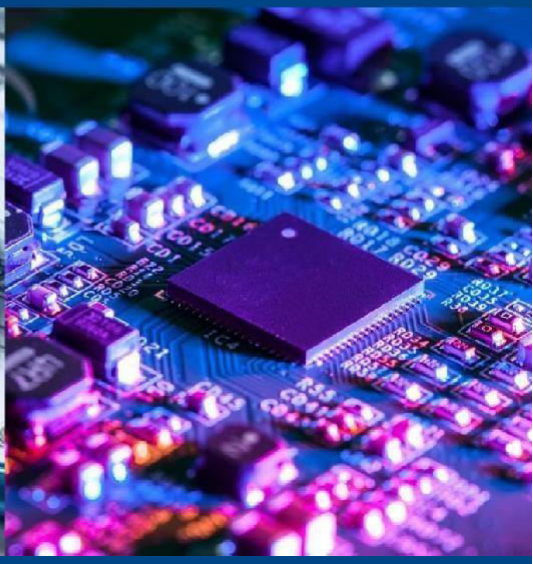
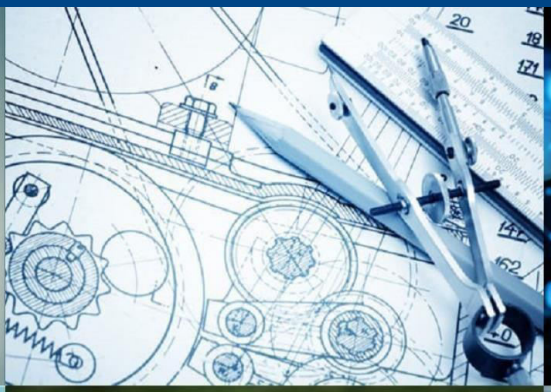
ISSN: 2582-7219

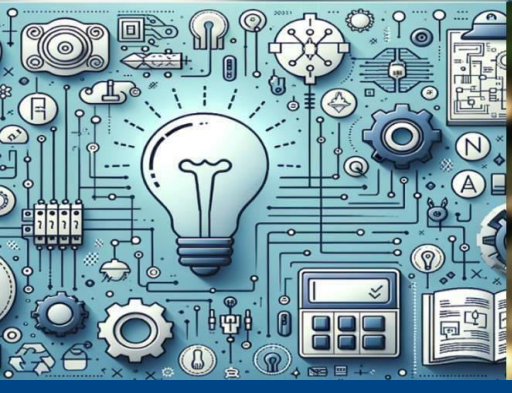




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808092

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

AI FOR SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR) IN CYBER SECURITY

Mr. Uday Kumar H, Mr. Kiran M

Dept. of Mechanical Engineering, The Oxford College of Engineering, Bangalore, India

Dept. of Mechanical Engineering, The Oxford College of Engineering, Bangalore, India

ABSTRACT: In today's cybersecurity landscape, the significance of artificial intelligence AI is increasing. AI systems boost threat in machine learning and data analysis by spotting dangers faster and more precisely than traditional approaches. They help security teams by reducing false positives, automating attack responses, and identifying abnormal behaviors. In spite of these advantages, AI has certain restrictions, including its reliance on high-quality data and susceptibility to adversarial attacks. To keep pace with the evolving nature of cyber threats, it is essential to conduct ongoing research to enhance AI technologies and improve the intelligence and reliable of cybersecurity measures.

KEYWORDS: Cyber security, Artificial Intelligence, machine Learning, automation attacks, data analysis

I. INTRODUCTION

Cybersecurity has become a major worry for people, businesses, and governments in today's digitally connected world. The swift escalation of cyberthreats, encompassing everything from malware and phishing attempts to advanced zero-day exploits, necessitates more responsive and smarter security solutions than conventional approaches can offer. In this field, artificial intelligence (AI) has become a game-changing technology, providing sophisticated threat detection, prediction, and response capabilities. Artificial intelligence (AI) systems can instantly detect possible security breaches, analyze enormous volumes of network data, and spot unusual trends by utilizing machine learning techniques. AI models, as opposed to rule-based security systems, are always learning and adjusting to new attack methods, increasing their accuracy and lowering false positives.

