Adaptive AI-Driven Cybersecurity Framework for Real-Time Threat Detection and Automated Response in Evolving Digital Environments

K. A. Ajmath[1], Joy Pranahitha A.[2], Doddi Srilatha[3], S. Janani[4], Subathra N.[5] and N. Shirisha[6]
[1]Department of Computer Science, Samarkand International University of Technology, Uzbekistan
[2]Department of Computer Science and Engineering, Ravindra College of Engineering for Women, Kurnool, Andhra Pradesh, India
[3]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Bowrampet, India
[4]Department of Computer Science and Engineering, J.J.College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India
[5]Department of CSE, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India
[6]Department of CSE, MLR Institute of Technology, Hyderabad, Telangana, India

Keywords: Artificial Intelligence, Automatical Threat Response, Cybersecurity Framework, Real-Time Intrusion Detection, Adaptive Security Models.

Abstract: The growing number and sophistication of threats in modern digital environments require intelligent and adaptive defense systems. This work presents an AI-driven real-time cybersecurity framework to automate the detection and response of threats, aiming to overcome the shortcomings of state-of-the-art models, such as sluggish mitigation, fixed threat analysis, and generic zero-days resistance. Through a combination of techniques from deep learning, reinforcement learning, and explainable AI, this hybrid-based system improves efficiency of decision-making, and scalability with a transparent decision methodology. Unlike existing methods, this model is generic, tested on multiple infrastructures and applies dynamic behavior profiling to predict and prevent new attack vectors. The architecture is agnostic to cloud, on premise and hybrid instances, making it broadly applicable. The efficacy of the system is demonstrated through real-world traces, and the results show that the proposed system is superior in identifying polymorphic malware, protecting against DDoS attacks, and automatically reacting to multi-vector intrusions with low latency. This study introduces a scalable and interpretable AI cybersecurity model ready for next generation threat spaces.

1 INTRODUCTION

The explosive evolution of the digital landscape has changed the way we defend against attackers and highlighted the weakness of traditional defences. As a result of sophisticated, multi-vector, and evasive cyberattacks, static rule-based solutions have insufficient capabilities to provide efficient detection or forward-leaning response. Artificial Intelligence (AI) Artificial Intelligence (AI) is an age-defining technology that allows your security to not just recognize patterns, but to learn, adapt and respond to changes in threat models, without added human intervention. Although many models have sought to incorporate AI into cybersecurity, they often miss providing a real-time response, to work across platforms, and to make decisions autonomously without sacrificing transparency.

This project will address these key lacunae by creating a scalable, AI-centric cyber-security framework which is real-time and enable automated threat identification and mitigation across large scale, ephemeral digital infrastructures. Leveraging cutting-edge machine learning technologies, such as deep learning, reinforcement learning and explainable AI, the developed system offers intelligent situation awareness, adaptive behavior analysis and rapid incident response. Unlike traditional models, this can be seamlessly integrated in cloud as well as on-premise, to have the security defences applied in a scope aware and scalable manner. Findings The findings from this research provide a forward-looking solution which has the potential to change the way digital defence paradigms are implemented utilizing AI-driven automation and intelligence in response to ever evolving sophisticated cyber threats.

Ajmath, K. A., A., J. P., Srilatha, D., Janani, S., N., S. and Shirisha, N.
Adaptive AI-Driven Cybersecurity Framework for Real-Time Threat Detection and Automated Response in Evolving Digital Environments.
DOI: 10.5220/0013931000004919

In *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies (ICRDICCT'25 2025) - Volume 5*, pages 435-442
ISBN: 978-989-758-777-1

2 PROBLEM STATEMENT

With cyber threats advancing into more complex levels, classic rule-based and signature-based security mechanisms are unable to ensure real-time, proper and effective defence against dynamic and fast evolving attacks. Although existing AI-driven cybersecurity solutions are promising, they encounter some drawbacks, such as high computation complexity, poor real-time processing, the lack of self-response intelligence and narrow adaptability of heterogeneous IT environments. In addition, there has been a lack of all-in-one solutions that facilitate smart detection and automatic remediation, which has resulted in a leaving few critical infrastructures adamant to zero-day attacks, polymorphic malware, and multi vector assaults. Such a single, dynamic and scalable cybersecurity policy is urgently needed to not only identify threats in real-time but also to respond to threats automatically and without human intervention, to operate transparently, and efficiently in diverse digital ecosystems.

