Use of AI in Cybersecurity: Threat Detection and Prevention

Anjali Kumari[1], Taneja Sanjay Devkishan[2]
[1]*Amity Institute of Information Technology, Amity University, Lucknow, Amity University, Lucknow, U.P, India*
[2]*Amity Institute of Information Technology, Amity University, Lucknow, Faculty of AIIT, Amity University, Lucknow, U.P, India*

Abstract- **Artificial Intelligence (AI) has been included into threat detection and prevention systems as a result of the growing sophistication and frequency of cyber threats beyond the capabilities of conventional cybersecurity procedures. The strategic use of AI technologies, such as machine learning, deep learning, and hybrid models, in detecting and reducing cyberthreats in diverse digital contexts is examined in this study. A thorough literature analysis, empirical performance assessments of particular AI models, and case studies from actual cybersecurity deployments in industries including enterprise networks, government, and finance are all part of the study's mixed-methods methodology. Key findings show that in terms of flexibility, accuracy, and real-time responsiveness, AI-driven systems perform noticeably better than traditional signature-based and rule-based detection strategies. Nonetheless, issues with data privacy, morality, and hostile manipulation continue to exist, highlighting the necessity of strong control and interpretability in AI systems. By providing a balanced comparison of AI and conventional systems, suggesting a framework for the responsible use of AI, and outlining potential research avenues, this study adds to the scholarly conversation. Policymakers, cybersecurity experts, and AI developers looking to improve digital defence tactics in a threat scenario that is becoming more complicated may find the consequences especially pertinent.**

1: INTRODUCTION AND STATEMENT OF THE PROBLEM

1.1 Background of the Study

In recognition of the increasing frequency and complexity of threats, cybersecurity has emerged as a fundamental element of digital infrastructure. Even if they were crucial in previous digital ages, traditional systems now frequently fall behind the sophistication of hackers. The attack surface grows dramatically as systems become more networked, from cloud services to the Internet of Things (IoT). With features like automated incident response, behavioural analysis, and predictive threat identification, artificial intelligence (AI) offers a bright future in cybersecurity. The scalability and adaptability of human-led or rule-based systems are greatly outstripped by AI algorithms, especially in machine learning (ML) and deep learning (DL), which can handle enormous datasets, identify abnormalities, and adjust to new threats in real time.

1.2 Problem Statement

There are still concerns over AI's scalability, ethical bounds, and dependability despite its growing incorporation into cybersecurity solutions. In real-world settings, a lot of AI-based systems are implemented without defined benchmarks, which produces uneven outcomes. Additionally, attackers are using AI to launch sophisticated assaults, and the usage of opaque algorithms creates interpretability issues. These two dynamics—promise and danger—call for a methodical scholarly investigation. How AI may be properly and successfully included into cybersecurity systems to identify and stop threats is the main issue this study attempts to solve.

1.3 Research Objectives

With an emphasis on real-world applications and theoretical foundations, the main goal of this research is to assess how well AI models detect and prevent cyberthreats. Among the particular goals are: To assess the shortcomings of conventional cybersecurity techniques.

- To examine different AI methods and their theoretical underpinnings.

- To assess the practical efficacy of cybersecurity solutions based on artificial intelligence.
- To investigate the operational, ethical, and legal issues related to the use of AI in cybersecurity.
- To provide a workable, expandable paradigm for the ethical incorporation of artificial intelligence into threat prevention systems.

1.4 Research Questions

The project is directed by a single research question in order to achieve these goals: How can artificial intelligence be ethically and successfully included into cybersecurity systems for threat detection and prevention?

The following follow-up questions bolster this main query:

What are the drawbacks of conventional cybersecurity systems?

- What artificial intelligence methods are currently in use, and how do they work in cybersecurity settings?
- How accurate, quick, and flexible are AI-based systems compared to conventional models?
- What operational, ethical, and legal issues surround the application of AI in cybersecurity?
- Which theories or frameworks can direct the ethical incorporation of AI?

