International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

AI-Enabled Cybersecurity System for Smart Threat Detection and User Authentication

Mrs. Gayathri N[1], Mrs.Nayana Rao S[2], Mrs. Bhavani K G[3], Mrs.Pankaja K N[4]

[1 2,3,4]ASST. Professor(CSE),
[1,2,3,4]Department of Computer Science and Engineering, City Engineering College, Bangalore,Karnataka, India.

Abstract:
Cybersecurity threats are increasing rapidly because of the growth of digital platforms, cloud systems, smart devices, and online communication. Traditional security systems are unable to detect advanced attacks effectively because they depend mainly on fixed rules and signature-based approaches. This research presents an AI-based cybersecurity structure that incorporates
Machine Learning, deep learning, phishing detection, adaptive authentication, and intelligent network monitoring techniques. The suggested framework improves attack detection accuracy, reduces fraud activities, supports Real time monitoring, and strengthens user authentication. The study also compares traditional cybersecurity systems with AI-driven systems and explains the benefits of intelligent automation in modern security environments.

Keywords: Artificial Intelligence(AI), Cybersecurity, Machine learning(ML), Deep Learning, Phishing Detection, Adaptive Authentication, Network Security

1. INTRODUCTION

Modern organizations rely heavily on digital infrastructure for communication, data storage, financial transactions, and online services. Because of this dependency, cyberattacks such as malware, phishing, ransomware, and identity theft are increasing continuously. Traditional cybersecurity techniques aren't always able to handle dynamic and complex attacks because they depend on predefined signatures and manual monitoring processes.
AI (Artificial Intelligence) and ML(Machine Learning) technologies have become important solutions for improving cybersecurity systems. AI-based systems are capable of analysing enormous volumes of data, identifying abnormal activities, and responding to threats automatically. Additionally, Deep Learning models can recognize hidden attack patterns and improve security performance in real-time environments.

This paper discusses the role of AI in threat detection, phishing prevention, endpoint security, adaptive authentication, and network monitoring. The study also explains AI's function in threat identification and presents an intelligent AI-based cybersecurity framework for better security management.

2. LITERATURE REVIEW

AI(Artificial Intelligence) has significantly improved cybersecurity systems by enabling intelligent threat detection, intrusion prevention, phishing detection, and adaptive authentication mechanisms. Several researchers have proposed AI-based approaches to strengthen cybersecurity frameworks. Abdiyeva Aliyeva and Hematyar [1] proposed an AI-based anomaly detection model for future network security systems. Their research focused on identifying abnormal network behavior using intelligent prediction techniques to improve defense against cyber threats. Abdulqadder et al. [2] introduced a multi-layer System for detecting and preventing intrusions in 5G cloud networks using AI-based defense mechanisms. Their framework combined SDN (Software Defined Networking)and NFV (Network Function Virtualization)technologies to enhance cybersecurity protection in modern communication networks.

Adewumi and Akinyelu [3] developed a hybrid strategy for identifying phishing emails utilizing Al-Khater et al. [6], who covered some methods for detecting cybercrime that make use of Machine Learning and artificial intelligence models. Their study classified several AI techniques and assessed their advantages and disadvantages in terms of successfully identifying cybercrimes. A hybrid deep learning system for phishing detection in cybercrime forensics was created by Alsubaei et al. [7]. Their model improved cybersecurity systems and real-time phishing attack detection by combining cutting-edge neural network algorithms. Alzaabi and Mehmood [8] examined new developments in machine learning-based insider threat identification. Their research demonstrated how AI methods may detect malevolent insider activity and enhance organisational security. improved phishing email identification accuracy and minimized false detection rates. Afzali Seresht.[4]suggested an Explainable Artificial Intelligence (XAI) model for security event analysis. Their work emphasized transparency and interpretability in AI-based cybersecurity systems to improve trust and decision-making capabilities. Ahmad et al. [5] provided a thorough analysis of AI-based phishing detection models. Their study analyzed Machine learning and provided a thorough analysis of learning approaches used for phishing attack detection and highlighted the significance of ensemble learning methods for achieving higher detection accuracy.