1.1 Advantages of the Proposed Model

AI boosts cybersecurity through rapid and accurate detection of possible threats. Improves cybersecurity through enabling quick and accurate detection of possible threats. process massive datasets in real time, identify irregular patterns, and forecast potential threats before harm occurs. It minimizes false positives, allowing security teams to concentrate on real threats, while automating responses to quickly address attacks. AI's ability to adapt and learn enables it to evolve with new cyber threats, enhancing its resilience against advanced attacks. Furthermore, AI collaborates with diverse security systems to deliver uninterrupted monitoring, round-the-clock protection, and advanced security.

1.2 Disadvantages

AI systems rely significantly on substantial amounts of high-quality data; inadequate or biased datasets may result in incorrect threat detection and misleading alerts. Creating and sustaining AI solutions demands significant investment and specialized knowledge, which limits their accessibility for smaller organizations

1.3 Objectives and Contributions

The main goal of using AI in cybersecurity threat detection is to improve the speed, precision, and effectiveness of recognizing and addressing potential attacks. AI aims to minimize false positives, automate threat detection and response, ensure round-the-clock monitoring, and adapt to changing attack methods with the help of machine learning. It also seeks to harmonize effortlessly with current security frameworks, building a defense system that is predictive, scalable, and resilient.

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808092

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This study showcases how AI algorithms can analyze and process large datasets in real-time, identify anomalies, and forecast threats before they intensify. The focus is on the importance of adaptive learning.

II. RELATED WORKS

Numerous studies have investigated the use of artificial intelligence AI in cybersecurity to improve threat detection and prevention. Signature based instruction detection system, like snort, have proven effective against known threats but are inadequate in detecting zero vulnerabilities and evolving attacks. To address these constraints, researchers have employed machine learning (ML) algorithms such as support Vector Machines (SVM), Decision Trees, and Random Forests to classify malicious network activities. Sommer and Paxson (2010) emphasizing that intrusion detection utilizing machine learning can adjust to changing attack patterns by analyzing ongoing data stream. Progress in deep learning (DL), especially in convolutional Neural (CNN) and Recurrent Neural Networks (RNN), has made it possible to identify complex anomalies in large dataset without the need for manual feature engineering. Shone and colleagues In 2018, it was shown that deep autoencoders can reveal concealed patterns within network traffic, enhancing the ability to detect advanced cyber threats. Hybrid methods that integrate supervised and unsupervised learning with Realtime threat intelligence feeds have demonstrated potential in minimizing false positives and enhancing detection accuracy. Recent studies have explored the challenges posed by adversarial attacks on AI models, highlighting the importance of developing robust and explainable AI (XAI) system to promote transparency and build trust in security operations. Although considerable progress has been made, current models still encounter issues with computational demands, dataset Imbalances, and the ability to generalize to unknown threats, underscoring the necessity for ongoing research.

III. PROPOSED WORK

2.1 Research Objectives

The primary objectives of our research were to:

- Create a model for threat detection using AI that can efficiently analyze and interpret extensive cybersecurity data, including network traffic patterns, user activities, and system logs.
- Improve the precision and dependability of cybersecurity systems by utilizing machine learning and deep learning techniques to reduce false positives and recognize sophisticated attacks.
- Establish capabilities for real-time threat detection and response by integrating advanced AI algorithms into automated security systems.
- Reach an enhanced level of adaptability and resilience in cybersecurity infrastructure, allowing for proactive defense against emerging and evolving cyber threats.

2.2 Proposed Model

For our research, we used a novel AI model named Intelligent Cyber Threat Detection and Response Model (ICTDRM). ICTDRM is specifically designed to integrate advanced machine learning algorithms with real-time data analysis and automated response mechanisms. This model leverages the adaptability of AI to detect, analyze, and mitigate various types of cyber threats, ensuring enhanced accuracy, faster detection times, and proactive defense in modern cybersecurity systems.