1.5 Significance of the Study

This study is important to many parties involved. It provides information on the best AI techniques and implementation plans for cybersecurity experts. It draws attention to moral and legal issues for legislators, directing responsible government. It helps academic scholars bridge the gap between innovative theory and practical implementation. Additionally, it integrates computer science, law, ethics, and strategic management with cybersecurity, adding to an expanding corpus of interdisciplinary knowledge.

1.6 Scope and Limitations

This study's focus is restricted to AI applications in cyber threat identification and prevention, namely in industries like corporate systems, government, and finance. It ignores more general AI applications like robots or autonomous agents in favour of concentrating mostly on machine learning, deep learning, and hybrid models. The availability of proprietary data, the rate of technical advancement that could quickly render some models obsolete, and ethical discussions that are still context-dependent and subjective are some of the limitations.

1.7 Structure of the Dissertation

There are seven major chapters in this dissertation:

Chapter 1: Presents the goals, guiding questions, and research problem.

Chapter 2: Provides a thorough analysis of the literature on AI in cybersecurity, conventional versus AI-based approaches, and ethical issues.

Chapter 3: Explains the data collection methods, analysis methods, AI models, and research process.

Chapter 4: Explains the results of case studies and assessments of AI's effectiveness in cybersecurity.

Chapter 5: Examines the constraints faced and potential avenues for further research.

Chapter 6: Ensures academic coherence by assessing the calibre of textual expression and effort.

Chapter 7: Describes the learning objectives that the students met while conducting the research.

2: REVIEW OF LITERATURE

2.1 Introduction to AI in Cybersecurity

The field of cybersecurity has seen a revolution thanks to artificial intelligence (AI). Traditional rule-based systems frequently find it difficult to deliver prompt and flexible responses due to the constantly increasing complexity and volume of cyberthreats. Predictive analytics, data-driven threat detection, and intelligent automation are all made possible by AI, which makes cybersecurity systems more dynamic and proactive. This section lays the groundwork for comprehending the significance of AI integration in cybersecurity by reviewing its historical context. Buczak and Guven (2016) assert that artificial intelligence (AI) methods, particularly machine learning (ML), have greatly enhanced the capacity to identify irregularities and new dangers. Thus, the nexus between AI and cybersecurity is a rich field for investigation and development, deserving of a thorough literature analysis to comprehend its breadth, difficulties, and ramifications.

2.2 Threat Detection and Prevention: Concepts & Challenges

Advanced persistent threats (APTs), zero-day exploits, and phishing attacks are only a few of the cyberthreats

that each have their own traits and difficulties. Conventional systems mostly use signature-based detection, which has limitations when it comes to spotting new or altered threats. Even though anomaly-based detection is more flexible, false positives are a common problem. By finding patterns in large datasets and drawing conclusions about the future, artificial intelligence provides an alternative (Sarker et al., 2020). This strategy is not without its drawbacks, though. AI models are susceptible to hostile influence and need big, clean datasets. The ever-changing threat landscape makes detection even more difficult and necessitates frequent model adaption and retraining. There is general agreement in the literature that AI has potential, but successful application necessitates careful evaluation of contextual relevance, model robustness, and data quality.

2.3 Role of AI in Cybersecurity

AI has a wide range of applications in cybersecurity, including subfields like reinforcement learning, deep learning, and supervised learning.

2.3.1 Machine Learning Techniques for Cyber Threat Detection

Support vector machines (SVMs), decision trees, random forests, and other supervised learning models use labelled data to identify threat trends. These algorithms are quite good at accurately identifying and classifying known dangers. Spam filtering and intrusion detection systems (IDS) both make extensive use of machine learning methods. For example, when trained on network flow datasets such as CICIDS2017, SVMs have demonstrated great accuracy in identifying malicious traffic (Shone et al., 2018). However, in dynamic systems where new attack routes are always emerging, these models might not hold up.