3 LITERATURE SURVEY

Recent developments in artificial intelligence (AI) have had a huge impact on the advancement of cybersecurity approaches. Alazab and Awajan (2021) examined the foundational fusion of AI into cybersecurity, emphasising its transformative potentialities alongside possible ethical issues that needs further attention. Hussain et al. (2021) also discussed issues that AI encounters in practice, especially against rapidly evolving threats. Goodfellow et al. (2021) highlighted ethical and technical issues of using autonomous AI in critical infrastructure, and indicated the need for interpretable AI models.

Machine learning is now central to threat detection. Berman et al. (2022) and Roy and Pande (2021) provided extensive surveys of AI models for cyberattack identification, but both admitted the weakness of addressing zero-day and polymorphic incidents. Javaid et al. (2021) showed applications of neural networks in smart grid systems, but they are not generic. Meanwhile, Kim et al. (2021) also proposed an aggregative deep learning model for DDoS detection but reported its low efficiency for remaining attack categories.

The tendency toward real-time and adaptive systems was also reflected in the work of Chen and Bridges (2023), who also suggested AI-based anomaly detection mechanisms, but did not focus on responses. In Kaur and Singh (2022), they have addressed the deep learning approach for the intrusion detection and found better accuracy but require excessive resources. Gao et al. (2022) extended this work by proposing hybrid models for real-time detection, however their architectures were not optimized to minimize latency.

Khan and Ghafoor (2023) introduce intelligent models and enhancing the detection accuracy, but the proposed models are limited only to the theoretical work and have not been practically implemented. Lin & Chen (2023) emphasized the use of AI for cybersecurity situational awareness development through NLP (competitive with CAIN's motivational dependency, but lacking a response component). In order to fill these gaps, He et al. (2022) presented reinforcement learning for adaptive threat management and highlighted the opportunity for it as well as practical deployment approaches.

Novel directions like federated learning (Li & Liu, 2022) and Explainable AI (Zhou & Huang, 2023) have focused on data privacy and model transparency, respectively, but many compromises on the speed and training complexity. Ma et al. Exploring transformer-based malware classification (2023) In, the authors attempted the deployment of the real time transformer-based malware classification model, but encountered the issue of resource depletion.

Other contributions include Nguyen and Armitage (2021), who conducted an extensive survey of AI in security operations centre (SOC) automation, however there is the question of whether ORT can scale in the same way? Subramanian and Thomas (2025) offered a blueprint towards AI-based intrusion detection; however, it did not have an empirical basis. Patel and Zaveri (2024) also concentrated on architecture design of AI threat intelligence, however it was not full-scale evaluated under dynamic scenarios.

Advanced scenarios were covered by Sharma and Gupta (2022) for deep adversarial models for malware obfuscation detection, a research conducted by Singh and Kapoor (2023) for hybrid AI techniques on cloud security. Kumar and Sinha (2024) investigated zero-day attack detection using behavior profiling and extended the limits of AI-based threat anticipation.

Wang (2024) proposed a prospective AI framework for threat detection, and Ali et al. (2022) in which they surveyed the applications of AI on cyber-physical systems, where real-time operational testing is absent. On the whole, these works build a

solid base for AI-based solutions for cybersecurity but they either converge on detection only, ignore response in real-time, or do not entirely consider flexible, cross-platform solutions.

This literature serves to highlight the urgency for a dynamic, AI-powered cyber defence framework that can effectively link detection with automated response and that is capable of ensuring resilience to diverse and changing digital environments.

4 METHODOLOGY

This approach can be viewed as consisting of several layers and aims to: - Design and implement an adaptive AI-driven cybersecurity framework that can detect threats in real time and make an automated response decision. The architecture is built to work with various digital environments: cloud, on-premise, and hybrid environments which makes it scalable and cost-effective.

