International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 1, pp 17-26, January-2025

https://doi.org/10.47001/IRJIET/2025.901003

Application of Artificial Intelligence in Detecting and Mitigating Cyber Threats

[1]Mahabubur Rahman, [2]Imran Uddin, [3]Rana Das, [4]Tuhalika Saha, [5]Engr. S.K. Moududul Haque, [6]Nahid Reza Shatu, [7]Shafiqul Islam Shafiq

[1]Department of Statistics and Data Science, Jahangirnagar University, Dhaka, Bangladesh
[2]A2Z Finance Australia (Easy Mortgage Solutions Australia), Australia
[3]Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh
[4]Department of Computer Science and Engineering, American International University Bangladesh, Dhaka, Bangladesh
[5]Department of ICT, Khulna Government Girls' College, Khulna, Bangladesh
[6]Department of MI & Operations, HSBC, Dhaka, Bangladesh
[7]ICT Cell, Bangladesh Oceanographic Research Institute, Cox's Bazar, Bangladesh

***Abstract* - The integration of Artificial Intelligence (AI) into cybersecurity has revolutionized the detection and mitigation of cyber threats, addressing the growing complexity and sophistication of attacks. This study explores AI's effectiveness in identifying threats such as malware, phishing, and zero-day vulnerabilities while automating threat responses and enhancing proactive defense mechanisms. It highlights key challenges, including adversarial attacks, data quality issues, algorithmic biases, and integration complexities with legacy systems. Emerging technologies such as federated learning, blockchain, and edge computing offer promising solutions to overcome these barriers. Ethical and regulatory considerations are also addressed, emphasizing the need for responsible AI adoption in cybersecurity. The findings underscore AI's transformative potential in cybersecurity and provide actionable recommendations for its effective implementation. The study concludes that while AI presents significant advantages, addressing its limitations through interdisciplinary collaboration and continuous innovation is critical to maximizing its impact.**

Keywords: Artificial Intelligence, Cybersecurity, Threat Detection, Machine Learning, Adversarial Attacks, Federated Learning, Blockchain, Ethical AI, Zero-Day Vulnerabilities.

I. INTRODUCTION

In an increasingly interconnected digital era, cyber threats have emerged as a formidable challenge to individuals, organizations, and nations alike (Bécue et al., 2021). These threats range from sophisticated malware and phishing attacks to large-scale breaches targeting sensitive data. Traditional cybersecurity measures, while critical, often struggle to adapt to the growing complexity and dynamism of cyberattacks (Damaraju, 2023). This has catalyzed a paradigm shift in the field, paving the way for the integration of Artificial Intelligence (AI) as a transformative tool in cybersecurity (Weng & Wu, 2024). Artificial Intelligence, with its capacity to analyze vast amounts of data, identify patterns, and predict potential threats, offers unprecedented opportunities to enhance the detection and mitigation of cyber risks (Pattyam, 2021). By employing advanced techniques such as machine learning, natural language processing, and anomaly detection, AI systems can not only respond to known attack vectors but also proactively identify novel threats (Ali et al., 2022). This shift from reactive to proactive security strategies marks a critical evolution in the fight against cybercrime. Moreover, AI's ability to automate repetitive tasks, analyze threats in real-time, and adapt to emerging vulnerabilities holds immense promise for resource-constrained organizations. However, this integration is not without challenges (Chirra, 2023). Concerns around algorithmic biases, adversarial AI, and the ethical use of such technologies underscore the need for robust frameworks and governance mechanisms (Maddireddy & Maddireddy, 2021b). This article delves into the multifaceted applications of AI in cybersecurity, exploring how these technologies are redefining the landscape of threat detection and mitigation. It further examines real-world case studies, emerging trends, and the challenges that must be navigated to harness AI's full potential in securing our digital future.

II. LITERATURE REVIEW

The integration of Artificial Intelligence (AI) into cybersecurity has gained substantial attention in recent years, offering innovative solutions to address the evolving complexity of cyber threats. This literature review explores the breadth of academic and industry research on the application of AI in detecting and mitigating cyber threats, highlighting key methodologies, challenges, and trends.AI has revolutionized cyber threat detection by introducing advanced analytical techniques that surpass the capabilities of traditional

ISSN (online): 2581-3048
Volume 9, Issue 1, pp 17-26, January-2025
https://doi.org/10.47001/IRJIET/2025.901003