Alshehri et al. [9] proposed a cyberattack detection framework using Machine Learning and (User Behavior Analytics)UBA. Their system analyzed user activities and network behaviors to detect abnormal activities and unauthorized access attempts. Ahamed et al. [10] developed A clever multimodal biometric verification system model for healthcare services. Their AI-based authentication framework utilized biometric techniques to provide secure and reliable access control in healthcare environments. Siam et al. [11] presented a comprehensive review of Artificial Intelligence applications in cybersecurity. Their study discussed AI techniques used in threat detection, endpoint security, phishing detection, network security, and adaptive authentication while identifying future research opportunities.

AI-based methods for identifying zero-day hacks were assessed by Ali et al. [12]. Deep learning and machine learning models significantly improve the detection of unknown and emerging cyberthreats, according to their comparison study. A machine learning-based Endpoint Detection and Response (EDR) system was presented by Lee et al. [13] to detect sophisticated cyberattacks on endpoint devices. Their approach improved endpoint protection methods and attained excellent detection accuracy.

Hybrid AI models for Using deep learning techniques for phishing detectionwere proposed by Basit et al. [14]. By using lexical and semantic analysis techniques, their work enhanced the performance of phishingURL detection. A thorough analysis of DeepLearning methods for phishing detection was carried out by Kyaw et al. [15]. Their research demonstrated how well Bi-LSTM and Transformer models can identify phishing scams and fraudulent activity with high Accuracy.

3. EXISTING SYSTEM

Traditional cybersecurity systems mainly use firewalls, antivirus software, Systems for detecting intrusions based on signatures, and password-based authentication mechanisms. Predefined rules and saved attack signatures are used by these systems.

Existing systems have several limitations:
• Unable to identify unknown or zero-day attacks effectively.
• Require continuous manual updates and monitoring.
• Produce higher false alarm rates.
• Sensitive to changing attack patterns.
• Limited real-time adaptability.

Traditional phishing detection systems usually depend on blacklists and static URL analysis. Similarly, standard authentication systems rely mainly on passwords, which may be stolen through phishing or brute-force attacks.

4. PROPOSED SYSTEM

The suggested system presents an AI-based cybersecurity framework that incorporates Behavioural Analytics, Machine learning, deep learning, and natural language processing (NLP). The architecture is intended to increase security precision, automate surveillance, and identify sophisticated cyberthreats.

The proposed system includes:
• AI-based threat detection and prevention.
• Intelligent phishing and Fraud detection.
• Real-time network anomaly monitoring.
• Adaptive authentication using behavioral biometrics.
• Deep learning-based endpoint protection.

By continuously learning from fresh attack data, machine learning models automatically enhance detection performance. In real-time, deep learning models like CNN, RNN, and BiLSTM analyze intricate attack patterns and spot questionable activity.

5. SYSTEM ARCHITECTURE

The proposed AI-based cybersecurity framework is designed to provide intelligent threat detection, phishing prevention, secure authentication, and continuous network monitoring using AI(Artificial Intelligence) and ML(Machine Learning) techniques. The approach is made up of a number of linked modules that cooperate to improve cybersecurity protection and reduce cyber threats.