2.2.1 Components of the proposed model

- AI Algorithm: The proposed model uses a hybrid deep learning setup that pairs Convolution Neural Networks (CNN) for extracting features with Long Short-Term Memory (LSTM) network for recognizing sequential patterns. detect anomalies in real time, and adapt continuously to evolving cyber threats.
- Threat Data Processing Unit (T-DPU): A specialized unit designed to process large volumes of cybersecurity data, including network packets, system logs, and user activity records. The T-DPU utilizes parallel computing and optimized data pipelines to ensure rapid analysis with minimal latency, enabling near-instantaneous detection of malicious activities.
- Security Infrastructure Integration: The AI algorithm and T-DPU integrated into the organization's cybersecurity infrastructure, allowing direct interaction with firewalls, intrusion prevention systems, and automated incident

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808092

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

response tools. This integration ensures real-time decision-making, faster containment of threats, and improved overall system resilience.

IV. METHODOLOGY

- Data Collection: We assembled a varied dataset from various cybersecurity resources, encompassing network traffic logs, firewall notifications, intrusion detection system (IDS) reports, and system activity logs. This information included both legitimate and harmful actions, offering a balanced basis for training and assessing the AI model.
- Experimental Setup: The cybersecurity system was linked to the Threat Data Processing Unit (T-DPU), which handled incoming data streams instantaneously. This data was utilized to train the hybrid CNN-LSTM algorithm for identifying patterns, detecting and classifying possible threats. Automated incident response systems were also set up to evaluate real-time mitigation effectiveness.
- Tools Used: Alongside conventional programming frameworks like Python and TensorFlow, we used targeted cybersecurity analysis applications, packet inspection systems, and real-time data processing libraries to enhance the AI model's efficiency.
- Assumptions: We presumed that the gathered cybersecurity datasets reflected authentic network environments and that the network infrastructure would ensure stable and continuous data transmission for efficient threat detection

3.1 Justification

suggested AI-powered cybersecurity framework matches our goals by combining sophisticated machine learning techniques with immediate threat for the information and flexible response strategies. This blend guarantees the required speed and accuracy to identify and counteract new cyber threats efficiently. Utilizing deep learning allows the system to recognize intricate attack patterns, whereas adaptive algorithms guarantee ongoing learning from updated threat information, improving resilience over time. The collaboration between AI and cybersecurity tools creates a strong defence able to manage changing attack vectors. This method is crucial for securing vital infrastructure, shielding sensitive information, and enabling safe digital activities in a progressively adverse cyber environment

IV. RESULTS AND DISCUSSION

AI in SOAR platforms monitors user behavior to detect anomalies like unusual login times or restricted access to flag compromised accounts. A real-world example includes Bank One using Darktrace's AI-driven UBA to catch phishing and impersonation attempts.AI-enhanced SOAR platforms sift through massive volumes of security data to detect patterns and anomalies, offering real-time incident analysis. These platforms can ingest, correlate, and contextualize threat intelligence from multiple sources, then share relevant indicators across tools and teams.