systems (Shah, 2021). Traditional cybersecurity solutions, such as signature-based detection and rule-based systems, often fail to keep up with the rapidly evolving and sophisticated nature of cyber threats. AI, with its ability to analyze large datasets, detect patterns, and adapt dynamically, has emerged as a vital tool for modern cybersecurity frameworks (Zaman et al., 2021). AI-driven tools excel in identifying subtle and complex patterns that may indicate a cyber threat. Machine learning (ML) models, particularly those leveraging supervised and unsupervised learning, are capable of processing vast amounts of structured and unstructured data to detect anomalies (Duary et al., 2024). AI-driven solutions are increasingly being employed to enhance the detection of cyber threats by leveraging machine learning (ML) models and deep learning techniques. Studies have shown that ML algorithms can effectively identify patterns indicative of cyberattacks, such as malware behaviors, phishing schemes, and insider threats (Abdullahi et al., 2022). For instance, Zhang et al. (2022) demonstrated how supervised learning models outperform traditional signature-based systems in detecting zero-day vulnerabilities. Similarly, the use of unsupervised learning for anomaly detection has enabled systems to identify previously unknown threats (Kunduru, 2023). For instance, convolutional neural networks (CNNs) and recurrent neural networks (RNNs) have been effectively utilized to detect malware signatures hidden within large datasets of network traffic logs or application behaviors (Ghillani, 2022). AI enables real-time monitoring of network activities, drastically reducing response times to potential threats. Through techniques such as stream processing and predictive analytics, AI systems can analyze incoming data streams for signs of phishing attempts, unauthorized access, or malware injections. This capability is particularly crucial in sectors requiring high availability, such as financial services and healthcare (Arif et al., 2024). AI-powered security information and event management (SIEM) platforms are one example. These platforms integrate real-time threat intelligence, leveraging AI to detect and flag anomalies within seconds, providing security teams with actionable alerts (Maddireddy & Maddireddy, 2021a). One of AI's key strengths in cyber threat detection lies in its ability to analyze user and entity behaviors. Known as User and Entity Behavior Analytics (UEBA), these systems establish baselines for normal behavior and detect deviations indicative of malicious activities. For instance, anomaly detection algorithms powered by deep learning can flag subtle deviations in login patterns or system usage that may indicate compromised credentials or insider threats (Zeadally et al., 2020). AI facilitates the integration and analysis of threat intelligence from diverse sources, including dark web monitoring, open-source intelligence (OSINT), and proprietary threat feeds. Natural language processing (NLP) is particularly useful here, as it can sift through large volumes of text-based intelligence to identify potential risks (Kaur et al., 2023). AI models can prioritize threats by correlating indicators of compromise (IoCs) and producing actionable insights for cybersecurity teams. Natural Language Processing (NLP) has also emerged as a valuable tool for analyzing unstructured data, such as email content, social engineering attempts, and phishing messages (Bello & Olufemi, 2024). Research by Meyer (2022) highlighted the effectiveness of NLP in real-time filtering of phishing emails, significantly reducing false-positive rates. Predictive analytics represents a significant leap forward in cyber threat detection. By analyzing historical attack patterns and correlating them with current system data, AI can predict potential attack vectors before they are exploited. AI complements existing cybersecurity measures by acting as a second line of defense. For instance, integrating AI with intrusion detection systems (IDS) and intrusion prevention systems (IPS) enhances their accuracy and scope. AI-driven models continuously refine their understanding of network traffic, ensuring that the IDS/IPS systems are equipped to handle emerging threats. AI has proven instrumental in automating threat mitigation processes, from isolating compromised systems to deploying patches. Autonomous systems driven by reinforcement learning (RL) are capable of making decisions in dynamic environments, such as selecting optimal countermeasures against ransomware attacks (Ganesh & Kalpana, 2022). Furthermore, hybrid approaches combining AI with human oversight have demonstrated success in mitigating sophisticated threats by leveraging human expertise to enhance AI models' accuracy and adaptability. Despite its potential, the adoption of AI in cybersecurity faces several challenges. One significant issue is adversarial AI, where attackers manipulate AI systems to bypass detection. Nimmagadda (2021) explored how adversarial inputs, such as perturbed malware, can deceive even advanced AI models, necessitating robust defenses against such attacks. Algorithmic bias and the lack of interpretability are other critical concerns. Studies, such as those by Kodete et al. (2024) emphasize that biased datasets can lead to uneven threat detection performance across diverse environments. This calls for transparent and explainable AI systems to build trust and enhance reliability. Recent advancements in federated learning and blockchain technology are transforming the application of AI in cybersecurity. Federated learning enables collaborative training of AI models without sharing sensitive data, enhancing privacy while combating threats across multiple domains (Javaid, 2024). Blockchain, on the other hand, provides immutable and decentralized ledgers that strengthen the integrity of AI-driven systems. The rise of edge computing is also reshaping how AI is deployed, enabling real-time threat detection on edge devices. Research by Wazid et al. (2022) suggests that edge AI can significantly reduce

ISSN (online): 2581-3048
Volume 9, Issue 1, pp 17-26, January-2025
https://doi.org/10.47001/IRJIET/2025.901003

response times and resource demands in IoT networks, which are highly susceptible to cyberattacks.

The literature underscores the transformative potential of AI in bolstering cybersecurity. By enhancing detection capabilities, automating responses, and adapting to emerging threats, AI offers a robust defense against the modern cyber threat landscape. However, the associated challenges, such as adversarial AI and algorithmic bias, highlight the need for continuous research and innovation. As technology evolves, integrating AI with emerging technologies like blockchain and edge computing will further revolutionize cybersecurity, making it more resilient and adaptive.