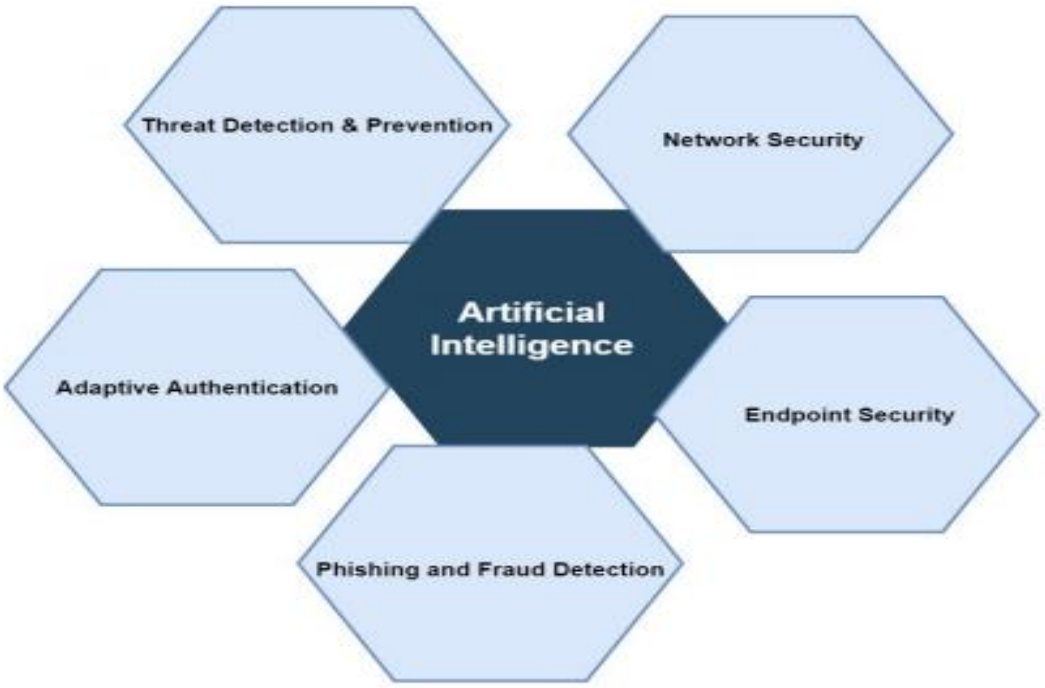

Figure 5.1:Artificial intelligence solution domain in security

A. THREAT DETECTION AND PREVENTION

1) Survey of AI-Based Approaches For Threat Detection

This section reviews research works related to AI-based threat detection systems. Malware is detected using a variety of Deep Learning and Machine Learning methods, intrusions, phishing attacks, and abnormal network activities. Studies show that AI improves detection accuracy and enables faster response to cyber threats. Researchers also discussed challenges such as false alarms, computational complexity, and privacy concerns.

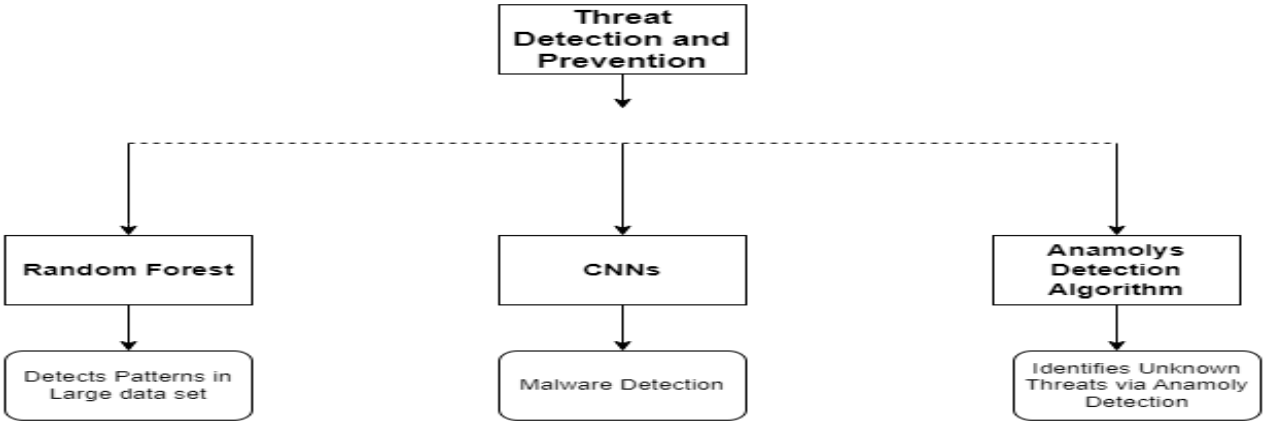

Figure 5.2 : Threat detection and prevention—key ML methods and their main roles

2) AI Model For Threat Detection And Prevention

A number of AI models are employed for threat detection and prevention. Random Forest algorithms help classify malicious activities from large datasets. Convolutional Neural Networks (CNNs) are effective in malware identification, whereas anomaly detection uses autoencoders and zero-day attack discovery. These models support proactive cybersecurity defense systems.

3) Key Comparisons of AI Models In Threat Detection And Prevention

Different AI models are compared based on detection accuracy, performance, scalability, and computational cost. Random Forest provides strong classification performance, CNNs improve malware analysis, and Autoencoders detect unknown threats effectively. However, some models require high processing power and large datasets.

