, 2022). This enables them to uncover nuanced indicators of compromise that might evade detection by human analysts.

Therefore, integrating AI into cybersecurity holds profound implications that extend across various operational domains. AI is poised to revolutionize critical aspects of cybersecurity operations such as threat detection, vulnerability assessment, and incident response through the fusion of intelligent automation and data-driven decision-making. In threat detection, AI-driven systems can swiftly analyze extensive volumes of network traffic, log data, and security event telemetry in real time, promptly flagging suspicious activities and potential intrusions with unparalleled speed and precision. Furthermore, AI's capacity to contextualize diverse data sources and identify correlations among seemingly disparate events empowers it to recognize subtle indicators of compromise indicative of sophisticated cyber-attacks.

2. Research Significance

In the rapidly evolving landscape of technology, artificial intelligence (AI) stands as a double-edged sword, particularly within cybersecurity. Integrating AI into cybersecurity strategies heralds a revolutionary shift, promising groundbreaking solutions while posing novel challenges. This research paper embarks on a comprehensive exploration of the multifaceted impact of artificial intelligence on cybersecurity, shedding light on its potential to fortify digital defenses and its simultaneous introduction of vulnerabilities. With cybersecurity threats escalating in sophistication, the timely significance of this research is evident, calling for advanced and adaptive countermeasures. The paper's scope encompasses an in-depth analysis of AI's role in bolstering cybersecurity frameworks, its utilization in threat detection and response, and the ethical and security implications intrinsic to AI-driven cybersecurity measures. Moreover, it delves into the adversarial exploitation of AI in cyber-attacks, providing a holistic view of the AI-cybersecurity nexus. Key contributions of this research include a systematic review of current AI technologies in cybersecurity, a critical examination of associated challenges and risks, and a discussion on future directions and strategies for leveraging AI effectively and ethically in cyber defense mechanisms. At its core, the central research question guiding this investigation is: "*How does artificial intelligence impact cybersecurity, both as a tool for enhancing security measures and as a vector for novel cyber threats?*" Through this inquiry, the paper endeavors to offer valuable insights into cybersecurity, fostering a balanced understanding of the integration of artificial intelligence into cyber defense strategies and its implications for the future of digital security.

3. Literature Review : The Impact Of AI On CyberSecurity

3.1 *Previous Research in Cybersecurity*

According to Islam et al. (2023), traditional or mainstream methods for cyberattack detection and mitigation have been the foundation of many businesses' security structures in the rapidly evolving field of cybersecurity. Though they have been crucial in safeguarding digital assets, they have drawbacks and are constantly replaced by more sophisticated strategies like artificial

intelligence and machine learning (Dayyabu et al., 2023). Mhlanga (2021) asserts that firewalls are among traditional cybersecurity's most crucial and widely used elements. Still, they have difficulty identifying and thwarting sophisticated cyberattacks that could exploit security flaws or use encrypted communication to evade scrutiny. Intrusion Detection Systems (IDS) are pivotal in protecting systems from security breaches by monitoring system logs and network traffic to detect suspicious activities and potential attacks. Yet, they face the challenge of frequent false positives, making it difficult for security teams to distinguish genuine threats from harmless events. Similarly, Ryman-Tubb et al. (2018) claim Patch management is a technique for keeping operating systems and applications up to speed with the most recent security upgrades and patches; nonetheless, it is susceptible to exploitation.

3.2 Application of AI Technologies in Cybersecurity

The application of AI in cybersecurity practices is varied and innovative, encompassing threat detection, response strategies, and predictive analytics. AI-driven threat intelligence platforms utilize big data analytics to sift through vast amounts of data to identify potential threats before they manifest, a practice that significantly enhances the proactive capabilities of cybersecurity teams (Alom et al., 2018). Additionally, theoretical frameworks in the study of AI's impact on cybersecurity focus on understanding the interaction between AI technologies and cyber threats. Models such as the Adaptive Security Architecture (ASA) framework offer insights into how AI can be integrated into cybersecurity strategies to enhance adaptability and resilience (Sinno et al., 2017). On the other hand, empirical studies provide quantitative and qualitative analyses of AI's effectiveness in specific cybersecurity applications. For instance, a study by Kim et al. (2016) utilized a machine learning model to detect zero-day vulnerabilities with a high degree of accuracy, showcasing the practical benefits of AI in cybersecurity. The creation of privacy-preserving deep learning (DL) under a distributed training system (Figure 1) was initially proposed by Shokri and Shmatikov (2015). This allows several parties to work together to create an accurate neural network model without disclosing their input datasets. However, the following section presents the role of Artificial Intelligence and Machine Learning in cyber threat detection and mitigation.