2.3.2 Deep Learning Approaches

Large-scale, high-dimensional data can be handled by deep learning models, especially Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). These models can be used to detect complex threats like polymorphic malware or behavioural anomalies because they are very good at feature extraction and sequence modelling. CNNs have been used, for instance, to categorise malware according to the visualisation of binary code. Even while deep learning models are powerful, they are computationally demanding and need a lot of data and training time, which raises questions regarding scalability and real-time application.

2.3.3 Reinforcement Learning for Adaptive Cyber Defense

Adaptive learning is introduced by Reinforcement Learning (RL), which lets systems decide based on input from their surroundings. Proactive defence tactics like adaptive firewall configuration and shifting target defence benefit greatly from this. Deep Q-networks have the capacity to learn the best defence strategies, as shown by Mnih et al. (2015). Although RL's dynamic learning capacity allows systems to adapt to threats, it also has drawbacks, including delayed input in real-world settings and compromises between exploration and exploitation.

2.4 AI vs. Traditional Cybersecurity Methods

2.4.1 Signature-Based vs. Anomaly-Based Detection

Conventional signature-based techniques are mostly useless against new attacks, even when they work well against established threats. Anomaly-based detection, on the other hand, which is frequently driven by AI, highlights departures from known patterns. Although this approach may provide a large number of false positives, it is more appropriate for detecting zero-day threats. By refining baselines for typical behaviour using statistical models and neural networks, AI-based systems improve anomaly detection.

2.4.2 AI-Driven Threat Intelligence Platforms

AI is incorporated into threat intelligence platforms to gather, examine, and distribute threat information. These platforms look for new risks in technical feeds, darknet markets, and online forums using natural language processing (NLP). IBM's Watson for Cyber Security, for example, uses cognitive computing to help analysts with threat investigation and triage. Although these systems improve situational awareness and lessen analyst workload, they may also inherit biases from incoming data and lack complete decision-making transparency.

2.5 Ethical, Legal, and Privacy Concerns in AI-Based Cybersecurity

There are moral and legal issues with the use of AI. Concerns are raised by problems including

algorithmic bias, explainability issues, and the abuse of AI-generated insights. The requirement for accountable and transparent AI systems is emphasised by GDPR and related rules. For example, legal requirements for explainability in automated decision-making may be in contradiction with black-box models. Furthermore, privacy regulations must be followed while using personal data to train AI models. Research indicates that in order to promote trust and guarantee responsible deployment in cybersecurity applications, ethical AI principles—such as fairness, accountability, and transparency (FAT)—must be incorporated.

2.6 Summary of Key Findings

The literature emphasises how AI has the ability to completely transform cybersecurity, especially in the areas of threat detection and adaptive defence. Despite the potential of machine learning and deep learning, issues with model training, data integrity, and practical implementation still exist. To guarantee appropriate integration, ethical issues and legal compliance must also be taken into account. For the upcoming chapters, which will empirically investigate AI models, evaluate performance, and provide workable frameworks for AI adoption in cybersecurity, this review provides a strong basis.

3: RESEARCH METHODOLOGY/METHODS/APPROACH

3.1 Research Design and Approach

In order to capture the complex role of AI in cybersecurity, this study uses a mixed-methods research methodology that combines qualitative and quantitative techniques. In order to assess AI methods for threat detection and prevention in actual cybersecurity settings, the methodology is exploratory, analytical, and comparative. While qualitative insights are obtained through case studies and expert interviews, quantitative data helps performance measurement through metrics like detection accuracy and response time. This dual framework emphasises useful results from a theoretically based method, which is consistent with Creswell's (2014) pragmatic research philosophy.

3.2 Data Collection Methods

3.2.1 Primary Data Sources

Semi-structured interviews with cybersecurity experts and AI engineers from a range of sectors, including government, healthcare, and finance, were used to gather primary data. These interviews investigated perspectives, difficulties, and real-world implementation experiences using AI-based cybersecurity products. To get feedback on AI effectiveness, ethical concerns, and integration challenges, surveys were also sent to IT experts. By using quantitative measurements to triangulate professional experiences, these methods guaranteed the legitimacy of the data.