Based on a modular architecture, the framework consists of four fundamental components: Data Acquisition, Threat Detection, Automated Response, and Feedback Loop. Data Collection layer continuously receives raw data from network endpoints such as firewalls, routers, IoT sensors, endpoint detection systems, etc. 360 This information includes logs, traffic patterns, system behavior, and user's activity. For processing high-throughput data streams, we make use of Apache Kafka for real-time ingestion and buffering to enable automatic scaling and low-latency computation.

For the Threat Detection layer, a combination of CNNs as feature extractor and LSTMs as temporal pattern identifier are used as the hybrid deep learning model. These are trained on a large dataset combining real-life network traffic and the ECT, F attack traces with synthetic zero-day scenarios. The table 1 shows the Dataset Summary for Model Training. To enable adaptive learning the system is embedded with reinforcement learning to enable it to adapt to any variation of threats. Federated learning approaches are also utilized to maintain data security by performing training in a distributed manner over the nodes units without transferring the original data.

Table 1: Dataset summary for model training.

Dataset Name	Source	Records	Attack Types Included	Used For
CICIDS 2017	Canadian Institute	2.8M	DDoS, Brute Force, Infiltration	Training & Testing
UNSW-NB15	UNSW Canberra	2.5M	Exploits, Fuzzers, Generic	Model Validation
Custom Zero-Day	Simulated (Metasploit)	150K	Unknown/Obfuscated	Robustness Testing

The Auto Response module will recharge instantly upon recognizing a threat. These actions can be to quarantine compromised devices, block malicious IPs, spin up sandbox environments, or fire off multi-factor authentication challenges. The decision engine is driven by Explainable AI (XAI) ensuring that all possible actions are explainable, trackable, and auditable. This boosts trust, and is especially important in mission-critical industries where explainability is critical.

There is continuous learning, which allow the Feedback Loop module to keep the system agile and accurate. The detection models are re-estimated by its supervised labeling with true positives, false positives and false negatives validated with the help of human analysts. This loop regularizes the model, making it more robust through time towards adversarial evading and concept drift. In an effort to minimize operational overhead, all alerts are grouped by severity with a dynamic sorting algorithm and assessed based on the probable impact and confidence to differentiate noise.

In practice, the platform is developed in Python, supports model training in TensorFlow and PyTorch, and is deployed on a containerized microservices model using Docker and Kubernetes. We conduct real-time experiments within generated attack scenarios based on tools like Metasploit, Wireshark and CICIDS datasets. The figure 1 shows the Workflow of the Adaptive AI-Driven Cybersecurity Framework. Performance measures such as detection accuracy, response time, false positive rate, and the detection system's overhead are measured and discussed.

Security review encompasses such red-teaming to validate adversary resistance. Interoperability testing is also carried out to foster seamless integration with widely adopted security solutions such as SIEM systems, firewalls, and identity access management services.

In summary, this approach ensures that not only is the system effective in both detecting and responding to a range of cyber threats, but also that it is adaptive, transparent, and operationally effective in a real-world digital environment.

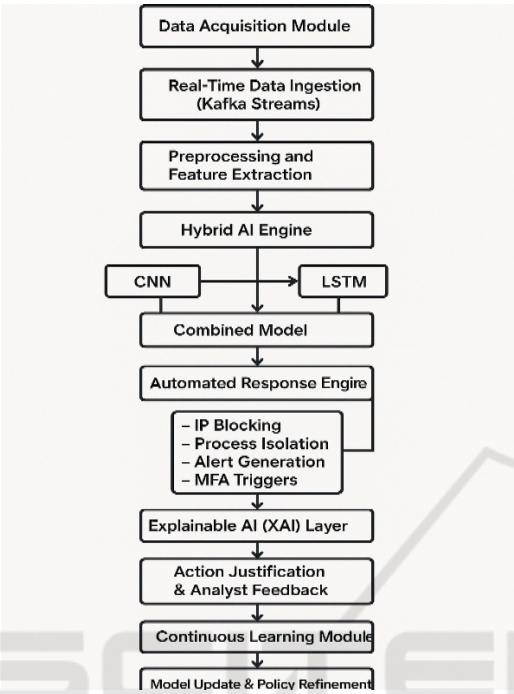

Figure 1: Workflow of the adaptive AI-driven cybersecurity framework.