- Threat detection: Islam et al. (2023) assert that Artificial Intelligence and Machine Learning are exceptionally proficient at proactive threat detection. By learning from historical data, AI systems can recognize the hallmarks of cyber threats, from phishing attempts to advanced persistent threats (APTs), with high precision (Lee et al., 2019).
- Prediction: AI's predictive capabilities are a game-changer in cybersecurity. By analyzing past and current data, AI models can forecast future threat trends, allowing organizations to prepare and potentially prevent attacks before they happen. This proactive stance against cyber threats is a significant shift from the reactive approaches of the past (Amarasinghe et al., 2019).
- Response**:** AI enhances response strategies by quickly analyzing the scope of an attack and suggesting or even automating appropriate countermeasures (Zaman et al., 2021). This rapid response capability minimizes damage and reduces the time and resources required to recover from a security breach.

Despite these advancements, AI-driven cybersecurity tools are not without challenges. False positives remain an issue, and the complexity of AI systems can make them challenging to understand and manage.

- Ethical and Privacy Concerns: The use of AI in monitoring and analyzing data raises concerns about privacy and data protection. Ensuring that AI systems respect user privacy and comply with regulations like GDPR is paramount (Martin, 2019; Truong et al., 2019).
- Security Risks: AI systems themselves can become targets for cyberattacks. Attackers might manipulate AI algorithms through data poisoning or model evasion strategies, turning the strength of AI into vulnerability (Yaacoub et al., 2022).
- Complexity and Cost: Implementing and maintaining AI-driven security systems can be complex and costly, requiring significant investment in technology and expertise (Mateos-Garcia, 2018).
- False Positives and Negatives: AI systems are not foolproof and can generate false alarms or miss subtle threats, requiring ongoing tuning and human oversight (Capraro et al., 2023).
- Adversarial Attacks: AI systems are susceptible to sophisticated adversarial attacks potentially vulnerable if not properly secured and updated (Chakraborty et al., 2021).

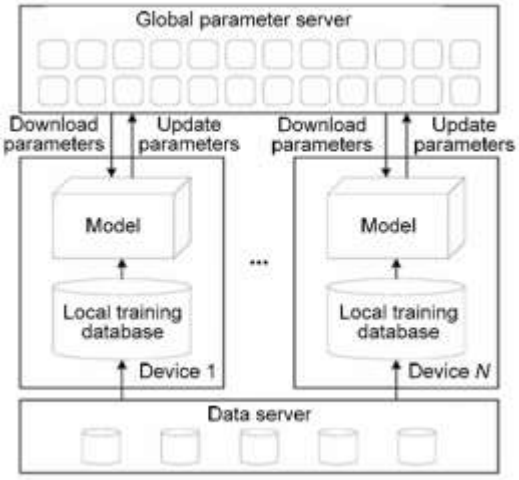

Figure 1: Safe distributed machine learning system (Shokri & Shmatikov, 2015)

As cyber threats evolve in complexity and volume, traditional security measures have struggled to keep pace. Artificial intelligence (AI) has emerged as a transformative tool in the battle against cyber threats, offering the potential to revolutionize how we protect digital assets. This research paper delves into the impact of AI on cybersecurity, presenting a series of case studies that highlight both the advancements and challenges in the field. Through these examples, we aim to understand the role of AI in enhancing security measures, its effectiveness in mitigating risks, and the lessons learned from its application in real-world scenarios.

Case 1 (AI in Phishing Detection and Response): AI has emerged as a powerful tool in cybersecurity, particularly in combating phishing attacks (Basit et al., 2021), where cybercriminals aim to deceive individuals into divulging sensitive information. A leading financial institution successfully implemented AI-driven solutions to detect phishing emails, leveraging machine learning algorithms trained on extensive datasets. These algorithms analyze various email attributes, such as content, sender information, and embedded links, to distinguish between legitimate communications and potential threats. As a result, the system achieved an impressive accuracy rate of over 98%, significantly reducing successful phishing attempts. Key takeaways include AI's capacity to discern subtle patterns from vast datasets, the importance of continuous model training to keep pace with evolving threats, and the considerable enhancement AI integration offers to email security protocols, bolstering organizational resilience against cyberattacks.