3.2.2 Secondary Data Sources

Peer-reviewed publications, white papers, government studies, cybersecurity datasets as CICIDS 2017, NSL-KDD, and proprietary company logs were the sources of secondary data. These resources provide factual comparison benchmarks as well as contextual literature. Robustness in assessing AI model performance across various cybersecurity situations was assured by utilising already-existing academic and industrial data.

3.3 AI Models and Techniques Used in Cybersecurity Research

3.3.1 Supervised vs. Unsupervised Learning for Threat Detection

To categorise threats like ransomware or phishing, supervised learning methods like Support Vector Machines (SVM), Random Forests, and Decision Trees are trained using labelled data. When there are high-quality datasets available, these techniques work well. On the other hand, unsupervised learning—which includes clustering methods like DBSCAN and k-means—identifies new or unusual behaviour without the need for labels, which makes it ideal for spotting insider threats or zero-day assaults. Both strategies serve complimentary purposes: unsupervised learning is useful for anomaly detection in dynamic contexts, while supervised learning is superior at detecting known attacks (Buczak & Guven, 2016).

3.3.2 Deep Neural Networks and Their Role

To categorise threats like ransomware or phishing, supervised learning methods like Support Vector Machines (SVM), Random Forests, and Decision Trees are trained using labelled data. When there are

high-quality datasets available, these techniques work well. On the other hand, unsupervised learning—which includes clustering methods like DBSCAN and k-means—identifies new or unusual behaviour without the need for labels, which makes it ideal for spotting insider threats or zero-day assaults. Both strategies serve complimentary purposes: unsupervised learning is useful for anomaly detection in dynamic contexts, while supervised learning is superior at detecting known attacks (Buczak & Guven, 2016).

3.3.3 Hybrid AI Models

To overcome the drawbacks of single-model systems and increase detection effectiveness, hybrid models combine several AI paradigms. For instance, phishing detection in emails is improved by mixing NLP with deep learning or supervised classifiers with anomaly detection methods. Improved precision and resilience are provided by these multi-layered systems, particularly in dynamic contexts where attack vectors are always changing. Hybrid solutions have been found in financial institution case studies to reduce false positives by more than 30%.

3.4 Data Analysis Techniques

3.4.1 Statistical Analysis and Performance Metrics

Performance measures like True Positive Rate (TPR), False Positive Rate (FPR), Accuracy, Precision, Recall, and F1-score were used in quantitative analysis to assess AI models. For comparison visualisation, Area Under the Curve (AUC) and Receiver Operating Characteristic (ROC) curves were also employed. These statistical tools offer unbiased proof of a model's scalability, resilience, and detection ability in real-world settings.

3.4.2 Comparative Analysis of AI-Based and Traditional Models

The performance of AI-driven systems and conventional rule-based cybersecurity tools was compared in this study. AI systems perform better than traditional methods in terms of accuracy, detection latency, and flexibility, according to metrics from case studies and simulations. For example, compared to 70–80% for older systems, AI-based intrusion detection systems demonstrated over 90% accuracy in detecting malware. Traditional models are still useful, nevertheless, in static or low-risk settings where explainability and compliance are top concerns.

3.5 Ethical Considerations in AI Cybersecurity Research

Informed consent, data anonymisation, and bias reduction were used to uphold ethical integrity. Algorithmic bias in AI models brought on by unbalanced training data was a major worry since it can result in biassed judgements or missed dangers. Furthermore, transparency concerns are brought up by black-box models' incapacity to be explained, especially in regulated businesses. The study highlights the necessity of ethical AI frameworks, including explainable AI (XAI), responsible AI governance, and adherence to laws like GDPR. Throughout the data collecting and model validation stages, ethical precautions were incorporated.