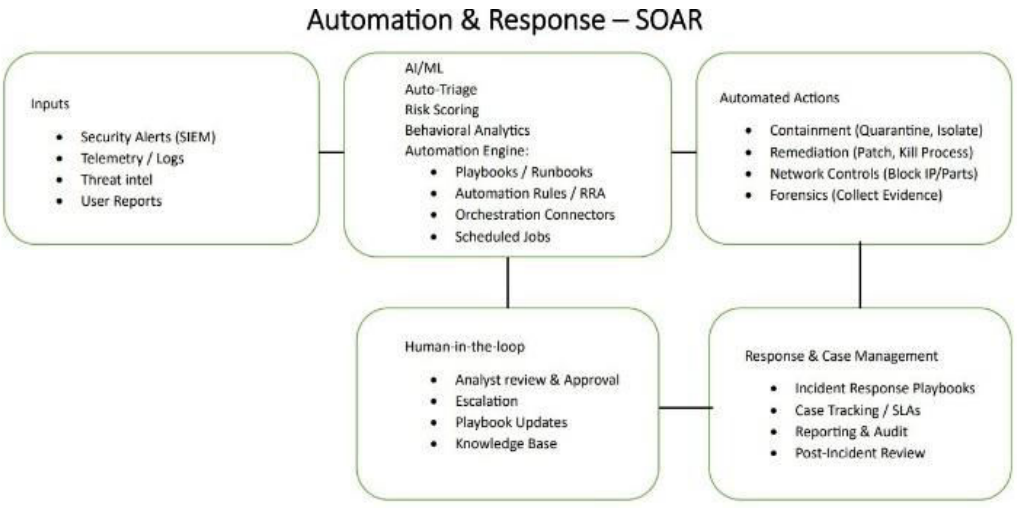


Figure 1: Automation & Response-(SOAR)

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808092

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The illustration depicts the AI-augmented SOAR process. Data from SIEM systems, telemetry/logs, threat intelligence, and user reports is processed by the automation engine, utilizing AI/ML for auto-triage, risk assessment, and behavioural analysis. Automation rules, playbooks, and orchestration

connectors facilitate swift prioritization of alerts. Automated processes encompass containment, remediation, network management, and collection of forensic evidence. A human-in-the-loop guarantees assessment, escalation, and guide updates for complicated incidents. Response and case management encompasses tracking incidents, monitoring SLAs, generating reports, and conducting post-incident evaluations. Combining AI with SOAR provides quicker, more precise, and flexible responses to cybersecurity threats

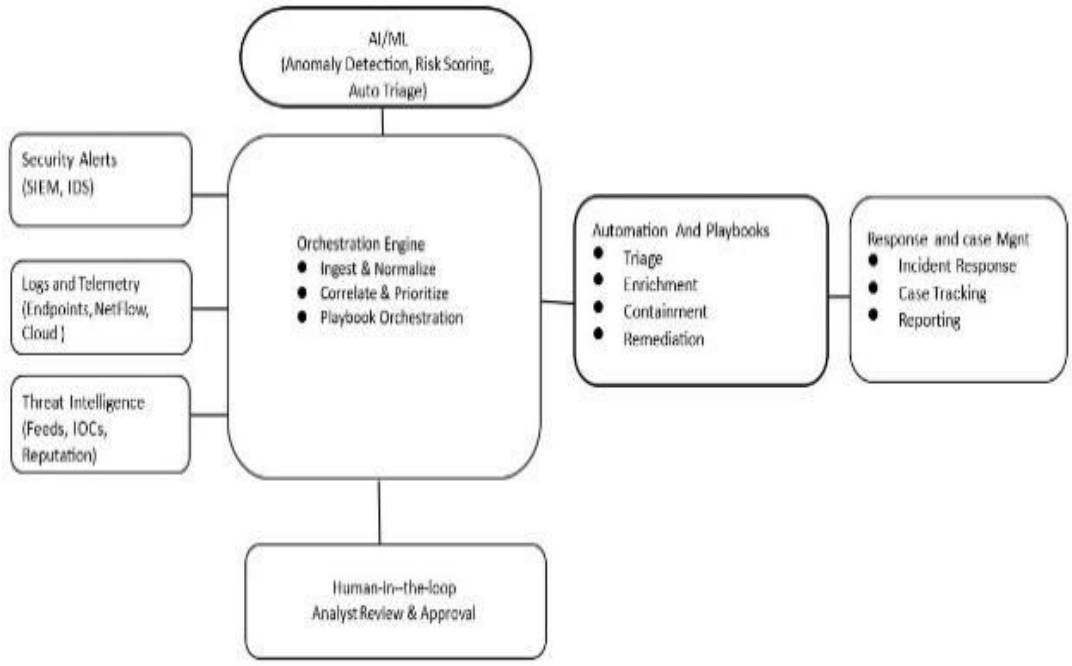


Figure 2: Security Orchestration — Conceptual Flow

The illustration depicts the conceptual process of AI-enhanced SOAR activities. Data like security alerts from SIEM/IDS, logs and telemetry from endpoints or cloud environments, along with threat