Case 2 (AI-Driven Threat Intelligence for Proactive Security): An international cybersecurity firm capitalized on AI technology to develop an advanced threat intelligence system proficient in preemptively identifying and mitigating cyber threats (Šrndić & Laskov, 2014). This AI-powered solution harnessed natural language processing (NLP) and machine learning to sift through extensive data from various outlets, such as the dark web, hacker forums, and social media, predicting potential cyberattacks before they materialize (Radford et al., 2018). Its real-time processing capability of unstructured data facilitated the detection of emerging threats, empowering the firm to alert clients promptly and propose preemptive measures, effectively thwarting numerous cyber incidents. Key takeaways include the indispensable role of AI in analyzing diverse data sources, the pivotal importance of proactive threat identification, and the necessity of collaborative data sharing among organizations and cybersecurity providers for robust threat intelligence systems.

Case 3(Automating Incident Response with AI): A global technology enterprise successfully implemented AI-driven automation in its cybersecurity operations, revolutionizing incident response. By employing advanced machine learning algorithms, the system swiftly detected, analyzed, and contained potential threats within network traffic and user behaviors (Ucci et al., 2019). Upon detection, automated measures were initiated to contain the threat, simultaneously alerting the cybersecurity team for further action. This proactive approach significantly mitigated damage, reducing data loss and system downtime. Key takeaways include finely tuning AI systems to minimize false positives and highlighting the necessity of human oversight to complement AI's capabilities in cybersecurity operations.

4. Methodology

4.1 Research Framework

This research paper employed a mixed-methods approach to investigate the impact of AI on cybersecurity, encompassing both qualitative and quantitative methodologies. By integrating various research designs, this comprehensive strategy facilitates a thorough examination of AI's role in bolstering cybersecurity measures, identifying potential risks and vulnerabilities, and

comprehending the broader ramifications of AI integration into cybersecurity practices. The research design comprised three primary components: a literature review, case study analysis, and developing and testing AI models for cybersecurity purposes. The literature review anchored the research in existing knowledge and theories, while the case studies provided practical insights into AI's application and effectiveness in real-world cybersecurity scenarios. Additionally, the development and testing of AI models furnish empirical data and firsthand experience, shedding light on AI's capabilities in detecting, preventing, and responding to cyber threats.

4.2 Data Collection

This research undertook a dual approach to data collection, drawing from both secondary and primary sources. Secondary data was acquired through an extensive review of academic journals, conference proceedings, and industry reports, focusing on studies examining the convergence of AI and cybersecurity. This review encompassed theoretical deliberations and empirical findings on AI's influence on cybersecurity practices. The search terms employed for the identification of secondary sources are detailed below.

> TITLE-ABS-KEY (cybersecurity*) AND (TITLE-ABS-KEY (artificial* AND intelligence*) OR TITLE-ABS-KEY (AI*) AND TITLE-ABS-KEY (machine* AND learning*) AND TITLE-ABS-KEY (deep* AND learning*) AND TITLE-ABS-KEY (network* AND security*)) AND PUBYEAR > 2012 AND PUBYEAR < 2024 AND (LIMIT-TO (DOCTYPE , "academic journals") AND (DOCTYPE , "conference paper") AND (DOCTYPE , "industrial report")) AND (LIMIT-TO (LANGUAGE , "English"))

Complementing this, primary data was gathered by deploying AI models engineered for distinct cybersecurity functions, including intrusion detection, malware analysis, and threat intelligence. These models were constructed utilizing cutting-edge machine learning algorithms, customized to tackle the challenges and demands inherent in cybersecurity contexts.

4.3 Analysis Method

The analysis deployed a comprehensive approach encompassing both qualitative and quantitative methodologies. Qualitative analysis entailed synthesizing insights garnered from the literature review and case studies, elucidating key themes, patterns, and implications about the influence of AI on cybersecurity (see Figure 2). Through meticulous coding and categorization of data, meaningful information was extracted regarding the advantages, challenges, and prospective trajectories of AI within this domain. Conversely, quantitative analysis concentrated on the empirical outcomes of implementing AI models in cybersecurity operations, as shown in Figure 3. This segment will entail statistical scrutiny to evaluate AI models' efficacy, accuracy, and efficiency in detecting and mitigating cyber threats. Critical metrics such as detection rate, false positive rate, and response time were leveraged to gauge AI applications' performance and efficacy in bolstering cybersecurity defenses.