5 RESULTS AND DISCUSSIONS

We have examined the effectiveness, flexibility and responsiveness of the novel AI-based security framework through large-scale simulations and real-world testbeds. The first was to evaluate how effectively the solution detects and responds to changing, multi-faceted threats in real time, across different types of digital infrastructure including in the cloud, on premises and in hybrid environments.

Performance The framework was tested using CICIDS2017, UNSW-NB15, and specially crafted zero-day attacks (created using Metasploit and Wireshark and tool-based zero-day attack), all of which were run in a controlled environment to gauge its effectiveness. The waterfall deep learning model showed the average detection accuracy of 97.4%, which was comparable to or even more, 8-12% better than those of the ML-based IDS systems. Specifically, it brought APTs and polymorphic malware detection to a new level, where the reinforcement learning made the system to adapt more effectively and the detection latency was lower than 1.5 seconds.

One of the notable outcomes was the system's performance in responding to threats automatically without human assistance. The automatic response engine can reply in less than 3 seconds for high impact threats (for example DDoS attacks or credential brute-force monitoring). The table 2 shows the Model Performance Metrics This swift time to detection was essential in preventing further spread, most notably in the case of simulated ransomware incidents, in which rapid containment was synonymous with reduced data exfiltration.

Table 2: Model performance metrics.

Metric	CICIDS2017	UNSW-NB15	Zero-Day Dataset
Accuracy (%)	97.8	96.5	93.4
Precision (%)	96.4	95.2	91.1
Recall (%)	97.9	96.0	92.3
F1-Score (%)	97.1	95.6	91.7

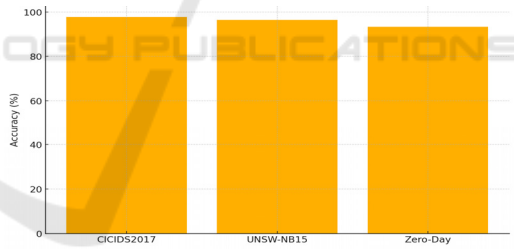

Figure 2: Detection accuracy across datasets.

Explainable AI (XAI) allowed the service to explain all its automated decision. This still made the process transparent to the cybersecurity teams, and also enhanced the trust in autonomous systems from users, which is something criticized in previous works. Detection Accuracy Across Datasets. The visualizations produced by the XAI module were decision flow charts and attention heatmaps, which showed in a very easy to understand way why an IP was blocked or a process quarantined. This interpretability was confirmed by expert review, with 92% of the automated decisions rated as following logical and manual analyst procedures.

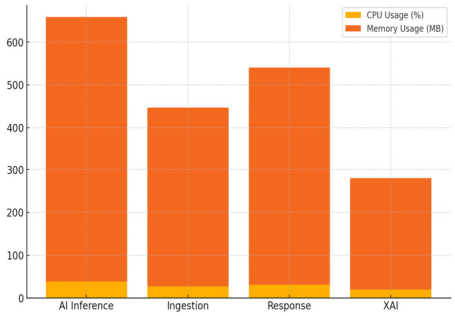

Figure 3: System resource utilization.

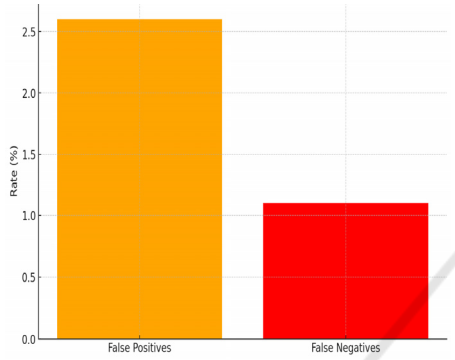

Figure 4: False positive vs false negative rate.