B. NETWORK SECURITY

1) Survey of AI-Based Approaches For Network Security

The application of AI in network security is the main topic of this section. Network Intrusion Detection Systems (NIDS) with AI capabilities examine network traffic to spot questionable activity and intrusions. Numerous studies emphasise how the application of machine learning techniques can enhance real-time monitoring and attack prediction in contemporary networks.

2) AI Models For Network Security

AI models such as Isolation Forest, RNNs (Recurrent Neural Networks), and CNNs are frequently utilised in network security. These models help detect anomalies, analyze traffic patterns, and identify network intrusions. AI improves the efficiency of dynamic and adaptive network protection systems.

3) Key Comparisons of AI Models In Network Security

The modules are compared based on intrusion detection capability, accuracy, and adaptability. Isolation Forest Algorithms work well at identifying anomalies. False positives can be produced by models. and need, while RNNs and CNNs perform better in traffic pattern analysis. Some high computational resources.

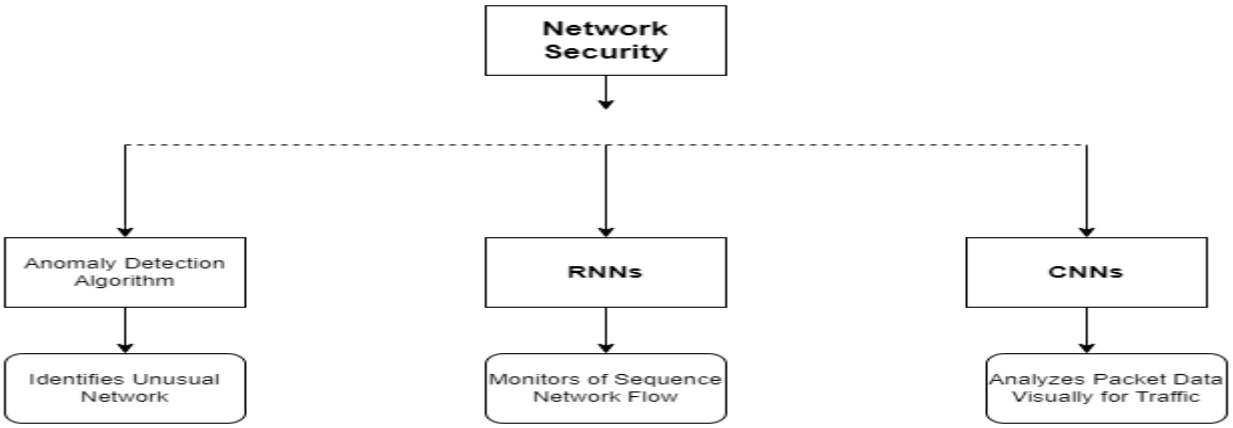

Figure 5.3 : Network security key ML methods and their main roles.

C. ENDPOINT SECURITY

1) Survey of AI-Based Approaches For Endpoint Security

This section reviews AI techniques used for protecting endpoint devices such as computers, laptops, and smartphones. AI-based systems monitor user and device activities to detect malware and unauthorized access. Research studies show improved attack detection and automated response mechanisms using AI technologies.

2) AI Model For Endpoint Security

RNNs, Deep Neural Networks (DNNs), and behavioral analysis models are commonly used in endpoint security. These models identify abnormal user behavior, insider threats, and advanced malware attacks. AI strengthens Endpoint Detection and Response (EDR) systems.

3) Key Comparisons of AI Models In Endpoint Security

The models are evaluated based on accuracy, behavioral analysis capability, and resource requirements. DNNs provide effective threat detection, while behavioral biometric models support real-time monitoring. But more Complex models require memory and computing power.