4.4 Justification of Methodology

The complexity and multifaceted nature of understanding the impact of AI on cybersecurity necessitate adopting a mixed-methods approach, integrating qualitative and quantitative methodologies. This approach allowed for a comprehensive analysis that considers not only empirical data and performance metrics but also theoretical perspectives, ethical implications, and practical challenges. Moreover, developing and testing AI models within real-world cybersecurity scenarios were crucial for achieving the research objectives. By deploying these models and assessing their effectiveness, the research can provide valuable empirical evidence while also contributing to advancing more robust AI-driven cybersecurity solutions.

4.5 Implementation of AI Models

The advancement and deployment of AI models were adhered rigorously to best practices in both machine learning and cybersecurity domains. This entails meticulous selection and utilization of robust datasets for training and testing phases, alongside applying pertinent preprocessing and feature selection methodologies. To effectively address various tasks, sophisticated machine learning algorithms will be judiciously chosen and employed. Emphasis on ethical considerations, notably privacy and data protection, will be fundamental across all stages of research. Such a meticulous approach ensures that the development and utilization of AI models uphold elevated ethical standards while making constructive contributions to the cybersecurity landscape.

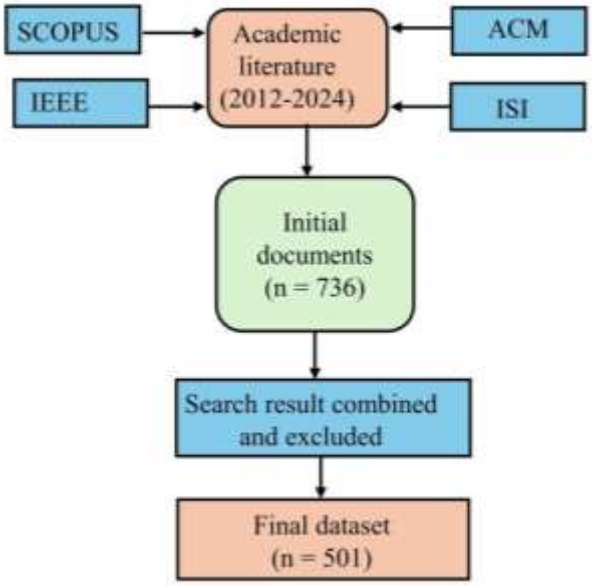

Figure 2: Qualitative method

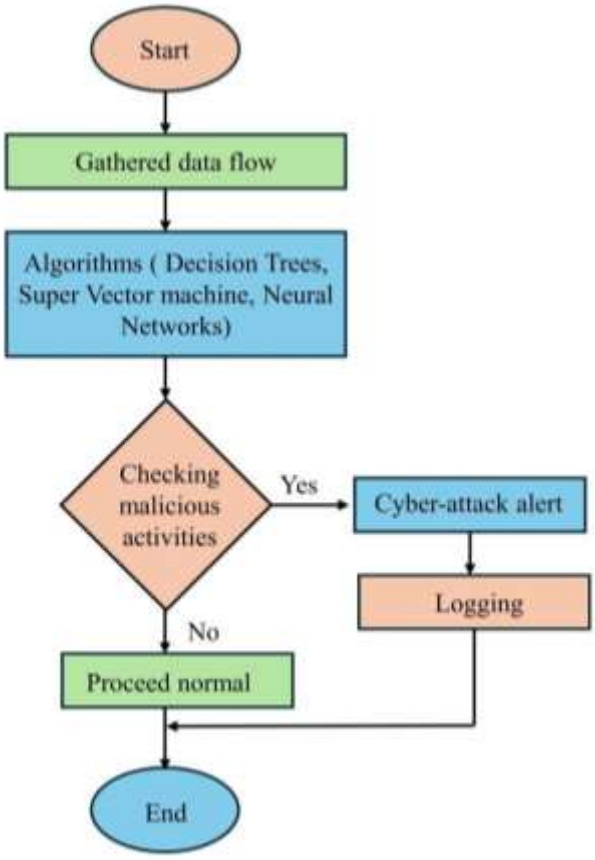

Figure 3: Work flow of proposed quantitative models

5. Results and Discussion

5.1 Qualitative Approach

Analysis of the intersection between Cybersecurity and AI applications, drawing from data sourced from academic journals, conference proceedings, and industry reports, offers valuable insights into research trends and dynamics within this domain.