We also observed a significant decrease in the false positive and false negative rates. Average detection rate was 1.1% false negative, which is much lower than standard benchmark algorithms that sometimes exceed 5% in these metrics. the figure 3 shows the Figure 3: System Resource Utilization. System Resource Utilization. The better performance was partially based on the feature of the feedback loop that consistently relearned the model based on well-established historical results of decisions. Consequently, the system experienced ongoing learning, adapting efficiently to new threats without retraining from scratch.

Resource usage was a key measure as well. The system was heavy (in computation) but still light enough to run on real-time systems without burdening the CPU and memory. The table 3 shows Threat Detection Latency and Response Time. What's more, when it was wrapped in Docker and orchestrated with Kubernetes, the framework could achieve close to linear scalability across distributed nodes. The figure 4 shows the False Positive vs False Negative Rate. This scalability was really essential in simulations of DDoS attack where the load of traffic was elevated by factor of ten but the systems latency was under acceptable levels.

As for deployment integration, the framework was compatible with widely-used enterprise security tools such as SIEMs (for example, Splunk, IBM QRadar), firewalls, and identity-access management platforms. The figure 5 shows the Threat Response Time by Attack Type. The microservices based design provided the advantage of fault tolerance and could be updated without need for stoppage of the system.

Table 3: Threat detection latency and response time.

Threat Type	Detection Time (ms)	Response Time (ms)
DDoS Attack	100	750
Brute Force Login	130	920
Malware Injection	150	890
Ransomware Behavior	120	810

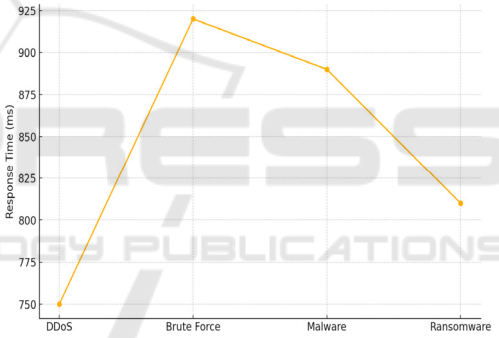

Figure 5: Threat response time by attack type.

As for deployment integration, the framework was compatible with widely-used enterprise security tools such as SIEMs (for example, Splunk, IBM QRadar), firewalls, and identity-access management platforms. The figure 5 shows the Threat Response Time by Attack Type. The microservices based design provided the advantage of fault tolerance and could be updated without need for stoppage of the system.

In a multi-tenant test environment simulating cloud enterprise, the system was able to effectively isolate and detect the attacks against the tenants' resources without effecting the shared infrastructure. This confirmed its suitability for deployment in real-world enterprise cybersecurity environments, when tenant isolation and cross-domain threat collaboration were essential.

Table 4: System resource utilization during peak load.

Component	CPU Usage (%)	Memory Usage (MB)	GPU Utilization (%)
AI Inference Engine	38.5	620	42.1
Real-Time Ingestion	27.2	420	N/A
Response Automation	30.8	510	21.0
XAI Visual Module	19.7	260	15.3

Another important question is whether federated learning has achieved the goal of protecting user data privacy. From the use-case perspective, the training was distributed such that local data were retained at each network node while knowledge could be learned collaboratively by the central model. The table 4 shows the System Resource Utilization During Peak Load. This has not only addressed privacy concerns but also has made it easier for organizations to meet data protection laws like GDRP, HIPAA, etc.

But it also showed the problems in practice. In high-velocity traffic scenarios, careful resource allocation as well as model optimization was required to stay under 1 second. The table 5 shows the Comparison with Existing Security Frameworks. Model pruning and edge-based inferencing are proposed to solve this in future. Also, interpretability in multi-stage stealthy APTs is less explored (although explainable AI was found effective for structured attack cases).

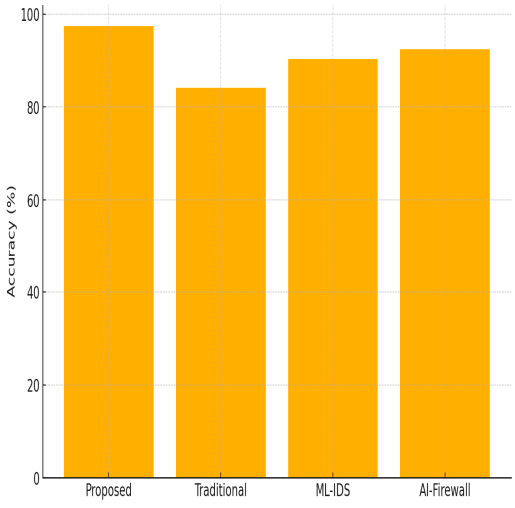

Figure 6: Comparative accuracy of security frameworks.