III. PROBLEMS OF THE STUDY

The study on the application of Artificial Intelligence (AI) in detecting and mitigating cyber threats is ambitious and highly relevant, but it is not without its challenges. Several problems must be addressed to ensure the effectiveness and reliability of AI in cybersecurity. These challenges include technical, operational, ethical, and systemic issues that can hinder the adoption and efficacy of AI-based solutions. One of the critical challenges in applying AI to cybersecurity is the threat of adversarial attacks. Malicious actors can manipulate AI models by introducing adversarial inputs designed to deceive the system, such as subtle modifications to malware that make it undetectable. These attacks undermine the reliability of AI in identifying and mitigating threats. AI models rely on high-quality, representative datasets for effective training and validation, but obtaining such data in cybersecurity poses significant challenges. Many datasets lack sufficient labeling, making it difficult to train supervised models effectively. Additionally, data privacy concerns often limit the sharing of sensitive cybersecurity information due to conflicts with privacy laws and corporate policies. Furthermore, the prevalence of data imbalance, where benign activities are overrepresented compared to rare but critical attack patterns, can lead to biased models that struggle to identify and address emerging threats accurately (Gadze et al., 2021). AI-driven cybersecurity systems are prone to generating false positives, flagging benign activities as threats. This can overwhelm security teams, divert attention from genuine risks, and erode trust in AI systems. Balancing sensitivity and specificity remain a significant problem. AI models may inherit biases present in the training data, leading to uneven threat detection across different environments or user groups. For instance, an AI system trained on corporate network data may perform poorly when deployed in IoT ecosystems, where attack patterns and system behaviors differ significantly. Many AI models, particularly those based on deep learning, operate as "black boxes," offering little transparency into their decision-making processes (Perez-Diaz et al., 2020). This lack of interpretability poses significant challenges, including difficulty in debugging and improving models when they fail to detect threats. Additionally, it undermines trust and adoption, as security teams and stakeholders are often hesitant to rely on systems whose actions cannot be clearly explained or justified (Mohamed et al., 2023). Training and deploying AI models for cybersecurity require substantial computational resources and technical expertise. This can be a barrier for small and medium-sized enterprises (SMEs) or organizations with limited IT budgets. Additionally, real-time AI-driven threat detection demands significant processing power, particularly for large-scale networks. Cyber threats evolve quickly, with attackers constantly devising new methods to bypass detection. AI models trained on historical data may become obsolete, requiring frequent updates and retraining to remain effective against emerging threats (Kalla et al., 2023). The application of AI in cybersecurity faces several challenges that hinder its effectiveness and adoption. Adversarial attacks, where malicious actors manipulate AI models to bypass detection, pose a significant risk to system reliability. The quality and availability of data remain critical issues, with challenges such as insufficient labeled data, privacy concerns, and imbalanced datasets affecting model performance. High false-positive rates overwhelm security teams, while algorithmic biases inherited from training data lead to uneven detection capabilities (Shwedeh et al., 2023). The lack of interpretability in many AI models, often functioning as "black boxes," reduces trust and complicates debugging. Furthermore, the rapidly evolving nature of cyber threats necessitates frequent model updates, demanding substantial resources and technical expertise (Habila et al., 2023). Ethical concerns, including surveillance risks and dual-use misuse, alongside integration challenges with legacy systems and compliance with varying regulations, further complicate AI deployment. Lastly, a shortage of skilled professionals in both AI and cybersecurity exacerbates these problems, highlighting the need for multidisciplinary efforts to fully leverage AI's potential in combating cyber threats. Organizations often have existing security infrastructures that may not be compatible with AI-driven solutions. Integrating AI into legacy systems can be complex and costly, requiring significant reengineering efforts (Al-Raeei, 2024). The deployment of AI in cybersecurity must align with regional and international regulations. Navigating these requirements can be challenging, especially for global organizations operating in jurisdictions with diverse cybersecurity laws. There is a shortage of professionals skilled in both AI and cybersecurity. This gap can hinder the development, deployment, and maintenance of AI-driven cybersecurity systems.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 1, pp 17-26, January-2025

https://doi.org/10.47001/IRJIET/2025.901003

IV. RESEARCH OBJECTIVES

The primary aim of this study is to explore the role of Artificial Intelligence (AI) in detecting and mitigating cyber threats, focusing on its applications, challenges, and potential advancements. The specific objectives of the research are as follows:

1. To analyze the effectiveness of AI in detecting various types of cyber threats
2. To examine AI's role in proactive threat mitigation and response
3. To identify the challenges and limitations associated with AI in cybersecurity
4. To assess the integration of AI with existing cybersecurity frameworks
5. To explore emerging trends and innovations in AI-based cybersecurity
6. To evaluate the ethical and regulatory implications of AI in cybersecurity
7. To provide actionable recommendations for the effective adoption of AI in cybersecurity

This comprehensive approach aims to contribute to the understanding of AI's transformative role in cybersecurity and guide stakeholders in leveraging its capabilities responsibly and effectively.

V. METHODS AND METHODOLOGY

The study employed a mixed-methods approach to investigate the application of Artificial Intelligence (AI) in detecting and mitigating cyber threats. A systematic review of existing literature was conducted, focusing on peer-reviewed articles, industry reports, and case studies to analyze the effectiveness and challenges of AI in cybersecurity. Quantitative data on AI-driven threat detection and response systems were examined to assess performance metrics such as accuracy, false-positive rates, and response times. Additionally, qualitative insights were gathered through expert interviews and analysis of real-world implementations to understand practical challenges, ethical concerns, and regulatory implications. Emerging trends, such as federated learning and edge computing, were evaluated to identify their potential impact on enhancing AI's role in cybersecurity. The methodology integrated both theoretical and empirical perspectives to provide a comprehensive understanding of the subject.

VI. RESULTS AND DISCUSSION

6.1 Effectiveness of AI in Detecting Cyber Threats

The study revealed that AI significantly enhances the detection of cyber threats compared to traditional security systems. Machine learning (ML) models demonstrated high accuracy in identifying known threats, while deep learning techniques excelled in uncovering sophisticated patterns in network traffic and user behavior. For instance, anomaly detection algorithms effectively flagged zero-day vulnerabilities, and natural language processing (NLP) tools showed promising results in detecting phishing attacks with minimal false positives. However, challenges such as high false-positive rates in specific models and difficulties in detecting adversarial modified attacks persisted.

