iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: II Month of publication: February 2026

DOI: https://doi.org/10.22214/ijraset.2026.77572

www.ijraset.com

Call: ☎ 08813907089 | E-mail ID: ijraset@gmail.com

Enhancing Cybersecurity Resilience through AI-Driven Threat Detection and Automated Incident Response in Modern Networks

Putha Sateesh Kumar[1], Dr. Akash Saxena[2]
[2]*Professor and Supervisor, Department of Computer Science, Shridhar University, Pilani*

Abstract: The rapid evolution of cyber threats, including advanced persistent threats (APTs), ransomware campaigns, phishing attacks, insider threats, and zero-day exploits, has significantly challenged conventional cybersecurity mechanisms. Traditional security frameworks primarily rely on signature-based detection, static rule sets, and manual incident response processes, which are increasingly inadequate against sophisticated and adaptive adversaries. As modern networks become more complex due to cloud computing, Internet of Things (IoT), edge computing, and large-scale digital transformation, there is an urgent need for intelligent, scalable, and automated cybersecurity solutions. This study explores the integration of Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) techniques into contemporary cybersecurity architectures to enhance proactive threat detection and automated incident response capabilities. AI-driven threat intelligence systems leverage behavioral analytics, anomaly detection models, predictive analytics, and real-time data processing to identify malicious activities before they escalate into critical security breaches. Supervised, unsupervised, and reinforcement learning approaches are examined for their effectiveness in detecting both known and unknown attack patterns. Furthermore, the research highlights the role of Security Orchestration, Automation, and Response (SOAR) platforms in minimizing response time, reducing human error, and improving operational efficiency. Automated incident response frameworks enable rapid containment, threat isolation, system recovery, and continuous monitoring without heavy reliance on manual intervention. A comparative analysis between traditional and AI-powered cybersecurity models demonstrates substantial improvements in detection accuracy, scalability, adaptability, and resilience. The findings suggest that AI-enhanced cybersecurity systems not only strengthen real-time network protection but also contribute to predictive defense strategies capable of mitigating emerging and zero-day threats. While challenges such as adversarial attacks, data quality issues, computational overhead, and explainability remain, AI-driven security architectures represent a transformative approach toward building resilient, intelligent, and self-adaptive cyber defense ecosystems for modern digital infrastructures.

Keywords: Cybersecurity, Artificial Intelligence, Threat Detection, Automated Incident Response, Machine Learning, Deep Learning, Network Security.

I. INTRODUCTION

The rapid digitization of global infrastructures has significantly transformed the technological landscape, enabling organizations to operate through interconnected systems, cloud platforms, Internet of Things (IoT) devices, and distributed enterprise networks. While this digital transformation has improved efficiency and scalability, it has simultaneously expanded the attack surface, making modern networks increasingly vulnerable to sophisticated cyber threats. Cybercriminals now employ advanced techniques such as Advanced Persistent Threats (APTs), ransomware-as-a-service (RaaS), polymorphic malware, insider attacks, and zero-day exploits, which are capable of bypassing traditional security mechanisms.

Conventional cybersecurity approaches primarily depend on signature-based detection systems, static rule configurations, and manual incident response processes. Although these mechanisms are effective against known threats, they lack the adaptability required to detect novel, evolving, and stealthy attack patterns. The dynamic nature of cyberattacks demands intelligent systems capable of learning from historical data, identifying behavioral anomalies, and responding autonomously in real time.

Artificial Intelligence (AI) has emerged as a transformative force in cybersecurity by introducing data-driven, adaptive, and predictive defense capabilities. Machine Learning (ML) algorithms analyze vast volumes of network traffic, system logs, and user behavior patterns to detect irregular activities that may indicate potential breaches.

Deep Learning (DL) models, including Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), enhance anomaly detection by identifying complex patterns that are difficult to detect through rule- based systems. Furthermore, reinforcement learning techniques enable adaptive response strategies that evolve alongside emerging threats.

Modern cybersecurity architectures increasingly integrate AI with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms to facilitate real-time threat intelligence, automated alert correlation, and rapid incident containment. By combining intelligent detection with automated remediation, organizations can significantly reduce response times, minimize operational disruptions, and improve overall cyber resilience.

This paper aims to examine the role of AI-driven threat detection and automated incident response in strengthening cybersecurity resilience within modern networks. It evaluates existing AI methodologies, compares them with traditional security frameworks, and identifies key challenges and research directions necessary for developing robust, scalable, and self- adaptive cybersecurity systems.