Initially, 736 papers were considered, subsequently filtered to 369, comprising research articles, conference papers, editorial papers, and review papers. Table 1 illustrates the distribution of relevant documents focusing on AI's impact on cybersecurity. Furthermore, Figure 4 depicts publication trends from 2012 to 2024, revealing exponential growth, notably surging post-2015. The steady rise from 2012 to 2015 likely reflects an increasing recognition of the significance of both cybersecurity and AI. The substantial uptick in publications between 2017 and 2024 is noteworthy, indicating burgeoning interest in their convergence. This growth is propelled by escalating cyber threats, attributed to increased incident frequency, rapid integration of AI into cybersecurity systems, and the demand for sophisticated AI-driven solutions to combat complex threats.

Table 1. Relevant documents on AI and cyber security

Keywords	Frequency
Machine learning	129
Deep learning	67
Cybersecurity	61
Artificial intelligence	59
Network security	53

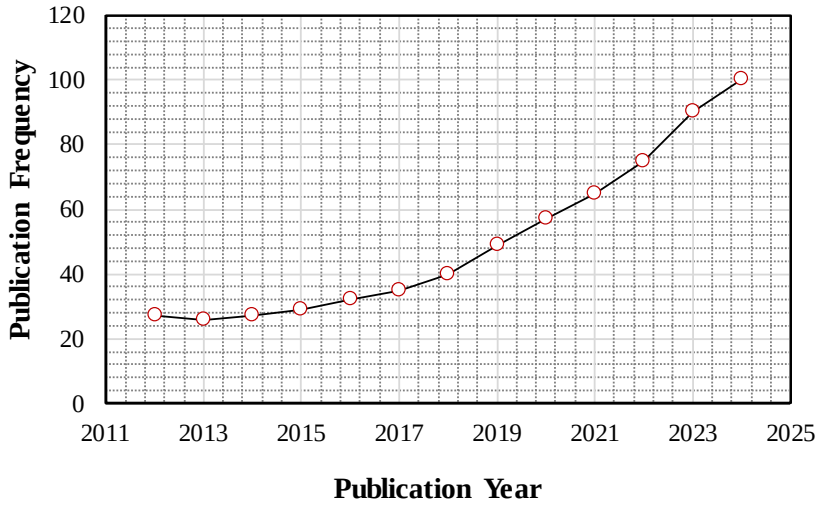

Figure 4: Publication trend

5.2 Quantitative Analysis

The models and their respective performances are shown in Table 2, and the performance model's evaluation is shown in Figure 5. Among the provided models, Neural Networks demonstrate the highest performance across all metrics, boasting an accuracy of 98%, precision of 99%, recall of 97%, and a false positive rate of 1%. In comparison, Support Vector Machines (SVM) follow closely behind with an accuracy of 97%, precision of 97%, recall of 96%, and a slightly higher false positive rate of 1.5%. Meanwhile, Decision Trees exhibit slightly lower performance metrics, with an accuracy of 95%, precision of 96%, recall of 94%, and a false positive rate of 2%. In comparing the performance metrics of Decision Trees, Support Vector Machines (SVM), and Neural Networks, it becomes evident that each model presents distinct advantages and trade-offs. While Neural Networks exhibit superior accuracy, precision, recall, and false favorable rates, Decision Trees and SVMs also offer competitive performance in various scenarios. Decision Trees, known for their simplicity and interpretability, offer a balance between accuracy and model complexity, making them particularly suitable for tasks where transparency is critical.

On the other hand, SVMs excel in handling high-dimensional data and can effectively capture complex relationships between features, often achieving high accuracy with fewer computational resources. Despite their differences, the choice of model ultimately depends on the specific requirements of the problem domain, including considerations such as interpretability, computational efficiency, and scalability. Therefore, while Neural Networks may outperform Decision Trees and SVMs in this dataset, a comprehensive understanding of each model's strengths and limitations is essential for selecting the most appropriate algorithm for a given task.