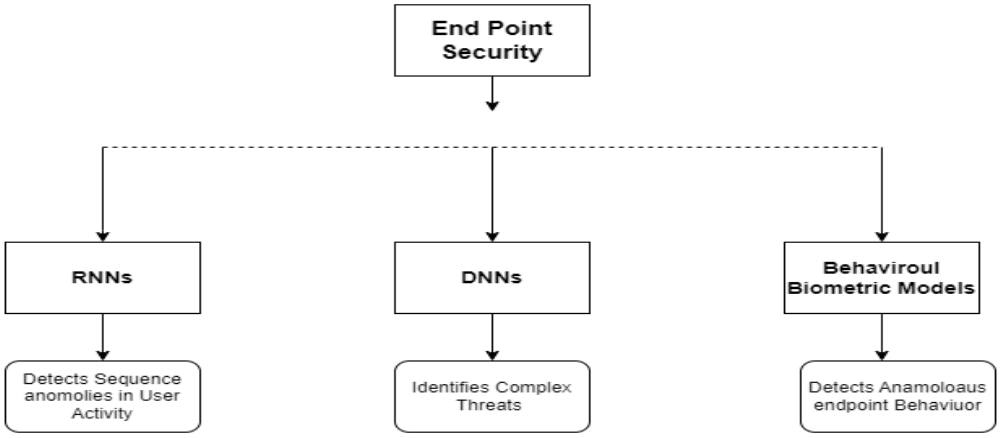

Figure 5.4: Endpoint security key ML Methods and their main roles

D. PHISHING AND FRAUD DETECTION

1) Survey of AI-Based Approaches For Phishing And Fraud Detection

The AI techniques for identifying phishing websites, bogus emails, and online fraud are examined in this section. Researchers examine URLs, website content, and user behaviour using deep learning and machine learning approaches. AI algorithms increase The accuracy of phishing detection and prevent fraud in real time.

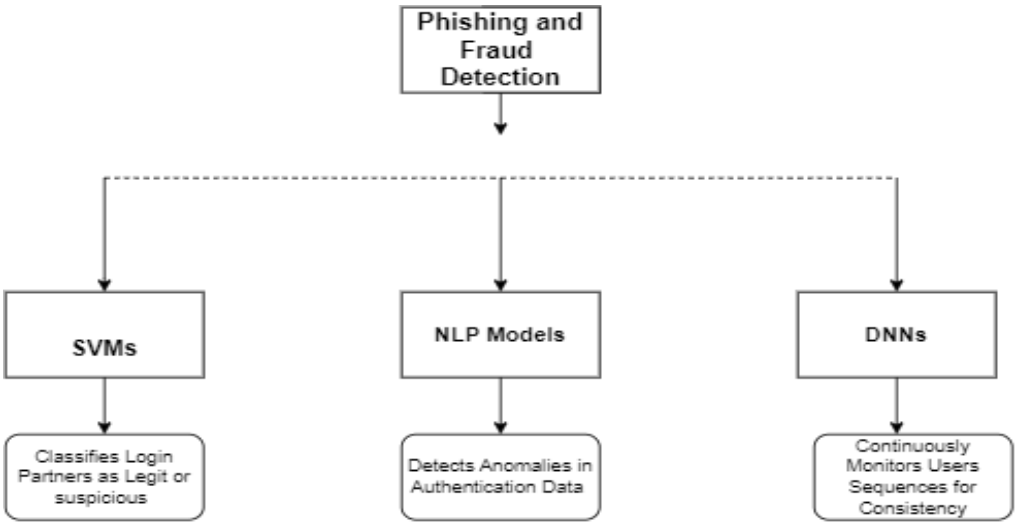

Figure 5.5: Phishing and fraud detection key ML methods and their main roles.

2) AI Models For Phishing And Fraud Detection

Phishing and fraud detection make extensive use of Natural Language Processing (NLP), Support Vector Machines (SVMs), and Deep Neural Networks (DNNs). To find malicious activity, these models examine transaction patterns, textual data, and suspicious activity.

3) Key Comparisons of AI Models In Phishing And Fraud Detection

The AI models are compared based on classification accuracy, scalability, and detection speed. NLP models effectively analyze phishing content, while DNNs improve fraud detection performance. Some techniques face challenges with imbalanced datasets and high computational complexity.

E. ADAPTIVE AUTHENTICATION

1) Survey of AI-Based Approaches For Adaptive Authentication

This section reviews AI-based adaptive authentication systems that improve access security using user behavior and biometric analysis. Studies discuss multimodal authentication methods, facial recognition, keystroke dynamics, and continuous user verification systems.

2) AI Models For Adaptive Authentication

Adaptive authentication frequently makes use of Support Vector Machines (SVMs), Random Forests, and RNNs (Recurrent Neural Networks). To ensure that enable secure authentication, these models examine user behaviour patterns and spot questionable login activity.

