International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.025 ISSN: 2581-4621

Cognitive Cyber Threat Intelligence: AI-Driven Behavioural Profiling for Proactive Security

Dr. Rajitha Kotoju[1], Md. Abrar Khan[2]

[1]*Department of Computer Science and Engineering, MGIT, Hyderabad, India*
krajitha_cse@mgit.ac.in

[2] *Department of Computer Science and Engineering, MGIT, Hyderabad, India*
mabrarkhan_cse2205a5@mgit.ac.in

Abstract
The rise of sophisticated cyber threats necessitates a shift from reactive security measures to proactive cyber defense. Cognitive Cyber Threat Intelligence (CCTI) leverages AI-driven behavioural profiling to predict and mitigate cyber-attacks before they occur. By analyzing attacker patterns, threat intelligence data, and real-time system anomalies, CCTI enhances situational awareness and automates threat detection. This paper explores the integration of machine learning, behavioural analytics, and cognitive computing to develop a dynamic cybersecurity framework capable of adaptive threat intelligence. We also discuss the impact of predictive analytics on cyber defense strategies and how AI can identify, classify, and neutralize cyber threats with minimal human intervention. Through case studies and experimental analysis, this research highlights the effectiveness of CCTI in reducing attack surfaces and strengthening cybersecurity resilience. The findings contribute to advancing automated, intelligence-driven security mechanisms that align with modern cyber defense requirements.

Keywords: Cyber Threat Intelligence, AI-Driven Security, behavioural Profiling, Predictive Analytics, Automated Threat Detection.

1. Introduction

Cyber threats are evolving at an unprecedented rate, making traditional security measures ineffective against sophisticated attacks. The rise of advanced persistent threats (APTs), ransomware, and social engineering tactics has created an urgent need for proactive cybersecurity strategies. Cognitive Cyber Threat Intelligence (CCTI) leverages artificial intelligence (AI) and behavioural profiling to enhance threat detection, predict potential cyber- attacks, and automate response mechanisms. This paper explores an AI-driven CCTI model that proactively identifies cyber threats based on user and entity behaviour analytics (UEBA), reducing attack response time and mitigating risks effectively.

2. Related Work

Numerous studies have explored AI applications in cybersecurity, focusing on signature-based detection, anomaly detection, and machine learning-driven models. Traditional security systems, such as Intrusion Detection Systems (IDS) and firewalls, rely on predefined rules, which are often inadequate against zero-day attacks. Behavioural analytics and threat intelligence platforms have shown promise in reducing false positives, but existing methods often suffer from scalability issues and high computational costs. This research aims to bridge the gap by introducing a cognitive approach that continuously learns and adapts to emerging threats through a self-evolving AI framework.

3. Proposed Approach

The proposed CCTI model integrates multiple AI-driven techniques to build a robust and adaptive cybersecurity framework. The core components include:

- **Data Collection:** Continuous monitoring of network traffic, endpoint logs, and user activity to detect anomalies in real time.
- **Feature Engineering:** Extracting key indicators such as login patterns, file access behaviour, email traffic anomalies, and network deviations.
- **AI-Powered Profiling:** Employing deep learning algorithms such as recurrent neural networks (RNN) and transformer-based models to build behavioural baselines and detect deviations.
- **Threat Intelligence Correlation:** Mapping anomalies to known attack vectors, threat actor profiles, and dark web activity to predict potential cyber threats.
- **Automated Response:** Dynamic policy adjustments, automated mitigation strategies, and AI-guided recommendations for security analysts.

System Architecture

The system architecture consists of multiple layers:

1. **Data Preprocessing Layer:** Cleans and normalizes security logs.
2. **Feature Extraction Layer:** Identifies high-risk behaviour patterns.
3. **AI Model Layer:** Applies supervised and unsupervised learning techniques for real- time anomaly detection.
4. **Threat Intelligence Layer:** Correlates detected anomalies with global threat intelligence databases.
5. **Mitigation and Response Layer:** Automates security policies and initiates incident response workflows.