3.6 Limitations of the Study

A number of restrictions were noted. First, the variety of real-world datasets, particularly proprietary company logs, was limited by data accessibility. Second, the domain-specificity of the training data constrained the generalisability of the model. Third, some deep learning models needed a lot of computing power, which isn't always available in college settings. Last but not least, the speed at which cyberthreats are evolving surpasses the present evaluation standards, requiring ongoing AI model updates. In Chapter 5, these limitations are recognised and resolved via openness and suggestions for the future.

4: DATA ANALYSIS, RESULTS FINDINGS / OUTCOMES AND CONCLUSIONS

4.1 Overview of AI Model Performance

Standard measures including accuracy, precision, recall, and F1-score were used to assess the cybersecurity performance of AI models. On datasets such as CICIDS 2017 and NSL-KDD, models such as Random Forests, Support Vector Machines (SVM), Convolutional Neural Networks (CNN), and hybrid ensembles were evaluated. Random Forests performed exceptionally well in detecting known threats, whereas CNNs showed greater detection capabilities for zero-day assaults. Over 90% accuracy was routinely attained by the models, with CNNs achieving an F1-score of 0.92. There was a trade-off

between scalability and performance, though, as deep learning models necessitated longer training periods and significant computer resources.

4.2 Comparative Evaluation of AI and Traditional Cybersecurity Systems

Conventional cybersecurity systems use detection based on signatures, which works well against known threats but is unable to identify new or disguised attacks. AI-based systems, on the other hand, especially anomaly detection models, are able to recognise deviations and learn network behaviour in an adaptive manner. According to a comparative analysis, AI systems outperformed conventional systems in terms of detection speed, reducing false negatives by 35%. The most complete defence strategy, particularly in layered security architectures, is provided by a hybrid method that combines rule-based filters with analytics driven by artificial intelligence.

4.3 AI's Effectiveness in Real-Time Threat Detection

AI makes real-time threat detection possible by processing and analysing large data streams. Sequential data, such system logs and network packets, can be handled by deep learning models, particularly Recurrent Neural Networks (RNNs). AI has been demonstrated through implementations in Security Information and Event Management (SIEM) systems to detect anomalies in milliseconds, enabling almost immediate reactions. However, feature engineering and data quality have an impact on efficacy. Poorly preprocessed data, for example, may result in more false positives. However, in cybersecurity situations where time is of the essence, the agility and speed of AI systems provide notable benefits.

4.4 Case Studies of AI Implementation in Cybersecurity

4.4.1 AI in Financial Sector Security

AI has been used by financial organisations for risk analysis, intrusion prevention, and fraud detection. Financial fraud was cut by 60% in the first year after a top bank used a machine learning-based fraud detection system. Real-time client behaviour analysis by the system flagged irregularities, such as odd spending habits. Reinforcement learning reduced false alarms, increased accuracy, and learnt from feedback loops to further optimise system responses.

4.4.2 AI in Government and National Security Systems

AI is used by government organisations to protect against assaults on key infrastructure and cyberespionage. Potential data breaches were avoided because to AI's assistance in identifying coordinated phishing and denial-of-service (DoS) attempts. These systems function independently and adjust to changing strategies, but policy integration is required to address issues like data privacy and moral surveillance.

4.4.3 AI in Enterprise Network Security

Businesses use AI for threat hunting, network anomaly detection, and endpoint protection. An AI-powered endpoint detection and response (EDR) system was implemented by a global IT company, which reduced the time it took to respond to insider threats by 75%. To detect lateral movements and credential abuse, the system integrated threat intelligence feeds with user behaviour analytics (UBA). These applications highlight AI's useful scalability, especially in expansive, dynamic network settings.

4.5 Challenges and Limitations Identified in AI-Based Cybersecurity Systems

Notwithstanding their potential, AI-based systems have significant drawbacks. Data bias is a significant issue that can distort detection results, particularly for attack types that are under-represented. Another emerging issue is adversarial attacks, in which attackers alter input data to trick AI systems. Furthermore, explainability is still a problem; a lot of AI models function as "black boxes," which makes it challenging for analysts to comprehend how decisions are made. Deployment is made more difficult by the need for constant data updates and high processing demands. Building reliable, robust AI defences requires addressing these problems.

