International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 10 October 2025
Page No: 3900-3905
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0568

AI Enhanced Cyber Triggered Threat Detection and Prevention using Deep Learning

Srihari K V[1], Srinivasa M[2], Suhas Patil[3], Sumanth T J[4], Dr. Nirmala S[5]
[1,2,3,4]Student, Dept. of Computer Science and Engineering AMC Engineering College Bengaluru, India
[5]Professor, Dept. of Computer Science and Engineering AMC Engineering College Bengaluru, India
Email ID: *srihari8944559@gmail.com[1], sinus9614@gmail.com[2], suhasspatil2004@gmail.com[3], sumanthtj123@gmail.com[4], drnirmala.sundaram@amceducation.in[5]*

Abstract
The complexity and regularity of cyberthreats have made the adoption of proactive and intelligent defence mechanisms necessary in the ever-changing field of cybersecurity. This paper presents an AI-enhanced framework for cyber threat detection and prevention applying methods from deep learning. The suggested system makes use of recurrent neural networks (RNNs), convolutional neural networks (CNNs), and autoencoders to look at network traffic, system logs, and behavioural patterns in real-time, enabling accurate threat identification with minimal false positives. The model incorporates anomaly detection, automated incident classification, and adaptive response strategies that improve over time via reinforcement learning. Furthermore, the system facilitates rapid recovery from attacks by isolating affected components and restoring data using predictive backup management. Experimental results demonstrate improved threat response times, increased detection accuracy, and robust recovery from both known and novel cyberattacks. This approach aims to move cybersecurity from a reactive to a proactive model, enhancing the resilience and autonomy of digital infrastructures.

Keywords: *Cybersecurity, Artificial Intelligence, Deep Learning, Threat Recovery, Threat Detection, Incident Response, Reinforcement learning, unsupervised learning, and supervised learning, Cyber Defence Systems, Automated Recovery, Anomaly Detection.*

1. Introduction

1.1. Overview

Cybersecurity is essential in today's digital world since malicious activity could jeopardize private information, disrupt services, and seriously damage one's finances and reputation [1]. Conventional defenses like firewalls, antivirus programs, and rule-based intrusion detection systems frequently fail to detect complex and adaptive cyberattacks. In order to automate the whole threat management cycle, from detection to prevention, this project suggests a comprehensive, tracks user behavior and network traffic, identifies irregularities instantly, categorizes possible threats, and launches clever counterattacks. It also includes recovery techniques to return to regular operations and stop future occurrences of the same threats. The system architecture is constructed with deep learning models trained on large datasets [2].

1.2. Objectives

The main objectives of this project are:

- **To develop an AI-driven system** for detecting, responding to, recovering from, and preventing cyber threats using methods from deep learning.
- **To enhance real-time threat detection** through the use of advanced models for deep learning that are able to look for anomalies in system logs, user behaviour, and network traffic.
- **To implement intelligent recovery processes** that can restore systems to a secure state with minimal downtime through

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 10 October 2025
Page No: 3900-3905
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0568

automated rollback and data recovery strategies.

- **To automate threat response mechanisms**, allowing for quick action to minimize damage, isolate impacted systems, and stop malicious activity [3].

1.3. Purpose, Scope, Applicability

1.3.1. Purpose

This project's goal is to create and deploy an AI-enhanced cybersecurity Deep learning-based system methods to offer a clever, automated, and flexible way to identify, address, recover from, and stop cyberthreats. The complexity and frequency of cyberthreats are constantly changing, traditional rule-based systems fall short in providing timely and effective protection. This project aims to bridge that gap by using advanced artificial intelligence to:

- Detect anomalies and threats in real-time with high accuracy.
- Trigger immediate and automated responses to contain attacks [4].
- Enable swift recovery of affected systems with minimal downtime, and
- To stop future attacks, keep learning and adjusting to new threat patterns.

By combining cybersecurity procedures with deep learning models, the project aims to improve the resilience, efficiency, and intelligence of digital defense systems, ensuring better protection for modern organizations and IT infrastructures.

1.3.2. Scope

This project's scope includes the creation and deployment of an all-encompassing, AI-powered cybersecurity system with an emphasis on deep learning-based proactive prevention, automated response, threat detection, and quick recovery [5].