II. LITERATURE REVIEW

AI-powered cybersecurity solutions have attracted considerable interest, with researchers investigating machine learning (ML) and deep learning (DL) methods for identifying threats and automating responses.

A. AI-Driven Threat Identification

Traditional threat detection mechanisms rely heavily on signature-based and rule-based systems that are effective only against previously identified attack patterns. However, with the emergence of polymorphic malware, zero-day exploits, and Advanced Persistent Threats (APTs), static detection techniques have become insufficient. Researchers have increasingly explored Artificial Intelligence (AI) and Machine Learning (ML) techniques to overcome these limitations by enabling adaptive and intelligent threat detection systems. Recent studies demonstrate that supervised learning algorithms such as Support Vector Machines (SVM), Decision Trees, Random Forests, and Gradient Boosting significantly improve intrusion detection accuracy when trained on labeled datasets. Wang et al. (2020) reported that ML-based intrusion detection systems (IDS) outperform traditional signature-based IDS in detecting both known and variant attacks. Similarly, Kumar et al. (2021) emphasized the effectiveness of Deep Learning (DL) models in handling high-dimensional and large-scale network traffic data.

Unsupervised learning techniques, including clustering (e.g., K-Means, DBSCAN) and anomaly detection models, have gained attention for identifying unknown threats without prior labeling. These methods detect deviations from normal behavioral patterns in network traffic, user activity, or system logs, making them highly effective against zero-day attacks. Furthermore, Deep Learning architectures such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) enhance detection capabilities by automatically extracting complex features from raw data. CNNs are particularly effective in traffic classification, while RNNs and Long Short-Term Memory (LSTM) networks capture temporal dependencies in sequential network events.

In addition, emerging research explores hybrid AI models that combine supervised and unsupervised learning for improved detection performance. Behavioral analytics powered by AI also enables User and Entity Behavior Analytics (UEBA), which helps identify insider threats and compromised accounts. Overall, AI-driven threat identification systems provide proactive, adaptive, and scalable solutions that significantly enhance detection precision and reduce false positives compared to traditional methods.

B. Automated Incident Management in Cybersecurity

Manual incident response processes are often slow, resource-intensive, and prone to human error, particularly in large-scale enterprise environments with thousands of daily security alerts. As cyber threats become more frequent and sophisticated, organizations require automated and intelligent incident management systems capable of responding in real-time. AI-driven automated incident management integrates Machine Learning, orchestration tools, and intelligent decision-making mechanisms to streamline the detection-to-response lifecycle. Zhang et al. (2019) proposed an AI-based automated incident response framework that reduced response time by approximately 40% compared to traditional manual methods. Security Orchestration, Automation, and Response (SOAR) platforms play a critical role in this process by integrating threat intelligence feeds, Security Information and Event Management (SIEM) systems, and endpoint detection tools. AI algorithms analyze alerts, prioritize incidents based on severity, and automatically trigger predefined response actions such as isolating compromised devices, blocking malicious IP addresses, resetting credentials, or quarantining infected systems.

Reinforcement learning has also been applied to develop adaptive response mechanisms. These systems learn optimal countermeasures by continuously interacting with the network environment and evaluating the effectiveness of previous responses.

Over time, the system improves its decision-making capabilities, enabling dynamic and context-aware mitigation strategies. Additionally, Natural Language Processing (NLP) techniques are being used to analyze threat intelligence reports, automate ticket classification, and assist in forensic investigations.

Automated incident management not only reduces mean time to detect (MTTD) and mean time to respond (MTTR) but also improves operational efficiency and scalability. By minimizing manual intervention, organizations can allocate cybersecurity professionals to strategic tasks such as threat hunting and security architecture enhancement. Despite challenges related to model explainability and trust, AI-powered incident management systems represent a significant advancement toward autonomous and resilient cybersecurity ecosystems.

Table 1: Comparison of Traditional vs. AI-Powered Cybersecurity Solutions

Feature	Traditional Cybersecurity	AI-Driven Cybersecurity
Threat Detection	Rule-based, Signature- dependent	Adaptive ML-based models
Response Time	Manual, slow	Automated, real-time
Accuracy	Moderate	High (ML/DL-enhanced
Zero-Day Threat	Limited	Proactive AI-based
Scalability	Redource-intensive	Highly scalable

C. AI-Driven Threat Detection Framework

AI-driven threat detection systems utilize machine learning, deep learning, and statistical techniques to pinpoint harmful activities in real-time.