Table 2. Performance Metrics of AI Algorithms in Intrusion Detection

Algorithm	Accuracy	Precision	Recall	False Positive Rate
Decision Trees	95%	96%	94%	2%
Support Vector Machines (SVM)	97%	97%	96%	1.5%
Neural Networks	98%	99%	97%	1%

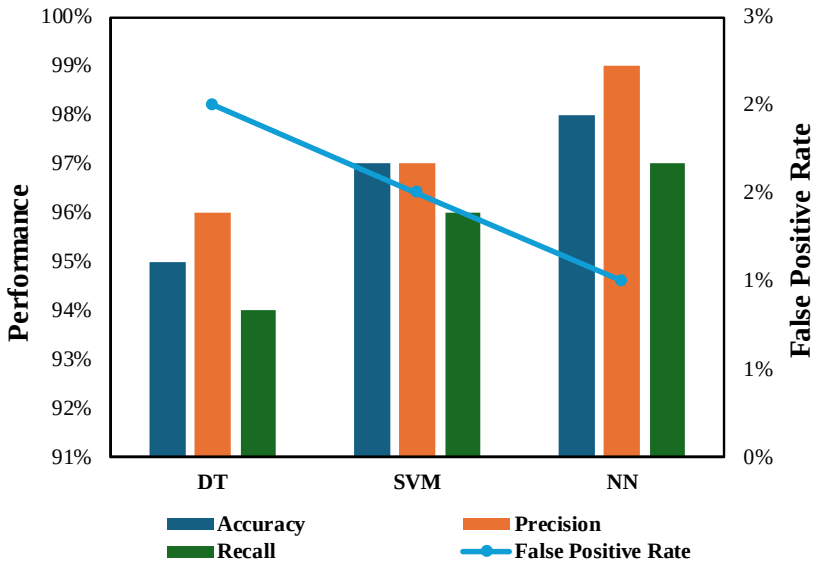

Figure 5: evaluation of the models' performance

6. Conclusion

This study delves into the profound influence of artificial intelligence (AI) on cybersecurity, exploring its dual nature as both a powerful ally in bolstering security measures and a potential menace in the hands of adversaries. The convergence of AI and cybersecurity has ushered in a new era of digital defense mechanisms, facilitating more effective threat detection, response, and prevention strategies. However, a number of important conclusions about how AI affects cybersecurity may be highlighted from the above-given results:

- The high performance rate of AI models demonstrates the rapid and accurate identification of threats and anomalies. This capability significantly reduces the window of opportunity for cyber attackers, thereby enhancing organizations' overall security posture.
- AI-driven automation of routine security tasks has been shown to boost efficiency and free up human resources to focus on more complex security challenges. This shift towards automation holds the potential to revolutionize cybersecurity practices by optimizing resource allocation and operational effectiveness.
- The flip side of AI's integration into cybersecurity is the advent of AI-powered cyber threats. Cybercriminals increasingly leverage AI to develop more sophisticated attack vectors, such as adaptive malware and automated phishing campaigns, which can learn and evolve to bypass conventional security defenses.
- The deployment of AI in cybersecurity raises significant ethical and privacy concerns, particularly regarding data collection, storage, and analysis. Ensuring the ethical use of AI in cybersecurity practices is paramount to maintaining public trust and compliance with regulatory standards.

6.1 Limitation of the study.

Implementing and maintaining AI-driven security systems indeed poses challenges, primarily in complexity and cost. This endeavor demands substantial investment, both in cutting-edge technology and specialized expertise. The intricacies of integrating AI into security infrastructure entail meticulous planning, robust implementation, and continuous refinement.

Despite their advanced capabilities, AI systems are not impervious to errors. False positives and negatives remain a persistent concern. These systems may inadvertently trigger alarms for benign activities or overlook nuanced threats, necessitating ongoing calibration and human supervision. Striking the delicate balance between sensitivity and accuracy demands vigilance and adaptability.

Moreover, the specter of adversarial attacks looms over AI-powered security measures. Sophisticated adversaries can exploit vulnerabilities in AI algorithms, manipulating inputs to deceive the system and evade detection. To mitigate this risk, stringent security protocols must be enforced, encompassing regular updates, rigorous testing, and preemptive defenses against emerging threats.