1.3.3. Applicability

The AI-enhanced Cyber Triggered Threat Detection, Recovery, Response, and Deep Learning-based prevention system is highly applicable across a wide range of domains and industries where cybersecurity is critical [6]. Its versatility and adaptability make it suitable for:

- **Enterprise IT Infrastructures:** Enhancing the security of corporate networks, data centres, and internal systems by providing real-time monitoring and intelligent threat response.
- **Financial Institutions:** Protecting sensitive financial data, preventing fraud, and ensuring compliance with strict cybersecurity regulations through predictive finding threats and responding automatically [7].
- **Healthcare Systems:** Safeguarding patient data and medical devices against ransomware, data breaches, and other cyber threats, while ensuring uninterrupted operation of critical services.
- **Educational Institutions:** Protecting academic records, research data, and digital learning platforms from unauthorized access and cyberattacks.
- **Cloud Computing and Data Centres:** Monitoring virtual environments and multi-tenant infrastructures for unusual behavior, ensuring secure cloud operations and data integrity [8].
- **IoT and Smart Devices:** Monitoring and securing connected devices against threats in real time, especially in smart homes, industrial systems, and critical infrastructure.
- **E-commerce and Retail:** Preventing data theft, payment fraud, and service disruptions by analyzing customer behavior and transaction patterns for potential threats

2. Literature Survey

2.1. Introduction

A literature survey (or literature review) involves a systematic examination and evaluation of the existing scholarly resources, such as books, journals, conference papers, and other research materials related to a particular subject or inquiry. The literature review for this study focuses on investigating how Deep Learning (DL) and Artificial Intelligence (AI) are transforming cybersecurity, especially in the domains of real-time threat detection, response, and prevention of cyberattacks.

2.2. Summary of Literature Survey

This literature review's primary objective is to examine how AI and deep learning are transforming cybersecurity, paying special attention to their capacity to identify and prevent cyber threats

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 10 October 2025
Page No: 3900-3905
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0568

dynamically and in real-time. The survey identifies and analyses various models, techniques, and frameworks proposed in recent research that aim to enhance cybersecurity using AI. To investigate how Both artificial intelligence and deep learning are transforming cybersecurity, particularly Regarding identifying, addressing, and thwarting cyberthreats instantly.

2.3. Key Technologies Reviewed

- **AI Methodologies:** The suitability of several learning paradigms for cybersecurity has been investigated, including reinforcement learning, supervised learning, and unsupervised learning.
- **Deep Learning models:** Well-known models such as Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM) networks, Generative Adversarial Networks (GANs), and Artificial Neural Networks (ANN) have been studied because of their ability to depict complex patterns in cybersecurity data.
- **Hybrid Models:** For improved threat detection capabilities, the combination of both deep learning and traditional machine learning techniques, like LSTM or Random Forest + CNN, have been evaluated.
- **AI Frameworks:** The function of frameworks like behaviour analytics, anomaly detection systems, and Security Orchestration, Automation, and Response (SOAR) in dynamic and automated cybersecurity defense has been studied.

2.4. 2.3 Drawbacks

- High computational resources required
- Adversarial attacks and model interpretability issues
- Ethical concerns and data privacy
- Difficulty in integrating AI into legacy systems.

3. Problem Statement

The increasing reliance on digital systems and networks has raised the risk of cyber threats that take advantage of weaknesses in critical infrastructures, businesses, and personal platforms. Traditional cybersecurity methods, like signature-based intrusion detection and rule-driven firewalls, struggle to deal with dynamic, polymorphic, and zero-day attacks. These methods need frequent manual updates, often produce high false-positive rates, and do not have the intelligence to adapt to shifting threat environments. The complexity of cyberthreats is increasing and using AI-driven malware, advanced persistent Ransomware and advanced persistent threats (APTs) make proactive and intelligent security frameworks imperative. Although machine learning detection methods offer some improvements, they frequently struggle with scalability, making quick decisions, and preventing attacks on their own. A significant research gap exists in developing a deep learning-based cybersecurity system enhanced by AI that not only correctly detects threats but also stops them in real time. This system should aim to reduce false alarms and adjust to new attack methods. Solving this issue is important to establish strong, scalable, and intelligent defenses that can protect modern digital environments.

4. Proposed Solution

Beyond the constraints of conventional, rule-based security systems, we offer a unified, AI-enhanced framework for proactive cyber defense. Our AI-based model continuously learns from new attack vectors, which makes it more adaptive and resilient against new threats than traditional systems that depend on predefined rules. Three interconnected phases make up the framework, which offers complete security:

- **AI-Enhanced Detection:** Using deep learning, this stage detects anomalies and malicious activity in real-time with previously unheard-of speed and accuracy. The system can even predict possible threats by identifying trends in historical attack data through the use of predictive analytics. This capability is critical for detecting subtle and previously unknown threats, such as zero-day attacks and polymorphic malware, that traditional systems would miss.
- **Automated Response and Prevention:** Our system starts automated mitigation techniques as soon as a threat is detected in

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 10 October 2025
Page No: 3900-3905
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0568

order to contain the situation and stop additional harm from being done. The system can automatically block suspicious activity or remove compromised devices from the network by utilizing AI-driven tools. This proactive strategy reduces possible harm by enabling early detection and prompt action.