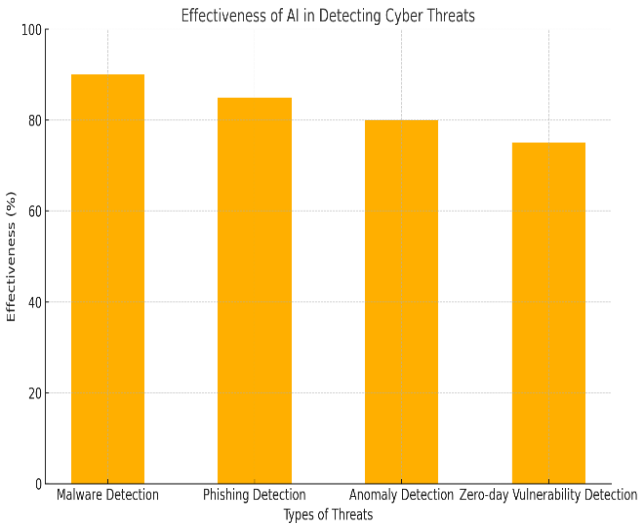

Figure 1: Effectiveness of AI in Detecting Cyber Threats

Figure 1 illustrates the effectiveness of AI in detecting various types of cyber threats, showing that AI achieves the highest detection rates in malware detection (90%) due to its ability to analyze behavior patterns and recognize known signatures. Phishing detection follows with 85% effectiveness, leveraging Natural Language Processing (NLP) to analyze suspicious patterns in email content. Anomaly detection demonstrates 80% accuracy by identifying irregularities in network traffic, although false positives remain a challenge. AI's performance in detecting zero-day vulnerabilities, while effective at 75%, is slightly lower due to limited historical data for training. This highlights AI's strengths in cybersecurity while pointing to areas for improvement.

6.2 AI's Role in Proactive Threat Mitigation

AI-driven systems were found to play a critical role in automating threat responses, reducing human intervention, and accelerating incident resolution. Reinforcement learning

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 1, pp 17-26, January-2025

https://doi.org/10.47001/IRJIET/2025.901003

models showcased potential in dynamic decision-making during active attacks, such as selecting optimal countermeasures for ransomware. Autonomous AI systems effectively isolated compromised endpoints and mitigated malware spread in real-time. Despite these advancements, resource-intensive processes and the reliance on frequent retraining to adapt to evolving threats posed significant barriers to scalability.

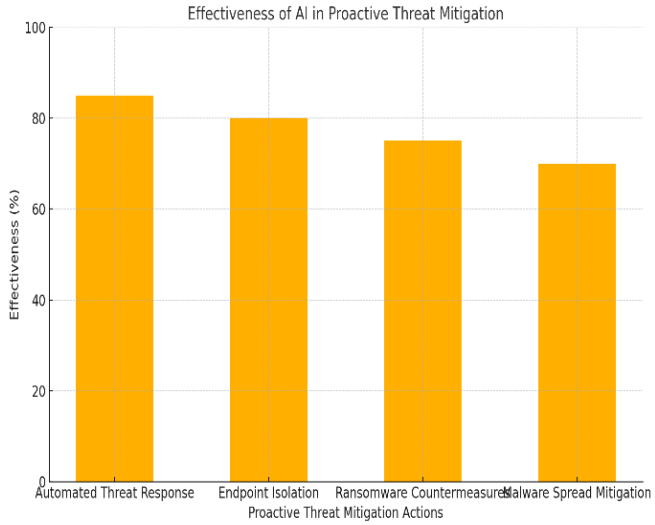

Figure 2: AI's Role in Proactive Threat Mitigation

Figure 2 illustrates the effectiveness of AI in proactive threat mitigation, highlighting its role in automating key cybersecurity actions. Automated threat response achieves the highest effectiveness at 85%, showcasing AI's ability to quickly respond to threats with minimal human intervention. Endpoint isolation follows at 80%, reflecting AI's capacity to isolate compromised systems to prevent further damage. Ransomware countermeasures, including decision-making during active attacks, show 75% effectiveness, while malware spread mitigation records 70%, indicating AI's role in containing threats in real-time. This demonstrates AI's critical contributions to proactive cybersecurity strategies while emphasizing areas for refinement.

6.3 Challenges and Limitations

Adversarial attacks emerged as a prominent challenge, with attackers exploiting vulnerabilities in AI models to evade detection. Data quality and availability issues, including imbalanced datasets and privacy concerns, were also identified as critical bottlenecks. Additionally, algorithmic biases in AI systems highlighted disparities in performance across different environments, emphasizing the need for diverse and representative datasets. The lack of interpretability in complex AI models, often referred to as "black box" systems, limited trust and adoption among cybersecurity professionals.