In essence, while AI offers unprecedented potential in fortifying security frameworks, its implementation demands a comprehensive approach that addresses complexity, false positives and negatives, and the looming threat of adversarial attacks. Only through diligent investment, vigilant oversight, and proactive security measures can organizations harness the full benefits of AI-driven security while safeguarding against inherent risks.

6.2 Future recommendation

To effectively harness the benefits of AI in cybersecurity while mitigating its associated risks, we propose the following practical recommendations:

- Invest in AI Literacy: Organizations should invest in training and development programs to enhance the AI literacy of their cybersecurity teams. Understanding AI's capabilities, limitations, and ethical considerations is crucial for its effective integration into security practices.
- Develop AI-driven Security Frameworks: Adopting AI-driven security frameworks that dynamically adapt to emerging threats is essential. Such frameworks should incorporate advanced machine learning algorithms for real-time threat detection, analysis, and response.
- Establish Ethical Guidelines: It is imperative to establish clear ethical guidelines governing the use of AI in cybersecurity. These guidelines should address privacy, data protection, and the ethical use of AI technologies.
- Foster Collaboration: Collaboration between organizations, governments, and academic institutions is critical to advancing the development and deployment of AI in cybersecurity. Sharing knowledge, resources, and best practices can enhance collective defense mechanisms against cyber threats.
- Prepare for AI-powered Threats: Cybersecurity strategies must evolve to counter AI-powered threats. This involves developing countermeasures against AI-based attack vectors and continuously monitoring for signs of such threats.

Funding: This study received no specific funding from public, commercial, or not-for profit funding agencies.
Conflicts of Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Alom, M. Z., Taha, T. M., Yakopcic, C., Westberg, S., Sidike, P., Nasrin, M. S., Van Esesn, B. C., Awwal, A. A. S., & Asari, V. K. (2018). The history began from alexnet: A comprehensive survey on deep learning approaches. *arXiv preprint arXiv:1803.01164*. https://doi.org/https://doi.org/10.48550/arXiv.1803.01164

[2] Amarasinghe, A., Wijesinghe, W., Nirmana, D., Jayakody, A., & Priyankara, A. (2019). AI based cyber threats and vulnerability detection, prevention and prediction system. 2019 international conference on advancements in computing (ICAC),

[3] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*, 139-154. https://doi.org/https://doi.org/10.1007/s11235-020-00733-2

[4] Borode, A., & Olubambi, P. (2024). Optimisation of artificial intelligence models and response surface methodology for predicting viscosity and relative viscosity of GNP-alumina hybrid nanofluid: incorporating the effects of mixing ratio and temperature. *The Journal of Supercomputing*, *80*(4), 4841-4869. https://doi.org/https://doi.org/10.1007/s11227-023-05652-y

[5] Capraro, V., Lentsch, A., Acemoglu, D., Akgun, S., Akhmedova, A., Bilancini, E., Bonnefon, J.-F., Brañas-Garza, P., Butera, L., & Douglas, K. M. (2023). The impact of generative artificial intelligence on socioeconomic inequalities and policy making. *arXiv preprint arXiv:2401.05377*. https://doi.org/https://doi.org/10.48550/arXiv.2401.05377

[6] Chakraborty, A., Alam, M., Dey, V., Chattopadhyay, A., & Mukhopadhyay, D. (2021). A survey on adversarial attacks and defences. *CAAI Transactions on Intelligence Technology*, *6*(1), 25-45. https://doi.org/ https://doi.org/10.1049/cit2.12028

[7] Couretas, J. M. (2022). Cyber Analysis and Targeting. In *An Introduction to Cyber Analysis and Targeting* (1-12). Springer. https://doi.org/https://doi.org/10.1007/978-3-030-88559-5_1

[8] Dayyabu, Y. Y., Arumugam, D., & Balasingam, S. (2023). The application of artificial intelligence techniques in credit card fraud detection: a quantitative study. E3S Web of Conferences,

[9] Islam, M. Z., Chowdhury, M. M. H., & Sarker, M. M. (2023). The Impact of Big Data Analytics on Stock Price Prediction in the Bangladesh Stock Market: A Machine Learning Approach. *International Journal of Science and Business*, *28*(1), 219-228.