1) Machine Learning for Intrusion Detection

ML algorithms scrutinize network traffic records, user actions, and system operations to uncover irregularities that suggest security violations. Supervised learning techniques, such as decision trees, support vector machines (SVMs), and gradient boosting, have shown exceptional precision in detecting intrusions.

2) Deep Learning for Network Security

Deep learning architectures, including CNNs and RNNs, are capable of analyzing extensive network data and uncovering concealed attack patterns. AI-enhanced security frameworks continually adapt by learning from emerging threats, rendering them more efficient than traditional rule-based systems.

D. Automated Incident Response Strategies

AI-driven threat detection systems utilize machine learning, deep learning, and statistical techniques to pinpoint harmful activities in real-time.

1) Machine Learning for Intrusion Detection

ML algorithms scrutinize network traffic records, user actions, and system operations to uncover irregularities that suggest security violations. Supervised learning techniques, such as decision trees, support vector machines (SVMs), and gradient boosting, have shown exceptional precision in detecting intrusions.

2) Deep Learning for Network Security

Deep learning architectures, including CNNs and RNNs, are capable of analyzing extensive network data and uncovering concealed attack patterns. AI-enhanced security frameworks continually adapt by learning from emerging threats, rendering them more efficient than traditional rule-based systems.

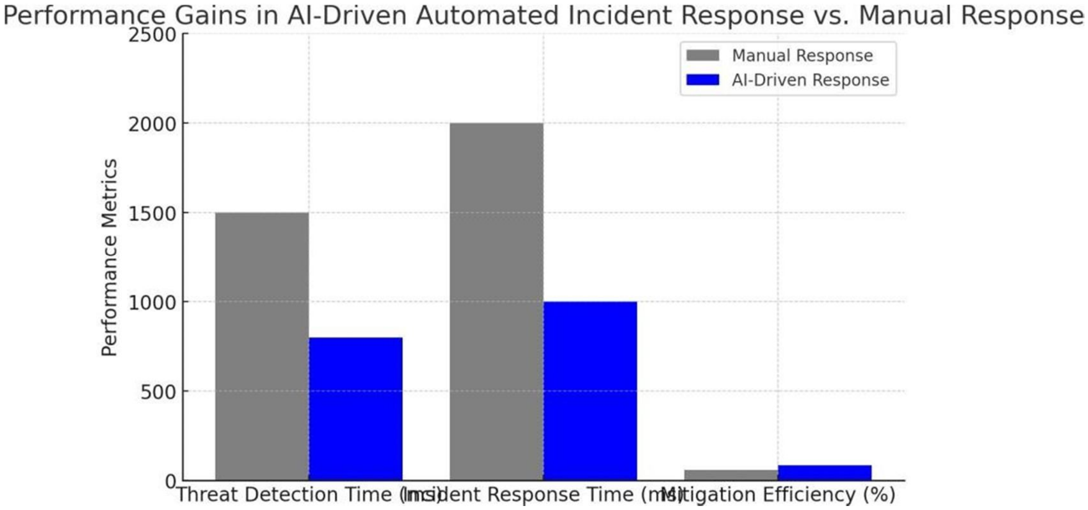


Figure 1: Performance Gains in AI-Driven Automated Incident Response vs. Manual Response

3) Challenges and Future Research Directions Difficulties with AI-Powered Cybersecurity

AI-based cybersecurity systems have a number of drawbacks despite their benefits:

- Problems with Data Quality: For AI models to produce precise predictions, high-quality datasets are necessary.
- Adversarial Attacks: False data can be introduced by attackers to manipulate AI models.
- Computational Overhead: AI-powered security solutions require a large amount of processing power.

4) Prospective Research Paths

- AI-Powered Blockchain Security for Decentralized Threat Detection
- Federated Learning for Secure AI Model Training
- Hybrid AI Models for Better Threat Classification

III. CONCLUSION

AI-powered cybersecurity solutions improve overall network security resilience, speed up response times, and improve threat detection. Modern cybersecurity frameworks can proactively counter evolving threats by combining deep learning, machine learning, and automated response mechanisms. To improve cyber defenses, future research should concentrate on hybrid security models, adversarial AI defense, and federated learning.

REFERENCES

[1] Wang, J., et al. (2020). Machine Learning-Based Intrusion Detection Systems: A Review. IEEE Access

[2] Kumar, R., et al. (2021). Deep Learning Approaches for Cyber Threat Detection. Journal of Network Security.