- **Recovery:** Our framework's recovery phase assists in reducing risks and reestablishing normalcy in the immediate aftermath of a security incident. By collecting and arranging logs in real-time, the system can be set up to start automated backups, perform data integrity checks, and expedite the documentation process. After an incident, this capability guarantees a speedier return to a secure and functional state.

5. Methodology

- **Data Collection:** Numerous sources, such as malware databases, intrusion detection systems, network logs, and open-source cybersecurity datasets, will be used to collect cyber threat intelligence.
- **Data Preprocessing:** Data will be cleaned and structured, ensuring consistency and removing redundancies. Techniques such as feature extraction, normalization, and labeling will be applied to improve model accuracy.
- **Model Development:** We will create and train a range of deep learning models, including Convolutional Neural Networks (CNNs) for image-based threat detection, Recurrent Neural Networks (RNNs) for sequential data analysis, and Transformer models for sophisticated anomaly detection.
- **Real-time Detection:** AI-driven monitoring mechanisms will analyze network traffic and system logs in real time to identify threats based on behavioral patterns and anomalies.
- **Response and Recovery:** Automated response strategies will be implemented using reinforcement learning and rule-based decision systems, allowing the system to take immediate action in case of detected threats.
- **Prevention Mechanism:** The system will use predictive analytics to anticipate potential threats and proactively strengthen security defenses.
- **Testing and Deployment:** The system will be tested in a controlled environment using real- world cyberattacks and scenarios to evaluate its efficiency before deployment.

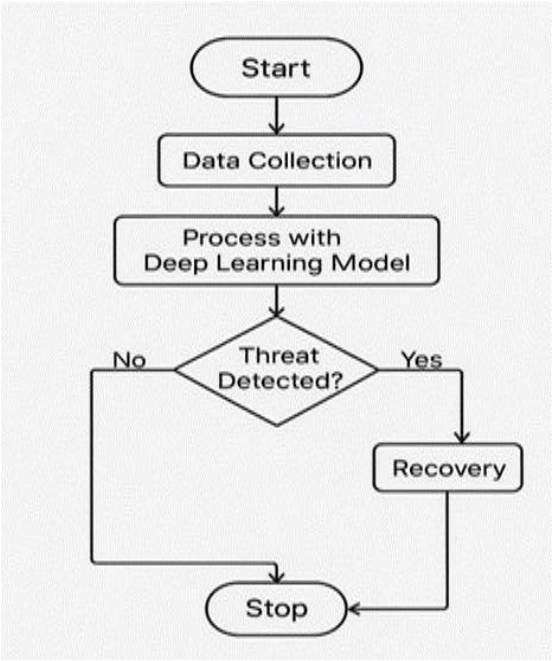

Figure 1 Flow Chart Describing the Data Collection Process

6. Working

Figure 1 above shows the operational workflow of an AI-driven cybersecurity system that detectsand recovers threats using deep learning techniques. By turning on the system, the Start point initiates the process. System logs, network traffic, and user activity are just a few of the sources from which data is gathered for analysis in the first step. This information is fed into the deep learning model. Next, A Deep Learning Model processes the data that has been gathered. This model analyzes the data to identify any anomalies, suspicious patterns, or known threat signatures that may indicate a cyber-attack or security breach. Following the data processing phase, the system evaluates whether a threat is detected. This decision point leads to two possible paths:

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 10 October 2025
Page No: 3900-3905
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0568

- If no threat is detected, the system proceeds to stop the process, indicating that no malicious activity was found during the analysis.
- If a threat is detected, the system transitions to the Recovery phase. In this phase, appropriate recovery actions are initiated to mitigate the impact of the detected threat, restore normal system operations, and prevent further damage.

Finally, after completing either the normal stopping procedure or the recovery process, the system reaches the Stop point, marking the end of that particular cycle of operation. This flow chart represents a streamlined and automated approach to cybersecurity, where deep learning is essential to guaranteeing the prompt identification and efficient handling of possible cyberthreats.