3) Key Comparisons of AI Models In Adaptive Authentication

The models are compared based on authentication accuracy, security performance, and adaptability. SVMs provide effective classification, Random Forest detects abnormal login patterns, and RNNs support continuous user authentication. Large training datasets and Certain models require a lot
Of computing power.

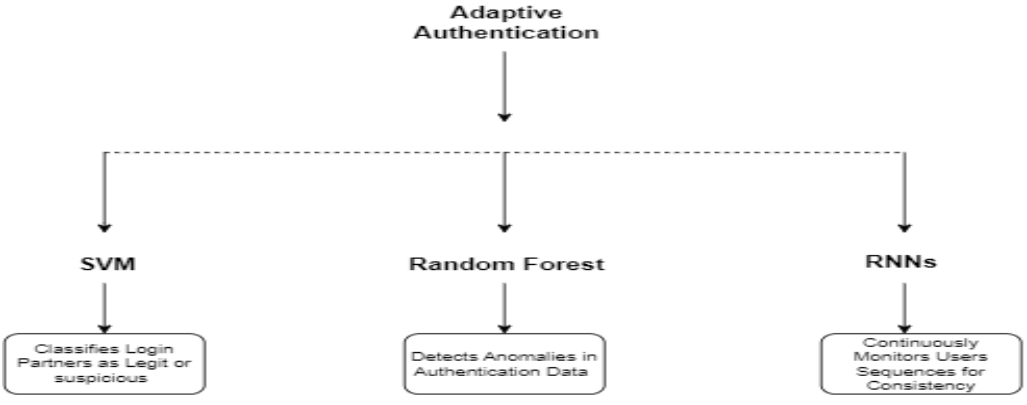

Figure 5.6 : Adaptive authentication key ML methods and their main roles

7. Results and Discussion

The proposed solution outperforms traditional cybersecurity systems. AI models reached a high level of threat detection accuracy, phishing identification, and adaptive authentication. The implementation of

deep learning and behavioral analysis improved overall security efficiency. The system also performed well under changing network conditions and evolving cyberattack strategies. Real-time monitoring reduced response delays and improved incident handling capabilities. Experimental analysis showed that AI-based systems significantly reduce fraud activities and improve overall cybersecurity management.

Solution Category Domain	AI Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Source
Threat Detection and Prevention	Random Forest + Autoencoder	99.83	99.86	99.82	99.83	PLOS ONE (2024) [28]
Endpoint Security	Support Vector Machine (SVM)	94.2	93.5	92.8	93.1	MDPI (2024) [12]
Phishing and Fraud Detection	BiLSTM + Attention Mechanism	99.61	99.00	99.50	99.24	Journal of Big Data (2024) [60]
Network Security	LSTM-Based Hybrid Model	95.74	95.8	96.2	96.0	arXiv (2024) [50]
Adaptive Authentication	Recurrent Neural Network (RNN)	95.78	94.5	94.8	94.6	Journal of Big Data (2024) [108]

Table 7.1: Result analysis of AI models across cybersecurity solution categories

LIMITATION AND FUTURE SCOPE

The prospect of implementing AI (Artificial Intelligence) in cybersecurity will dramatically alter approaches to security protection across diverse sectors. Nonetheless, some minor issues need to be brought to light to make the AI idea much more successful. In the table below, this section outlines the current constraints in addition to potential future research avenues to get beyond these obstacles.

Domain	Limitations	Future Research Directions
Threat Detection	Computational complexity - Data privacy concerns	Investigation of novel AI techniques - Addressing scalability issues, Real time threat detection capabilities
Endpoint Security	Adaptability to evolving threats - Scalability	Differentiation of ransomware family specific behaviors, Enhancement of detection tool functionality
Phishing and Fraud Detection	Handling evolving attack techniques - Maintaining detection accuracy over time	Incorporation of additional features like visual clues - Continuous model retraining and adaptation
Network Security	Protocol coverage limitations - Real-world applicability	Exploration of real time threat detection capabilities - Utilization of diverse data sources
Adaptive Authentication	Data quality issues - Spoofing attacks	Improvement of biometric system reliability - Enhancement of system scalability and real-time authentication capabilities