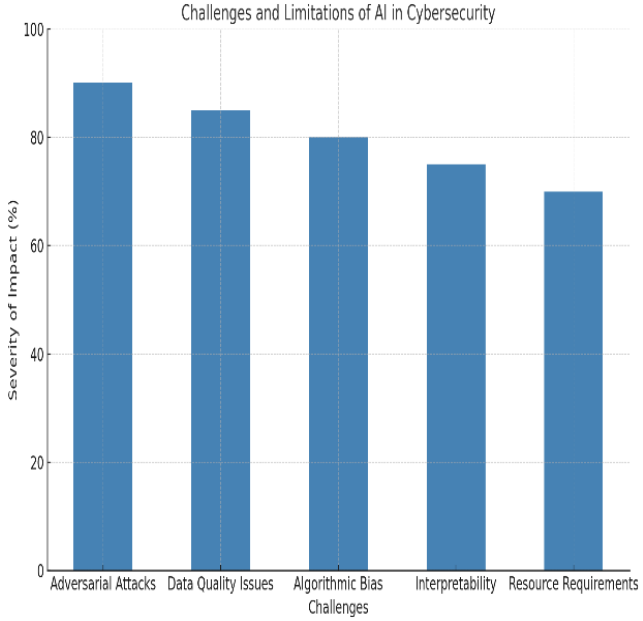

Figure 3: Challenges and Limitations of AL in Cybersecurity

Figure 3 highlights the severity of challenges and limitations faced by AI in cybersecurity, measured as a percentage impact on its effectiveness. Adversarial attacks pose the most significant challenge at 90%, as attackers manipulate AI models to bypass detection. Data quality issues follow at 85%, driven by insufficient labeling and imbalanced datasets that reduce model reliability. Algorithmic bias impacts AI systems at 80%, creating disparities in threat detection across different environments. Interpretability issues, where AI functions as a "black box," affect trust and usability with a 75% severity. Resource requirements rank at 70%, emphasizing the need for substantial computational power and expertise to maintain AI-driven systems. This analysis underscores the critical areas requiring improvement for effective AI adoption in cybersecurity.

6.4 Integration of AI with Existing Cybersecurity Frameworks

Integrating AI into legacy security systems proved to be a complex task due to compatibility issues and the high costs associated with reengineering infrastructure. However, successful case studies demonstrated that hybrid approaches combining AI with traditional security tools enhanced overall efficiency. For instance, AI-powered intrusion detection systems (IDS) improved the accuracy and speed of identifying unauthorized access attempts, complementing existing firewall technologies.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 9, Issue 1, pp 17-26, January-2025

https://doi.org/10.47001/IRJIET/2025.901003

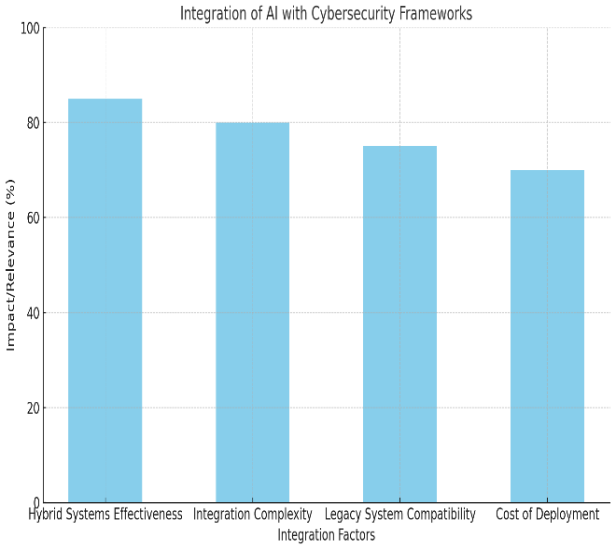

Figure 4: Integration of AI with Existing Cybersecurity Frameworks

Figure 4 illustrates key factors in integrating AI with existing cybersecurity frameworks, highlighting their impact or relevance. Hybrid systems' effectiveness is rated highest at 85%, indicating the potential of combining AI with traditional tools to enhance detection and response capabilities. Integration complexity follows at 80%, reflecting the technical challenges and resource requirements for incorporating AI into established frameworks. Legacy system compatibility poses a significant hurdle at 75%, as older infrastructure often lacks the flexibility to support AI-driven solutions. The cost of deployment, at 70%, underscores financial constraints as a barrier for organizations, particularly smaller ones. This analysis emphasizes the opportunities and challenges in embedding AI into existing cybersecurity systems.

6.5 Emerging Trends and Innovations

The study highlighted promising trends in AI-based cybersecurity. Federated learning models provided a solution to data privacy concerns by enabling collaborative training without direct data sharing. Blockchain integration improved the integrity and reliability of AI systems by creating immutable logs of cyber incidents. Edge computing emerged as a game-changer, enabling real-time threat detection and response in IoT environments. These innovations underscored the potential for future AI-driven cybersecurity systems to overcome current limitations.

6.6 Ethical and Regulatory Implications

Ethical concerns, particularly around data privacy and potential misuse of AI technologies, were significant findings. Surveillance risks associated with AI-driven monitoring raised questions about balancing security with individual rights. Regulatory compliance was also a challenge, with organizations navigating diverse cybersecurity laws across jurisdictions. Clear governance frameworks and adherence to ethical AI practices were identified as critical for responsible adoption. Based on the findings, several actionable recommendations were proposed. Organizations should focus on improving data quality by utilizing diverse and representative datasets while investing in adversarial defense mechanisms to counter AI-specific threats. Enhancing the interpretability of AI models through explainable AI techniques can build trust and foster adoption. Collaboration between industry, academia, and regulators is essential to address ethical and regulatory challenges. Emerging technologies like federated learning, blockchain, and edge computing should be further explored to optimize AI-driven cybersecurity systems.

In summary, the study demonstrated that while AI offers transformative capabilities in detecting and mitigating cyber threats, addressing its challenges requires a multidisciplinary approach involving technological innovation, ethical considerations, and policy development.