7. Result

Standard cybersecurity datasets were used to assess the AI-Enhanced Cyber Triggered Threat Detection and Prevention system. High detection accuracy was attained by the deep learning models in a number of threat categories:

- The system will immediately analyze the data when you upload a CSV file containing network traffic. It will clearly display "Analysis complete" for benign traffic. "No threats detected" alert. It will display real-time alerts for every threat found in malicious traffic.
- Every red alert will have a "Prevention Action" badge on the web interface's "Live Analysis" section. This will display a simulated action, like "Isolated host" or "Blocked IP address." The system's proactive action to prevent the threat from spreading is validated by this visual feedback.
- Additionally, a "Recovery Action" badge will be displayed on the alerts. This mimics the automated procedures used to repair the damage. "Initiated system rollback" and "Scanned for malware remnants" are two examples. This demonstrates that the system can assist a network in recovering from attacks in addition to defending against them.

Conclusion

This project offers a thorough AI-driven framework for addressing current cybersecurity challenges through deep learning techniques. Traditional approaches often fail to detect and respond to evolving cyberthreats in real time due to their static nature and lack of flexibility. By integrating models such as CNNs, LSTMs, and GANs with intelligent automation, this system enables real-time anomaly detection, rapid response, efficient recovery, and proactive prevention. The solution demonstrates improved accuracy, adaptability, and resilience compared to conventional approaches. Through effective data preprocessing, behavioural analysis, and reinforcement-based decision-making, the system showcases the potential to minimize human intervention and protect critical digital infrastructure. Overall, the project successfully validates the feasibility of deploying AI-enhanced cybersecurity solutions in dynamic and threat-prone environments.

Future Scope

The proposed system lays the foundation for several advancements and enhancements in the domain of cybersecurity:

- **Integration with Blockchain:** Future versions could incorporate blockchain to ensure secure, tamper-proof data logging and transparent threat auditing.
- **Zero-Day Threat Detection:** Expanding training datasets and leveraging unsupervised and semi-supervised learning can improve detection of zero-day attacks.
- **Cloud and Edge Deployment:** Optimizing the system for lightweight deployment at the edge or in cloud environments can extend its applicability to IoT and real-time systems.
- **Explainable AI (XAI):** Introducing explainability mechanisms can improve model transparency and help security professionals understand and trust AI decisions.
- **User Behaviour Profiling:** Enhancing user behaviour analytics can enable personalized threat modelling and insider threat detection.
- **Adversarial Robustness:** Further work can focus on strengthening the models against

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 03 Issue: 10 October 2025
Page No: 3900-3905
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2025.0568

adversarial attacks to make the system more secure.

- **Global Threat Intelligence Sharing:** Future implementations may support federated learning and collaborative models that share anonymized threat patterns across organizations without compromising data privacy.

References

[1]. Alevizos, L., & Dekker, M. (2024). Towards an AI-Enhanced Cyber Threat Intelligence Processing Pipeline. Electronics, 13(11), 2021. https://doi.org/10.3390/electronics13112021

[2]. Arif, H., Kumar, A., Fahad, M., & Hussain, H. K. (2024). Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research. International Journal of Multidisciplinary Sciences and Arts, 2(2), 242–251. https://doi.org/10.47709/ijmdsa.v2i2.3452

[3]. Chahal, S. (2023). AI-Enhanced Cyber Incident Response and Recovery. International Journal of Science and Research (IJSR), 12(3), 1795–1801. https://doi.org/10.21275/SR231003163025

[4]. Chukwu, N., Yufenyuy, S., Ejiofor, E., Ekweli, D., Ogunleye, O., Clement, T., Obunadike, C., Adeniji, S., Elom, E., & Obunadike, C. (2024). Resilient Chain: AI-Enhanced Supply Chain Security and Efficiency Integration. International Journal of Scientific and Management Research, 07(03), 46–65. https://doi.org/10.37502/IJSMR.2024.7306

[5]. Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era. Journal of Computers, Mechanical and Management, 2(3), 31–42. https://doi.org/10.57159/gadl.jcmm.2.3.23064

[6]. Pooja, & Shilpa. (2017). Implementation On Intrusion Detection System In Mobile Computing. International Journal for Research Publication and Seminar, 8(5), 9–13. Retrieved from https://jrps.shodhsagar.com/index.php/j/article/view/1048

[7]. Singh, S. (2017). Study of Security in Cloud computing. Universal Research Reports, 4(1), 22 30. Retrieved from https://urr.shodhsagar.com/index.php/j/article/view/25

[8]. Thapliyal, V., & Thapliyal, P. (2024). Machine Learning for Cybersecurity: Threat Detection, Prevention, and Response. Darpan International Research Analysis, 12(1), 1–7. https://doi.org/10.36676/dira.v12.i1.01