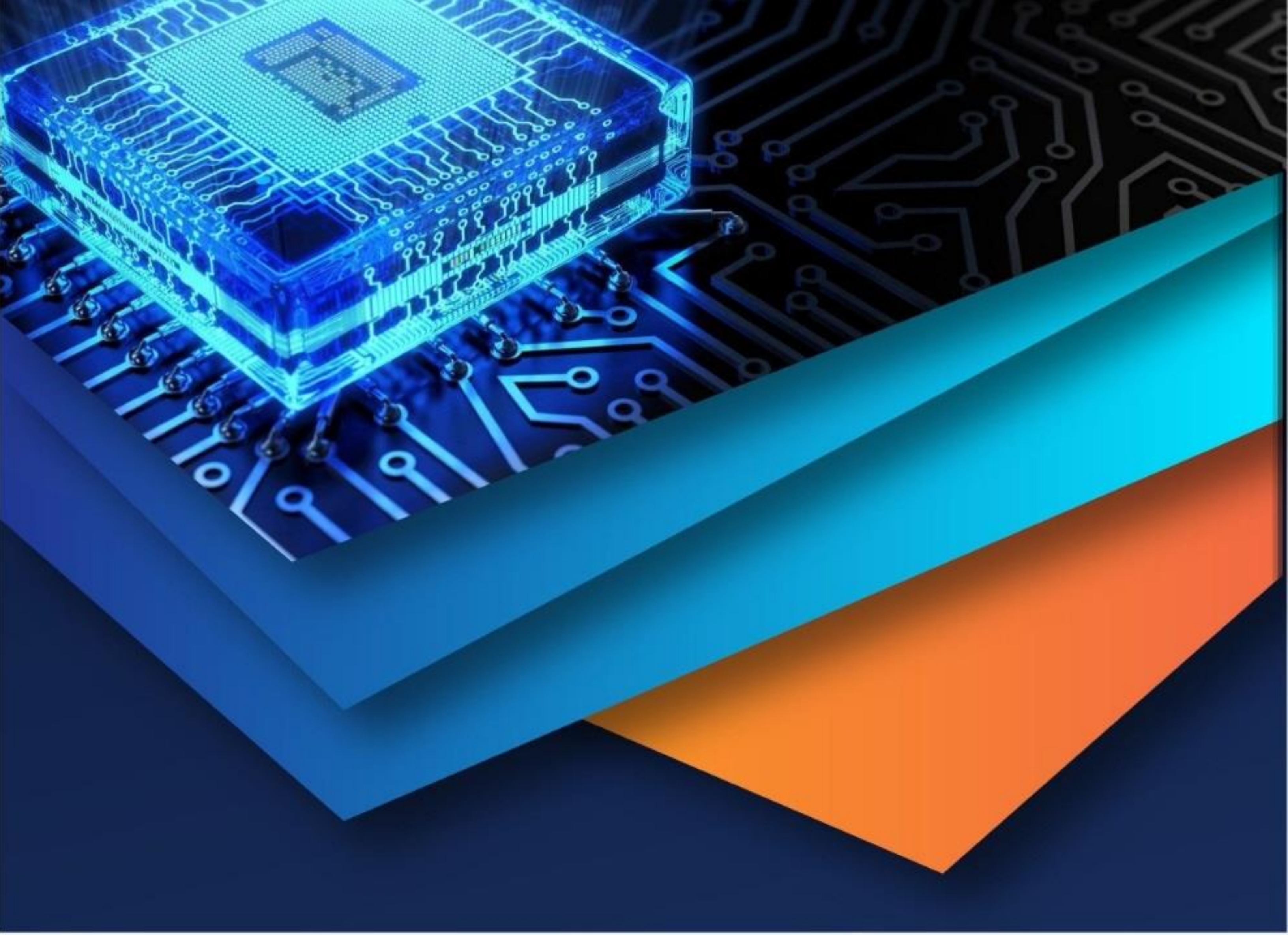
[3] Zhang, Y., et al. (2019). AI-Driven Automated Incident Response in Cybersecurity. ACM Digital Library.

[4] Sommer, R., & Paxson, V. (2010). Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy.

[5] ENISA (2023). Threat Landscape Report. European Union Agency for Cybersecurity.

[6] IBM Security (2023). Cost of a Data Breach Report.

[7] NIST (2022). Cybersecurity Framework (CSF 2.0 Draft).



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429