VII. FINDINGS

The study on the application of Artificial Intelligence (AI) in detecting and mitigating cyber threats revealed several critical insights:

1. AI demonstrated superior effectiveness in identifying complex and evolving cyber threats compared to traditional security systems. Techniques like machine learning (ML), deep learning, and natural language processing (NLP) were particularly successful in detecting malware, phishing attacks, and zero-day vulnerabilities.
2. AI's capability to automate threat responses and predict vulnerabilities was highlighted as a significant advantage. Systems powered by reinforcement learning and anomaly detection effectively isolated compromised systems and mitigated malware spread in real time.
3. Despite its potential, AI faces significant challenges, including adversarial attacks that exploit model vulnerabilities, data quality issues such as imbalanced datasets, and algorithmic biases affecting performance consistency. The lack of model interpretability ("black box" problem) and high resource requirements further hinder adoption.
4. Incorporating AI into existing cybersecurity frameworks proved challenging due to compatibility issues with legacy systems, technical complexity, and the high costs of deployment. However, hybrid approaches that combine AI with traditional systems showed promise in

ISSN (online): 2581-3048
Volume 9, Issue 1, pp 17-26, January-2025
https://doi.org/10.47001/IRJIET/2025.901003

enhancing overall cybersecurity effectiveness (M. Halimuzzaman, Sharma, & Khang, 2024).

5. Emerging trends such as federated learning, blockchain integration, and edge computing were identified as transformative advancements. These technologies address challenges like data privacy, system reliability, and real-time threat detection, respectively, enhancing AI's future potential in cybersecurity.
6. The study underscored ethical concerns related to AI-driven surveillance and dual-use misuse, along with the challenges of adhering to diverse cybersecurity regulations. Addressing these concerns is essential for responsible and widespread adoption of AI in cybersecurity.
7. The findings emphasized the need for improved data quality, adversarial defense mechanisms, and explainable AI techniques to enhance model reliability and trust. Multidisciplinary collaboration among industry, academia, and regulators was recommended to navigate technical, ethical, and policy challenges effectively.

These findings highlight the transformative potential of AI in cybersecurity while acknowledging the complexities and challenges that must be addressed to fully leverage its capabilities.

VIII. RECOMMENDATIONS

1. Organizations should focus on collecting diverse and representative datasets to reduce biases and improve the reliability of AI models in detecting cyber threats across varied environments (Hossain & Islam, 2022).
2. Robust adversarial defense mechanisms should be developed and integrated into AI systems to prevent attackers from exploiting vulnerabilities (K. Hassan et al., 2022).
3. Efforts should be made to design interpretable AI models that provide clear insights into their decision-making processes, fostering trust among security teams and stakeholders (S. Hassan et al., 2022).
4. Collaboration between cybersecurity experts, AI developers, and policymakers is essential to address technical challenges and ethical concerns effectively (Rasheed et al., 2022).
5. Organizations should explore innovative technologies like federated learning for privacy-preserving AI, blockchain for system integrity, and edge computing for real-time threat detection in IoT environments (Ghosh, Afnan, et al., 2023).
6. Increasing investments in training programs for professionals in both AI and cybersecurity domains will bridge the talent gap and enhance the effective implementation of AI systems (Islam et al., 2022).
7. Establishing clear governance frameworks and adhering to ethical principles in AI-driven cybersecurity solutions will address concerns about surveillance risks, data privacy, and misuse (Ghosh, Mozumder, et al., 2023).

IX. LIMITATIONS

1. AI models require vast amounts of labeled data for training, which is often limited by privacy concerns and the proprietary nature of cybersecurity information (M. , W. H. A. , C. P. K. , & M. S. Halimuzzaman, 2024).
2. Deploying and maintaining AI-driven cybersecurity systems demand substantial financial and technical resources, posing a barrier for smaller organizations (Honey, 2019).
3. Ensuring AI systems perform effectively in large-scale and dynamic network environments remains a challenge due to processing demands and evolving threats (M. Halimuzzaman& Sharma, 2022).
4. AI models are susceptible to adversarial attacks, which can compromise their reliability and effectiveness in detecting sophisticated threats (M. Halimuzzaman, Sharma, Karim, et al., 2024).
5. The use of AI for monitoring and threat detection raises ethical dilemmas, such as potential misuse for surveillance and conflicts with privacy laws (M. Halimuzzaman et al., 2023).
6. The integration of AI into legacy systems is challenging due to compatibility issues and the need for significant reengineering efforts (M. Halimuzzaman& Sharma, 2024).
7. AI systems require frequent updates to address new attack vectors, which can be resource-intensive and time-consuming (M. Halimuzzaman, Sharma, Bhattacharjee, et al., 2024).
8. A lack of skilled professionals in AI and cybersecurity hinders the development, deployment, and optimization of these technologies (Honey & Hossain, 2024).

By addressing these recommendations and limitations, organizations can harness AI's full potential to enhance cybersecurity while mitigating associated challenges.

X. CONCLUSION

The integration of Artificial Intelligence (AI) into cybersecurity represents a transformative step in combating the growing complexity and sophistication of cyber threats. This study highlights AI's exceptional capabilities in threat detection, mitigation, and proactive defense, surpassing traditional methods in accuracy, speed, and adaptability. Techniques such as machine learning, deep learning, and natural language processing have proven particularly effective in addressing challenges like malware detection, phishing

ISSN (online): 2581-3048
Volume 9, Issue 1, pp 17-26, January-2025
https://doi.org/10.47001/IRJIET/2025.901003

identification, and zero-day vulnerabilities. Despite its potential, AI's application in cybersecurity is not without challenges. Issues such as adversarial attacks, data quality limitations, algorithmic biases, and the "black box" nature of AI models hinder its reliability and widespread adoption. Integration with legacy systems, high implementation costs, and ethical concerns further complicate the deployment of AI-driven solutions. However, emerging trends like federated learning, blockchain technology, and edge computing present promising avenues to overcome these challenges and enhance AI's effectiveness. The study underscores the need for a multidisciplinary approach that combines technical innovation, ethical considerations, and policy alignment to maximize AI's impact in cybersecurity. By improving data quality, investing in adversarial defense mechanisms, fostering explainable AI, and addressing skill gaps, organizations can harness AI's potential responsibly. With continued advancements and collaboration among stakeholders, AI is poised to play an increasingly pivotal role in safeguarding digital ecosystems against evolving cyber threats.