8. CONCLUSION

The rapid growth of the use of digital technologies has greatly improved cybersecurity challenges, making traditional security approaches less effective against advanced cyber threats. This study explored the role of Artificial Intelligence) AI in strengthening cybersecurity systems and improving the capacity to

identify, stop, and react to attacks efficiently. The research analyzed the application of artificial intelligence across important cybersecurity domains, including threat detection and prevention, network security, endpoint protection, phishing and fraud detection, and adaptive authentication. Different AI techniques, such as ML(Machine Learning), DL(Deep Learning), NLP(Natural Language Processing), and behavioral analysis models, were examined to understand their efficiency in modern security environments. The results show that AI-based cybersecurity systems provide several advantages, including improved threat identification, automated response mechanisms, faster attack analysis, and enhanced real-time monitoring capabilities. AI models are capable of identifying complex attack patterns and detecting abnormal activities that may not be recognized by conventional security methods. Despite these benefits, certain limitations remain in AI-driven cybersecurity solutions. High computational requirements, dependency on quality training data, scalability challenges, and concerns related to data privacy continue to affect implementation. In addition, cyber attackers constantly develop new attack techniques, which require continuous updates and improvements in AI security models. Overall, this study demonstrates that artificial intelligence is now a crucial part of contemporary cybersecurity frameworks. Future studies must concentrate on creating more adaptable, scalable, and explainable AI models that can provide stronger protection against emerging cyber threats. The incorporation of advanced AI technologies will support the evolution of secure and resilient digital systems for individuals, organizations, and critical infrastructures.

REFERENCES:

1. G. Abdiyeva-Aliyeva and M. Hematyar, “AI-based network security anomaly prediction and detection in future network,” in Proc. Int. Conf. Artificial Intelligence Applications and Innovations, Springer, 2022, pp. 149–159.
2. I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, and S. M. A. Akber, “Multi-layered intrusion detection and prevention in the SDN/NFV enabled cloud of 5G networks using AI-based defense mechanisms,” Computer Networks, vol. 179, 2020, Art. no. 107364.
3. O. A. Adewumi and A. A. Akinyelu, “A hybrid firefly and support vector machine classifier for phishing email detection,” Kybernetes, vol. 45, no. 6, pp. 977–994, 2016.
4. N. AfzaliSeresht, Q. Liu, and Y. Miao, “An explainable intelligence model for security event analysis,” in Proc. 32nd Australasian Joint Conference, Springer, 2019, pp. 315–327.
5. S. Ahmad et al., “Across the spectrum in-depth review AI-based models for phishing detection,” IEEE Open Journal of the Communications Society, 2024.
6. W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, “Comprehensive review of cybercrime detection techniques,” IEEE Access, vol. 8, pp. 137293–137311, 2020.
7. F. S. Alsubaei, A. A. Almazroi, and N. Ayub, “Enhancing phishing detection: A novel hybrid deep learning framework for cybercrime forensics,” IEEE Access, vol. 12, pp. 8373–8389, 2024.
8. F. R. Alzaabi and A. Mehmood, “A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods,” IEEE Access, vol. 12, pp. 30907–30927, 2024.
9. A. Alshehri, N. Khan, A. Alowayr, and M. Y. Alghamdi, “Cyberattack detection framework using machine learning and user behavior analytics,” Computer Systems Science and Engineering, vol. 44, no. 2, pp. 1679–1689, 2023.

10. F. Ahamed et al., “An intelligent multimodal biometric authentication model for personalised healthcare services,” Future Internet, vol. 14, no. 8, p. 222, 2022.
11. A. A. Siam, M. Alazab, A. Awajan, and N. Faruqui, “A Comprehensive Review of AI’s Current Impact and Future Prospects in Cybersecurity,” IEEE Access, vol. 13, pp. 14029–14046, 2025.
12. S. Ali, S. U. Rehman, A. Imran, G. Adeem, Z. Iqbal, and K.-I. Kim, “Comparative evaluation of AI-based techniques for zero-day attacks detection,” Electronics, vol. 11, no. 23, p. 3934, 2022.
13. Lee et al., “Machine Learning Enhanced Endpoint Detection and Response Framework,” Cybersecurity Journal, 2024.
14. Basit et al., “Hybrid AI Approaches for Phishing Detection Using Deep Learning,” IEEE Access, 2024.
15. Kyaw et al., “Deep Learning Techniques for Phishing Detection: A Systematic Review,” Journal of Information Security, 2024.