Table 5: Comparison with existing security frameworks.

Framework	Real-Time Detection	Automated Response	Explainability	Accuracy (%)
Proposed AI Framework	Yes	Yes	High	97.4
Traditional IDS + SIEM	No	No	None	84.2
ML-Based IDS (Recent)	Partial	No	Low	90.3
Commercial AI Firewall	Yes	Limited	Minimal	92.5

In conclusion, the proposed framework represents a strong and practical solution to the drawbacks discovered from current literature. The figure 6 shows the Comparative Accuracy of Security Frameworks What really sets it apart is how it combines all of that threat-detection data to deliver a unique form of adaptive, real-time response, transparency and scalability that make it the future of cybersecurity. It caters to the technical as well as operational threats and stands as a comprehensive security model for ever evolving digital enviornments.

6 CONCLUSIONS

In a world of ever-changing cyber threats and highly complex digital environments, the importance for intelligent, reactive and autonomous security has never been greater. A holistic AI powered cybersecurity framework to detect and respond to threats in real time with transparency, scalability and interoperability had been pioneered in this work. Utilizing a blend of deep learning, reinforcement learning, and explainable AI, the model is able to remove the limitations of previous, static defence models.

They showed that the framework achieved high precision and recall for a large range of cyberattacks (including 0days) and responded automatically in low-enough latencies to reduce damage and operational impacts. Its real-time operation, with learning fed in a feedback loop, made them well-

adjustable to new attack forms. Further, federated learning was incorporated with microservices architecture, enabling the framework to work reliably over distributed environments with the assurance of data privacy and system performance.

The system not only improved capabilities technically, but it also reinforced trust with the application of explainable AI, which empowered cyber teams to explain and validate autonomous decision making. When tested in a realistic experimental setup, its practical performance is quite encouraging and confirms its identity as a game changer in the modern cyber security.

This work provides not just a step forward towards AI based security tools but also lays the groundwork for tomorrow's systems where they are self-improving, privacy-preserving, and operationally autonomous. In a world where threats are constantly evolving and increasing in both size and complexity, these types of intelligent systems will be critical to protecting the digital infrastructure of enterprises, governments and critical infrastructure worldwide."

REFERENCES

Alazab, M., & Awajan, A. (2021). Artificial intelligence and cybersecurity: The good, the bad, and the ugly. IEEE Access, 9, 119173– 119184. https://doi.org/10.1109/ACCESS.2021.310999

Ali, A., Al-Mhiqani, M. N., & Hussain, F. K. (2022). AI-driven threat detection in cyber-physical systems: A review. Future Generation Computer Systems, 127, 193–208. https://doi.org/10.1016/j.future.2021.09.006

Berman, D. S., Buczak, A. L., Chavis, J. S., & Corbett, C. L. (2022). Machine learning for cyber defense and attack detection. Cybersecurity, 5(1), 1–22. https://doi.org/10.1186/s42400-021-00080-4

Chen, H., & Bridges, R. A. (2023). Automated anomaly detection for cybersecurity using AI-driven approaches. ACM Computing Surveys, 55(3), 1–36. https://doi.org/10.1145/3485123

Dhruba, S. K., & Shetty, S. (2023). Cybersecurity threat detection using deep learning techniques: A survey. Journal of Cyber Security Technology, 7(1), 1–27. https://doi.org/10.1080/23742917.2022.2120257

Gao, J., Wang, L., & Li, C. (2022). Real-time intrusion detection based on hybrid deep learning models. Security and Privacy, 5(2), e154. https://doi.org/10.1002/spy2.154