REFERENCES

[1] Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review. *Electronics*, 11(2), 198.

[2] Ali, A., Septyanto, A. W., Chaudhary, I., Al Hamadi, H., Alzoubi, H. M., & Khan, Z. F. (2022). Applied artificial intelligence as event horizon of cyber security. *2022 International Conference on Business Analytics for Technology and Security (ICBATS)*, 1–7.

[3] Al-Raeei, M. (2024). The smart future for sustainable development: Artificial intelligence solutions for sustainable urbanization. *Sustainable Development*.

[4] Arif, H., Kumar, A., Fahad, M., & Hussain, H. K. (2024). Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research. *International Journal of Multidisciplinary Sciences and Arts*, 3(1), 242–251.

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

[6] Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. *Computer Science & IT Research Journal*, 5(6), 1505–1520.

[7] Chirra, D. R. (2023). AI-Based Threat Intelligence for Proactive Mitigation of Cyberattacks in Smart Grids. *Revista de Inteligencia Artificial En Medicina*, 14(1), 553–575.

[8] Damaraju, A. (2023). Artificial Intelligence in Cyber Defense: Opportunities and Risks. *Revista Espanola de Documentacion Cientifica*, 17(2), 300–320.

[9] Duary, S., Choudhury, P., Mishra, S., Sharma, V., Rao, D. D., & Aderemi, A. P. (2024). Cybersecurity threats detection in intelligent networks using predictive analytics approaches. *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)*, 1–5.

[10] Gadze, J. D., Bamfo-Asante, A. A., Agyemang, J. O., Nunoo-Mensah, H., &Opare, K. A.-B. (2021). An investigation into the application of deep learning in the detection and mitigation of DDOS attack on SDN controllers. *Technologies*, 9(1), 14.

[11] Ganesh, A. D., & Kalpana, P. (2022). Future of artificial intelligence and its influence on supply chain risk management–A systematic review. *Computers & Industrial Engineering*, 169, 108206.

[12] Ghillani, D. (2022). Deep learning and artificial intelligence framework to improve the cyber security. *Authorea Preprints*.

[13] Ghosh, P. R., Afnan, M., & Biswas, J. (2023). Neurocybernetic Assistive Technologies to Enhance Robotic Wheelchair Navigation. *Journal of Primeasia*.

[14] Ghosh, P. R., Mozumder, T., & Rashid, S. (2023). Navigating the AI Frontier: Advancements Redefining the World Wide Web's Future–A. *Journal of Primeasia*.

[15] Habila, M. A., Ouladsmane, M., &Alothman, Z. A. (2023). Role of artificial intelligence in environmental sustainability. In Visualization techniques for climate change with machine learning and artificial intelligence (pp. 449–469). *Elsevier*.

[16] Halimuzzaman, M. , W. H. A. , C. P. K. , & M. S. (2024). Public Relation and Educational Outcomes of Films in Bangladesh: A Study on Hawa. *Journal of Primeasia*, 5(1), 1–7. https://doi.org/10.25163/primeasia.519834

[17] Halimuzzaman, M., Sharma, D. J., Bhattacharjee, T., Mallik, B., Rahman, R., Rezaul Karim, M., Masrur Ikram, M., & Fokhrul Islam, M. (2024). Blockchain Technology for Integrating Electronic Records of Digital Healthcare System. *Journal of Angiotherapy*, 8(7).

[18] Halimuzzaman, M., & Sharma, J. (2022). Applications of accounting information system (AIS) under Enterprise resource planning (ERP): A comprehensive review. *International Journal of Early Childhood Special Education (INT-JECSE)*, 14(2), 6801–6806.

ISSN (online): 2581-3048
Volume 9, Issue 1, pp 17-26, January-2025
https://doi.org/10.47001/IRJIET/2025.901003

[19] Halimuzzaman, M., & Sharma, J. (2024). The Role of Enterprise Resource Planning (ERP) in Improving the Accounting Information System for Organizations. In Revolutionizing the AI-Digital Landscape (pp. 263–274). *Productivity Press*.

[20] Halimuzzaman, M., Sharma, J., Islam, D., Habib, F., & Ahmed, S. S. (2023). FINANCIAL IMPACT OF ENTERPRISE RESOURCE PLANNING (ERP) ON ACCOUNTING INFORMATION SYSTEMS (AIS): A STUDY ON PETROLEUM COMPANIES IN BANGLADESH. *China Petroleum Processing and Petrochemical Technology*, 23(2), 219–244.

[21] Halimuzzaman, M., Sharma, J., Karim, M. R., Hossain, M. R., Azad, M. A. K., & Alam, M. M. (2024). Enhancement of Organizational Accounting Information Systems and Financial Control through Enterprise Resource Planning. *In Synergy of AI and Fintech in the Digital Gig Economy* (pp. 315–331). *CRC Press*.

[22] Halimuzzaman, M., Sharma, J., & Khang, A. (2024). Enterprise Resource Planning and Accounting Information Systems: Modeling the Relationship in Manufacturing. *In Machine Vision and Industrial Robotics in Manufacturing* (pp. 418–434). *CRC Press*.

[23] Hassan, K., Ferdaus, J., & Mosharaf, T. (2022). Spirituality in Hospitality Services: An Assessment of Halal Tourism Practices. *Journal of Primeasia*.