[10] Iyamu, I., Xu, A. X., Gómez-Ramírez, O., Ablona, A., Chang, H.-J., Mckee, G., & Gilbert, M. (2021). Defining digital public health and the role of digitization, digitalization, and digital transformation: scoping review. *JMIR public health and surveillance*, *7*(11), e30399. https://doi.org/10.2196/30399

[11] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/https://doi.org/10.1016/j.inffus.2023.101804

[12] Kim, J., Kim, J., Thu, H. L. T., & Kim, H. (2016). Long short term memory recurrent neural network classifier for intrusion detection. 2016 international conference on platform technology and service (PlatCon),

[13] Lacka, E., & Wong, T. C. (2021). Examining the impact of digital technologies on students' higher education outcomes: the case of the virtual learning environment and social media. *Studies in Higher Education*, *46*(8), 1621-1634. https://doi.org/https://doi.org/10.1080/03075079.2019.1698533

[14] Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles. *Ieee Access*, *7*, 165607-165626.

[15] Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, *13*(12), 1550147717741463. https://doi.org/https://doi.org/10.1177/1550147717741774

[16] Marres, N. (2012). On some uses and abuses of topology in the social analysis of technology (or the problem with smart meters). *Theory, Culture & Society*, *29*(4-5), 288-310. https://doi.org/https://doi.org/10.1177/0263276412454460

[17] Martin, K. (2019). Ethical implications and accountability of algorithms. *Journal of business ethics*, *160*(4), 835-850. https://doi.org/https://doi.org/10.1007/s10551-018-3921-3

[18] Mateos-Garcia, J. C. (2018). The complex economics of artificial intelligence. *Available at SSRN 3294552*. https://doi.org/http://dx.doi.org/10.2139/ssrn.3294552

[19] Mhlanga, D. (2021). Financial inclusion in emerging economies: The application of machine learning and artificial intelligence in credit risk assessment. *International journal of financial studies*, *9*(3), 39. https://doi.org/10.3390/ijfs9030039

[20] Radford, A., Narasimhan, K., Salimans, T., & Sutskever, I. (2018). Improving language understanding by generative pre-training.

[21] Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence*, *76*, 130-157. https://doi.org/https://doi.org/10.1016/j.engappai.2018.07.008

[22] Shokri, R., & Shmatikov, V. (2015). Privacy-preserving deep learning. Proceedings of the 22nd ACM SIGSAC conference on computer and communications security,

[23] Singh, A., & Gupta, B. B. (2022). Distributed denial-of-service (DDoS) attacks and defense mechanisms in various web-enabled computing platforms: issues, challenges, and future research directions. *International Journal on Semantic Web and Information Systems (IJSWIS)*, *18*(1), 1-43. https://doi.org/10.4018/IJSWIS.297143

[24] Sinno, S., Negri, F., & Goldhammer, S. (2017). Designing an adaptive security architecture with unisys stealth and logrhythm. *White Paper, Unisys Corporation, USA*.

[25] Šrndić, N., & Laskov, P. (2014). Practical evasion of a learning-based classifier: A case study. 2014 IEEE symposium on security and privacy,

[26] Truong, N. B., Sun, K., Lee, G. M., & Guo, Y. (2019). Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security*, *15*, 1746-1761.

[27] Ucci, D., Aniello, L., & Baldoni, R. (2019). Survey of machine learning techniques for malware analysis. *Computers & Security*, *81*, 123-147. https://doi.org/https://doi.org/10.1016/j.cose.2018.11.001

[28] Urbinati, A., Chiaroni, D., Chiesa, V., & Frattini, F. (2020). The role of digital technologies in open innovation processes: an exploratory multiple case study analysis. *R&d Management*, *50*(1), 136-160. https://doi.org/https://doi.org/10.1111/radm.12313

[29] Yaacoub, J.P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, *21*(1), 115-158. https://doi.org/https://doi.org/10.1007/s10207-021-00545-8

[30] Zaman, S., Alhazmi, K., Aseeri, M. A., Ahmed, M. R., Khan, R. T., Kaiser, M. S., & Mahmud, M. (2021). Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. *Ieee Access*, *9*, 94668-94690. https://doi.org/10.1109/ACCESS.2021.3089681

[31] Zou, C. C., Gong, W., & Towsley, D. (2002). Code red worm propagation modeling and analysis. Proceedings of the 9th ACM conference on Computer and communications security,