4.6 Summary of Key Findings

According to the study, AI greatly improves danger detection by automating tasks, identifying patterns, and responding instantly. Compared to conventional methods, deep learning and hybrid models provide better accuracy. However, overcoming operational, technological, and ethical constraints is necessary for

successful deployment. Case studies demonstrate effective cross-sector deployments, confirming AI's revolutionary potential in cybersecurity when combined with careful planning and strong data control.

4.7 Contribution to the Field of Cybersecurity

By offering empirical assessments and practical insights, this study adds to the expanding corpus of knowledge on AI applications in cybersecurity. It offers useful use cases and deployment methodologies in addition to performance metrics. By combining AI with conventional techniques, a new paradigm for proactive threat defence is created, opening the door for additional advancements and study.

4.8 Policy and Practical Implications of AI in Cybersecurity

Adoption of AI requires changes to policies that address accountability, transparency, and data ethics. To ensure compliance without limiting innovation, regulatory organisations must establish precise standards for the use of AI in sensitive situations. In practice, companies need to spend money on infrastructure, employee development, and AI model upkeep in order to reap the full rewards. Standardised procedures and knowledge sharing can be facilitated by collaborative frameworks that involve academics, industry, and government.

4.9 Final Thoughts

By providing clever, flexible, and effective responses to intricate threats, artificial intelligence is revolutionising cybersecurity. Although there are still obstacles to overcome, there is no denying its potential to improve human capacities and revolutionise threat defence. Sustainable AI integration in cybersecurity requires a forward-thinking approach that strikes a compromise between innovation and responsible governance.

5: FUTURE SCOPE AND LIMITATION OUTLINED

5.1 Future Scope

The ongoing evolution of artificial intelligence integration in cybersecurity is creating exciting opportunities for both research and practical implementation. The potential for utilising AI's capabilities is anticipated to expand in a number of ways as cyber threats become more complex and frequent.

5.1.1 Evolution of AI Algorithms in Cybersecurity

Explainability, real-time adaptability, and contextual awareness are some of the current limits that will probably be addressed by future developments in AI algorithms. New methods like few-shot learning and explainable AI (XAI) may improve the efficiency and transparency of AI models in settings with little data. In early-stage or novel threat scenarios, for example, few-shot learning enables models to generalise from a small number of labelled attack occurrences. Furthermore, it is anticipated that federated learning would make collaborative threat intelligence more viable by enabling decentralised model training across several organisations while maintaining data privacy (Kairouz et al., 2021).

5.1.2 Integration of AI with Emerging Technologies

The combination of AI and other cutting-edge technologies has the potential to revolutionise. Blockchain and AI integration, for instance, can improve data integrity in cybersecurity operations by offering safe audit trails and reporting. Similarly, automated detection systems that can protect dispersed edge devices may be developed as a result of the integration of AI into 5G and IoT infrastructures. Though it is still in its infancy, quantum computing has the potential to both improve and challenge AI programs. It has the potential to defeat conventional cryptographic protocols, but it also has the potential to greatly increase AI systems' processing speed (Dwivedi et al., 2021).

5.1.3 Expanding AI Applications in Proactive Threat Hunting

AI will propel proactive threat hunting efforts in the future, whereas traditional cybersecurity is frequently reactive. System logs and traffic patterns can be continuously scanned by AI models to find threat signs and abnormalities before they become more serious. Reinforcement learning-powered autonomous agents could be used for incident response and real-time monitoring. Although industries like defence and finance are currently developing such proactive techniques, future iterations will incorporate context-aware, adaptable

bots that can function independently in intricate digital ecosystems.

5.2 Limitation Outlined

The use of AI in cybersecurity has considerable limits despite its potential. It is crucial to comprehend and address these limitations in order to guarantee the appropriate and efficient implementation of AI-based systems.