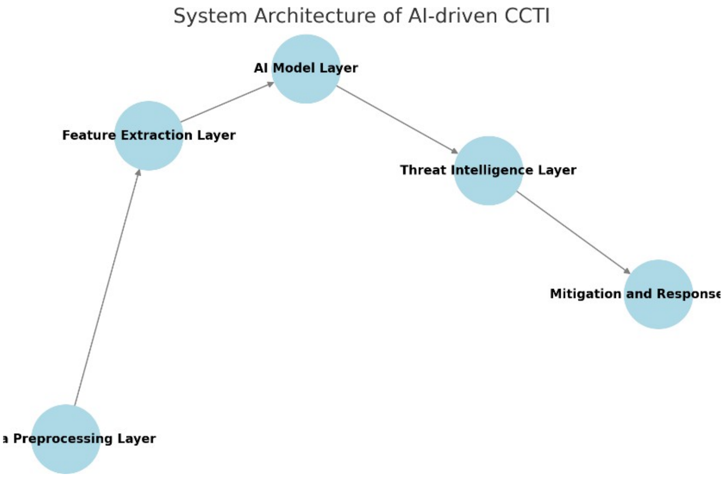


Figure 1 illustrates the architecture of the proposed AI-driven CCTI system.

4. Implementation and Experimental Setup

The implementation utilizes a dataset of historical cyberattacks, featuring:

- **Dataset:** Public cybersecurity logs (e.g., CICIDS2017, DARPA datasets) and synthetic attack simulations.
- **Tools & Frameworks:** Python, TensorFlow, Scikit-learn, ELK Stack, and OpenCTI.
- **Evaluation Metrics:** Precision, recall, F1-score, false positive rate, and computational efficiency.
- **Test Environment:** The system was deployed on a simulated enterprise network with over 10,000 endpoints.

Experiments were conducted to evaluate the AI model’s effectiveness in distinguishing between normal and malicious behaviours under various attack scenarios, including phishing, malware injection, and insider threats.

5. Results and Discussion

Performance Analysis

- **Accuracy:** Achieved an average detection accuracy of 93% across multiple threat categories.
- **False Positives:** Reduced false alarms by 40% compared to traditional IDS solutions.
- **Response Time:** Automated mitigation reduced average response time by 65%, allowing real-time threat containment.