intelligence feeds, are fed into the orchestration engine. In this context, AI/ML aids in anomaly detection, risk assessment, and automatic triage, while methods such as normalization, correlation, and prioritization ready incidents for management. Automation and playbooks manage triage, enrichment, containment, and remediation activities. A human-in-the-loop facilitates assessment and validation for intricate situations. Ultimately, response and case management manage incident resolution, monitoring, and documentation, facilitating quicker, more precise, and flexible cybersecurity protections.

V. CONCLUSION

The landscape of Security Orchestration, Automation, and Response (SOAR) by enhancing the speed, accuracy, and effectiveness of cybersecurity operations. As cyber threats grow in complexity and volume, traditional security tools and human analysts alone struggle to keep pace. AI-powered SOAR platforms address this challenge by automating routine tasks, intelligently correlating threat data, and orchestrating responses across diverse security tools and systems. Faster Threat Detection and Response: AI enables real-time analysis of massive datasets, identifying anomalies and triggering rapid, automated responses to threats.

Improved Decision-Making: Machine learning models can prioritize incidents based on risk, helping analysts focus on high-impact threats.
Operational Efficiency: Automation reduces the burden on human teams, decreases response times, and minimizes alert fatigue.

Continuous Learning: AI systems can learn from past incidents, improving accuracy and reducing false positives over time.

REFERENCES

1.Albanese et al. (2025) – Towards AI-Driven Human-Machine Co-Teaming for Adaptive and Agile Cyber Security Operation Centers (arXiv, May 2025) — on LLM-augmented SOC workflows
2. Kremer et al. (2023) – IC-SECURE: Intelligent System for Assisting Security Experts in Generating Playbooks for Automated Incident Response (arXiv, Nov 2023)
3. Rjoub et al. (2023) – A Survey on Explainable Artificial Intelligence for Cybersecurity (arXiv, Mar 2023)
4. Bernardez Molina et al. (2023) – Tackling Cyberattacks through AI-based Reactive Systems: A Holistic Review and Future Vision (arXiv, Dec 2023)
5. MDPI (2025) – Toward Robust Security Orchestration and Automated Response in Security Operations Centers with a Hyper-Automation Approach Using Agentic Artificial Intelligence — real-world pilot of AI-driven SOA
6. Bartwal et al. (2022) – Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots (arXiv) — dynamic SOAR honeypot deployment
7. Springer (2025) – Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms — includes section "AI-driven security orchestration"
8. MDPI (Symmetry journal) – Cloud Security Automation Through Symmetry: Threat Detection and Response — explores SOAR and AI-automation in cloud security
9. Link Springer (2025) – Leveraging AI for enhanced cybersecurity: a comprehensive review — broader AI threat intelligence and operations context
10. Link Springer (2021) – Artificial intelligence in cyber security: research advances, challenges, and opportunities
11. MDPI (2023) – Cybersecurity for AI Systems: A Survey — addresses security implications for AI-centric systems
12 Wikipedia (AIOps) – Not strictly SOAR but covers AI-driven operations in IT and cybersecurity
13. Survey on Offensive AI Within Cybersecurity (arXiv, Sep 2024) — adversarial and malicious uses of AI
14. Wikipedia – Mariarosaria Taddeo (2024) – ethics and trust in AI for cybersecurity
15. ACM TSE Methods (APIRO) – automated support for SOC teams in tool API orchestration
16. ITPro (Jul 2025) – adoption trends of AI in cybersecurity environments
17. Axios "Future of Cybersecurity" (Aug 2025) – AI tools like Claude in red-teaming and defense
18 Investopedia (10 months ago) – CISO concerns: AI-driven phishing & defence deployment
19. Business Insider (Mar 2025) – generative AI threat landscape vs banking defences
20 Deloitte / WSJ guide (1.3 years ago) – guide for CISOs using AI in cyber defines

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com