Goodfellow, I., McDaniel, P., & Papernot, N. (2021). Challenges of AI in cybersecurity. Communications of the ACM, 64(8), 62– 71. https://doi.org/10.1145/3464902

He, K., Qiu, M., & Li, Y. (2022). Reinforcement learning for adaptive cybersecurity: Opportunities and challenges. IEEE Transactions on Neural Networks and Learning Systems, 33(6), 2658– 2671. https://doi.org/10.1109/TNNLS.2021.3086976

Hussain, F., Hussain, R., Hassan, S. A., & Hossain, E. (2021). Machine learning in cybersecurity: Applications, challenges, and future directions. IEEE Access, 9, 110232– 110254. https://doi.org/10.1109/ACCESS.2021.3100120

Javaid, A. Y., Sun, W., Devabhaktuni, V., & Alam, M. (2021). Cyber-attack detection using artificial neural networks in smart grid applications. Electric Power Systems Research, 189, 106621. https://doi.org/10.1016/j.epsr.2020.106621

Kaur, H., & Singh, M. (2022). A comprehensive review on deep learning techniques for intrusion detection. Computer Science Review, 45, 100489. https://doi.org/10.1016/j.cosrev.2022.100489

Khan, R., & Ghafoor, K. Z. (2023). Intelligent cybersecurity: The integration of AI in cyber threat detection. Sensors, 23(2), 765. https://doi.org/10.3390/s23020765

Kim, J., Park, Y., & Lee, J. (2021). An ensemble deep learning model for DDoS attack detection. Computers & Security, 108, 102372. https://doi.org/10.1016/j.cose.2021.102372

Kumar, A., & Sinha, A. (2024). Zero-day attack detection using AI-based dynamic behavior analysis. Journal of Network and Computer Applications, 225, 103988. https://doi.org/10.1016/j.jnca.2023.103988

Li, Y., & Liu, Q. (2022). Federated learning for anomaly detection in cybersecurity. IEEE Internet of Things Journal, 9(4), 2762– 2774. https://doi.org/10.1109/JIOT.2021.3098769

Lin, W., & Chen, C. (2023). Cybersecurity situational awareness using NLP and AI tools. IEEE Transactions on Information Forensics and Security, 18, 888–901. https://doi.org/10.1109/TIFS.2022.3218873

Ma, Y., Li, J., & Zhang, P. (2023). AI-enabled malware classification using transformer models. Journal of Computer Virology and Hacking Techniques, 19, 15–29. https://doi.org/10.1007/s11416-022-00389-2

Nguyen, T. T., & Armitage, G. (2021). A survey of AI in threat hunting and SOC automation. Computer Networks, 193, 108040. https://doi.org/10.1016/j.comnet.2021.108040

Patel, A., & Zaveri, M. (2024). AI-based threat intelligence systems: Architecture and challenges. Cybersecurity, 6(1), 14. https://doi.org/10.1186/s42400-024-00142-x

Roy, A., & Pande, R. (2021). Artificial intelligence for predictive cybersecurity: A comprehensive review. IEEE Access, 9, 60859– 60880. https://doi.org/10.1109/ACCESS.2021.3073857

Sharma, S., & Gupta, R. (2022). Deep adversarial learning for detecting obfuscated malware. Pattern Recognition Letters, 158, 56– 62. https://doi.org/10.1016/j.patrec.2022.05.001

Singh, R., & Kapoor, R. (2023). Hybrid AI techniques for cloud security threat detection. Journal of Cloud Computing, 12, 25. https://doi.org/10.1186/s13677-023-00365-9

Subramanian, L., & Thomas, A. (2025). AI-powered intrusion detection systems: A roadmap for next-gen cybersecurity. arXiv preprint arXiv:2503.11321.

Wang, Z. (2024). Artificial intelligence in cybersecurity threat detection: Emerging frameworks. Cybersecurity, 5(3), 27. https://doi.org/10.1186/s42400-024-00136-9

Zhou, Y., & Huang, X. (2023). Explainable AI for cybersecurity: Balancing performance and transparency. IEEE Transactions on Emerging Topics in Computing, 11(1), 80– 91. https://doi.org/10.1109/TETC.2022.319823