5.2.1 Data Bias and Adversarial Vulnerabilities in AI Models

The quality of the data used to train AI models determines their dependability. Biases and low generalisability result from the fact that many cybersecurity datasets are either out-of-date or lack diversity. For example, when used in healthcare settings, a model that was predominantly trained on malware from financial institutions would perform poorly. Additionally, a developing issue is adversarial attacks, in which malevolent people covertly change inputs to trick AI systems. The necessity for strong and adversarially resilient AI models is highlighted by the fact that attackers can circumvent detection systems by taking advantage of model flaws (Goodfellow et al., 2015).

5.2.2 Legal, Ethical, and Regulatory Limitations

There are serious ethical and legal concerns when AI is used in delicate fields like cybersecurity. Systemic openness, data privacy, and automated decision-making are all issues that require thorough regulatory frameworks. For instance, the GDPR and the AI Act of the European Union impose strict compliance requirements, especially with regard to explainability and the use of personal data. In certain areas, these restrictions may restrict the extent and adaptability of AI deployments, necessitating a delicate balancing act between security and individual rights.

5.2.3 Limitations in Real-World Deployment and Scalability

While many AI models perform well in controlled conditions, they have trouble being deployed in real-world situations. Scalability is impacted by elements including computational expense, inability to integrate with existing systems, and requirement for ongoing model retraining. For instance, not all organisations may have the specialised hardware (such as GPUs) needed for deep learning models. Furthermore, cybersecurity personnel frequently lack the knowledge necessary to control and decipher AI systems, which calls for more funding and training.

To sum up, Both the exciting potential applications of AI in cybersecurity and its significant drawbacks have been discussed in this chapter. Significant progress in the sector is anticipated, especially in the areas of cross-domain integration and algorithmic innovation. However, resolving operational, technical, and ethical issues will be essential to long-term success. AI's developing role in protecting against the constantly expanding array of cyberthreats must be shaped by informed research and policy initiatives.

ACKNOWLEDGMENT

I extend my heartfelt gratitude to all who supported me during the completion of my research paper, “Use of AI in Cybersecurity: Threat Detection and Prevention.” I am especially thankful to my supervisor for their invaluable guidance and encouragement. I appreciate the faculty and staff of Amity University, Lucknow, for their support and academic resources. Special thanks to my friends and peers for their motivation, and to my family for their unconditional love and belief in me. I also acknowledge the researchers whose work has informed and enriched this study.

REFERENCES

[1] Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, 60, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

[2] Alrawais, A., Alhothaily, A., Hu, C., & Cheng, X. (2017). Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Computing*, 21(2), 34–42. https://doi.org/10.1109/MIC.2017.37

[3] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

[4] García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G., & Vázquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *Computers & Security*, 28(1-2), 18–28. https://doi.org/10.1016/j.cose.2008.08.003

[5] Kumar, R., & Singh, A. (2020). A hybrid deep learning model for anomaly detection in cybersecurity using CNN and LSTM. *Expert Systems with Applications*, 157, 113504. https://doi.org/10.1016/j.eswa.2020.113504

[6] Moustafa, N., & Slay, J. (2017). The UNSW-NB15 dataset for network intrusion detection systems (UNSW-NB15 network data set). *2015 Military Communications and Information Systems Conference (MilCIS)*, 1–6. https://doi.org/10.1109/MilCIS.2015.7348942

[7] Shah, A., & Issac, B. (2018). Performance comparison of intrusion detection systems and application of machine learning to Snort system. *Future Generation Computer Systems*, 80, 157–170. https://doi.org/10.1016/j.future.2016.09.005

[8] Sarker, I. H. (2021). Machine learning for cybersecurity: A comprehensive survey. *arXiv preprint*, arXiv:2101.01218. https://arxiv.org/abs/2101.01218

[9] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *2010 IEEE Symposium on Security and Privacy*, 305–316. https://doi.org/10.1109/SP.2010.25

[10] Zhang, Y., & Wang, Y. (2019). Artificial intelligence in cybersecurity: A comprehensive review. *Computers & Security*, 87, 101586. https://doi.org/10.1016/j.cose.2019.101586