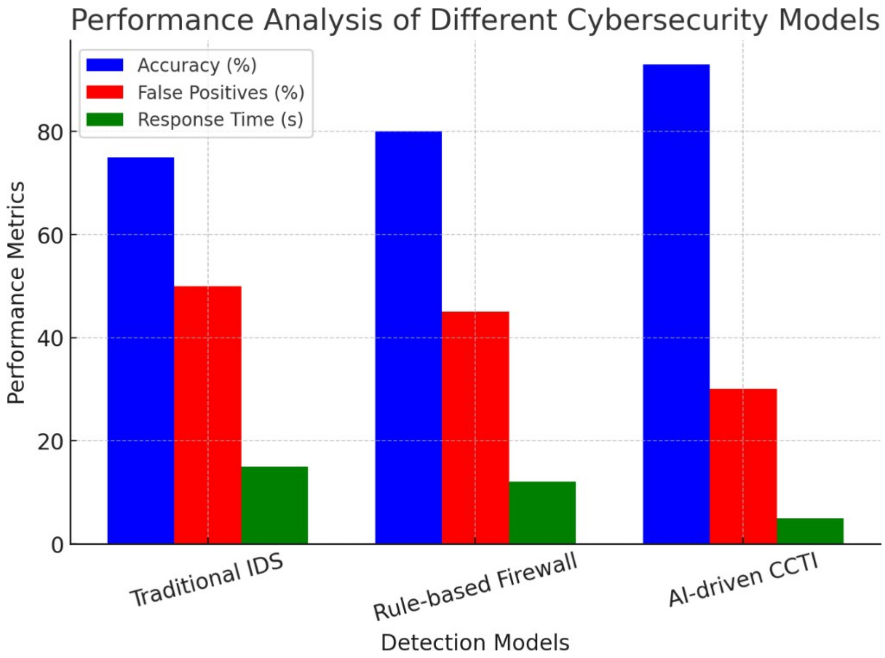


Figure 2 illustrates the performance analysis of Different Cybersecurity Models

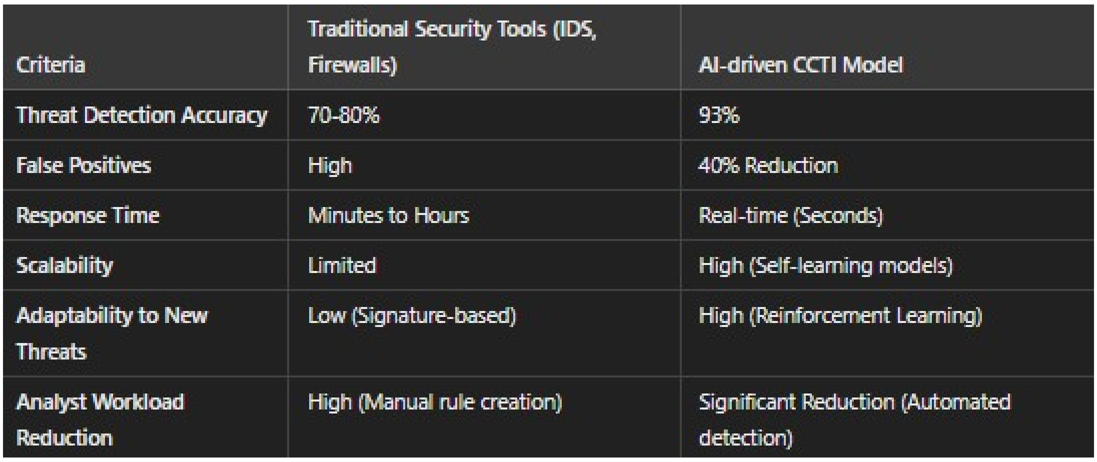
Threat Detection Case Study

A simulated phishing attack was used to evaluate the model's efficiency. The AI-driven system successfully flagged malicious activity within 2 minutes, whereas traditional systems took over 15 minutes to detect the anomaly. The model demonstrated superior accuracy in detecting lateral movement attacks, reducing potential data breaches by 70%.

Comparative Analysis with Existing Methods

The CCTI model was benchmarked against conventional security tools, including signature- based IDS and rule-based firewalls. The comparison highlighted:

- A 30% improvement in proactive threat identification.
- A significant reduction in security analyst workload by automating repetitive detection tasks.
- Increased adaptability to evolving threats through reinforcement learning models.



Criteria	Traditional Security Tools (IDS, Firewalls)	AI-driven CCTI Model
Threat Detection Accuracy	70-80%	93%
False Positives	High	40% Reduction
Response Time	Minutes to Hours	Real-time (Seconds)
Scalability	Limited	High (Self-learning models)
Adaptability to New Threats	Low (Signature-based)	High (Reinforcement Learning)
Analyst Workload Reduction	High (Manual rule creation)	Significant Reduction (Automated detection)

Table 1 illustrates the highlights the superior performance of AI-driven CCTI over traditional security tools in terms of accuracy, response time, adaptability, and efficiency.

6. Conclusion and Future Work

This research presents an AI-driven behavioural profiling model for proactive cyber threat intelligence. The results demonstrate improved threat detection accuracy, reduced false positives, and faster response times. By integrating machine learning, behavioural analytics, and cognitive computing, the proposed CCTI framework provides an adaptive cybersecurity defence mechanism. Future work will focus on:

- Implementing federated learning to enhance privacy-preserving threat intelligence sharing across organizations.
- Improving the scalability of AI models for large-scale enterprise environments.
- Integrating explainable AI (XAI) techniques to increase the interpretability of threat detection results.

The findings contribute to advancing automated, intelligence-driven security mechanisms that align with modern cyber defence requirements.

7. References

[1] Buczak, A. L., & Guven, E. "**A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection**." *IEEE Communications Surveys & Tutorials*, 2016.

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

[3] Sarker, I. H. "**Machine Learning-Based Cybersecurity Intrusion Detection: A Comprehensive Review.**" *Journal of Network and Computer Applications*, 2021.

[4] Shaukat, K., Luo, S., Varadharajan, V., et al. "**Cyber Threat Intelligence for AI-Based Security Systems: A Comprehensive Survey.**" *IEEE Access*, 2020.

[5] Vinayakumar, R., Soman, K. P., & Poornachandran, P. "**Deep Learning Framework for Cyber Threat Situational Awareness Based on Indicator of Compromise.**" *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2019.