[24] Hassan, S., Afrin, S., & Islam, M. R. (2022). A Wavelet-Based Approach to Rapidly Identify Drug-Addicted Individuals Using Voice Signal Analysis. *Journal of Primeasia*.

[25] Honey, S. (2019). Promoting Sustainable Marketing in the RMG Sector: A Step for Transformation. *AIUB Journal of Business and Economics*, 16(1), 30–42.

[26] Honey, S., & Hossain, M. J. (2024). Consumer Perception of Eco-Friendly Apparel: Insights from Bangladesh's RMG Sector. *INTERNATIONAL JOURNAL OF RESEARCH AND INNOVATION IN SOCIAL SCIENCE (IJRISS)*, VIII. https://doi.org/10.47772/IJRISS

[27] Hossain, M. M., & Islam, M. S. (2022). Policy Recommendations and Guidelines on Sustainable Tourism Development in Bangladesh–A Systematic Review. *Journal of Primeasia*, 3(1), 1–9.

[28] Islam, T., Islam, M. N., Zihad, M. A., & Datta, S. (2022). Toxic Leadership and Employee Misconduct of Hotel and Tourism Institution: A Frontline Perspective. *Journal of Primeasia*.

[29] Javaid, H. A. (2024). How Artificial Intelligence is Revolutionizing Fraud Detection in Financial Services. *Innovative Engineering Sciences Journal*, 4(1).

[30] Kalla, D., Kuraku, S., & Samaah, F. (2023). Advantages, disadvantages and risks associated with chatgpt and ai on cybersecurity. *Journal of Emerging Technologies and Innovative Research*, 10(10).

[31] Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804.

[32] Kodete, C. S., Thuraka, B., Pasupuleti, V., &Malisetty, S. (2024). Determining the efficacy of machine learning strategies in quelling cyber security threats: Evidence from selected literatures. *Asian Journal of Research in Computer Science*, 17(8), 24–33.

[33] Kunduru, A. R. (2023). Artificial intelligence advantages in cloud Fintech application security. *Central Asian Journal of Mathematical Theory and Computer Sciences*, 4(8), 48–53.

[34] Maddireddy, B. R., &Maddireddy, B. R. (2021a). Cyber security Threat Landscape: Predictive Modelling Using Advanced AI Algorithms. *Revista Espanola de Documentacion Cientifica*, 15(4), 126–153.

[35] Maddireddy, B. R., & Maddireddy, B. R. (2021b). Enhancing Endpoint Security through Machine Learning and Artificial Intelligence Applications. *Revista Espanola de Documentacion Cientifica*, 15(4), 154–164.

[36] Meyer, T. (2022). Cyber Resilience Assessment Frameworks for Autonomous Vehicle Ecosystems: Develops frameworks to assess cyber resilience within the ecosystems of autonomous vehicles. *Journal of Artificial Intelligence Research and Applications*, 2(2), 1–11.

[37] Mohamed, N., Almazrouei, S. K., Oubelaid, A., Bajaj, M., Jurado, F., & Kamel, S. (2023). Artificial intelligence (AI) and machine learning (ML)-based Information security in electric vehicles: A review. *2023 5th Global Power, Energy and Communication Conference (GPECOM)*, 108–113.

[38] Nimmagadda, V. S. P. (2021). Artificial Intelligence and Blockchain Integration for Enhanced Security in Insurance: Techniques, Models, and Real-World Applications. *African Journal of Artificial Intelligence and Sustainable Development*, 1(2), 187–224.

[39] Pattyam, S. P. (2021). Artificial Intelligence in Cybersecurity: Advanced Methods for Threat Detection, Risk Assessment, and Incident Response. *Journal of AI in Healthcare and Medicine*, 1(2), 83–108.

[40] Perez-Diaz, J. A., Valdovinos, I. A., Choo, K.-K. R., & Zhu, D. (2020). A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning. *IEEE Access*, 8, 155859–155872.

ISSN (online): 2581-3048
Volume 9, Issue 1, pp 17-26, January-2025
https://doi.org/10.47001/IRJIET/2025.901003

[41] Rasheed, S., Nazneen, F., & Huda, M. N. (2022). The Kamranga Mosque: Architectural Synthesis and Heritage Significance in Colonial Dhaka-Review. *Journal of Primeasia*.

[42] Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. *Revista Espanola de DocumentacionCientifica*, 15(4), 42–66.

[43] Shwedeh, F., Malaka, S., & Rwashdeh, B. (2023). The Moderation Effect of Artificial Intelligent Hackers on the Relationship between Cyber Security Conducts and the Sustainability of Software Protection: A Comprehensive Review. *Migration Letters*, 20(S9), 1066–1072.

[44] Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. *ICT Express*, 8(3), 313–321.

[45] Weng, Y., & Wu, J. (2024). Leveraging artificial intelligence to enhance data security and combat cyberattacks. *Journal of Artificial Intelligence General Science (JAIGS) ISSN: 3006-4023*, 5(1), 392–399.

[46] 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.

[47] Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *IEEE Access*, 8, 23817–23837.

[48] Zhang, Z., Al Hamadi, H., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access*, 10, 93104–93139.

Citation of this Article:

Mahabubur Rahman, Imran Uddin, Rana Das, Tuhalika Saha, Engr. S.K. Moududdul Haque, Nahid Reza Shatu, & Shafiqul Islam Shafiq. (2025). Application of Artificial Intelligence in Detecting and Mitigating Cyber Threats. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 9(1), 17-26. Article DOI https://doi.org/10.47001/IRJIET/2025.901003

****

