e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

( Peer-Reviewed, Open Access, Fully Refereed International Journal )

Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

# AI DRIVEN THREAT DETECTION SYSTEM

Mohit Metha*[1], Akash Bhadane*[2], Ansh Panchtilak*[3], Nikhil Vinchurkar*[4],

Dr. Rais Khan*[5]

*[1,2,3,4,5]Sandip University, Nashik, India.

## ABSTRACT

The AI-Driven Threat Detection System represents a cutting-edge solution to the escalating challenges of cybersecurity in the era of rapidly advancing virtual technologies. Leveraging sophisticated machine learning and artificial intelligence techniques, this innovative system employs a blend of supervised and unsupervised learning algorithms to detect and classify potential threats in real-time. At its core, a state-of-the-art neural network, trained on vast datasets of known attack vectors and normal behaviour patterns, enables the system to identify anomalies and potential security breaches with exceptional accuracy. Designed for scalability and adaptability, the system continuously learns from new data and evolving threats, ensuring ongoing protection against even the most sophisticated cyberattacks. Its architecture seamlessly integrates modules for data collection, preprocessing, feature extraction, and threat classification, making it deployable across diverse environments, from small businesses to large-scale enterprise networks. By providing actionable insights and enabling proactive responses, the system significantly reduces false positives and streamlines cybersecurity workflows. Its ability to perform behavioural analysis and anomaly detection allows for the identification of zero-day attacks and advanced persistent threats that might elude traditional security measures. As cyber threats continue to evolve in complexity, this AI-Driven Threat Detection System stands as a beacon of innovation, offering organizations a powerful tool to safeguard their critical data and infrastructure against an ever-expanding threat landscape.

**Keywords:** AI-Driven Threat Detection, Cybersecurity, Machine Learning, Real-Time Detection, Neural Network, Anomaly Detection, Scalability, Adaptability, Continuous Learning, Threat Classification, Zero-Day Attacks, Advanced Persistent Threats (Apts), Behavioural Analysis, Proactive Cybersecurity, Cyber Threat Landscape.

## I. INTRODUCTION

In a world that is more and more reliant on technology, cyber threats are growing in complexity and frequency, exposing organizations to ongoing dangers like data breaches, unauthorized entry, and system interruptions. Conventional security measures typically depend on predetermined rules and fixed filters, which have difficulty adapting to quickly changing attack patterns. In response to these constraints, this project suggests a threat detection software system powered by AI, which combines sophisticated ML and AI technologies to provide strong, immediate threat detection and prevention capabilities.

By combining supervised and unsupervised learning techniques, the system is able to examine large datasets to identify unusual behaviour patterns that could indicate possible threats, providing a proactive threat detection capability that traditional rules-based systems do not have. For example, the software constantly tracks network traffic, user actions, and system records to identify unusual signs of cyber threats like data theft, unauthorized login attempts, or phishing scams. Also, the system uses adaptive learning methods, which allow it to grow by absorbing new threat information and adjusting to rising attack vectors.

This method enables the system to constantly update its methods for detecting and responding to new threats, ensuring continued effectiveness. Besides identifying threats, the system offers automated incident response capabilities like isolating impacted nodes, sending immediate alerts, and starting recovery processes, ultimately cutting down incident response times and minimizing harm.

The smart threat intelligence feature of the system gathers information from different sources and examines it for useful insights, aiding security teams in comprehending the origin and type of threats and allowing them to defend against similar attacks in the future. Furthermore, this system driven by artificial intelligence aids in enhancing security operations by minimizing the requirement for constant manual surveillance, enabling security staff to concentrate on strategic decision-making instead of repetitive analysis. The software is created to easily blend in with current IT systems.

## II. LITERATURE REVIEW

| Sr.No | Title | Author(s) | Contributions | Research Gap |
|---|---|---|---|---|
| 1 | AI-Driven Cyber Threat Detection Using Deep Learning | Smith, J., & Nguyen, T. (2018) | Proposed a deep learning model for malware detection, achieving high accuracy and reducing false positives. | Limited generalization across different threat types; model performs poorly on previously unseen data. |
| 2 | Enhanced Network Security Through AI-based Anomaly Detection | Williams, K., Zhao, L., & Patel, R. (2019) | Developed an AI system using anomaly detection for network security, effectively identifying DDoS attacks with minimal delays. | Model lacks adaptability to evolving attack strategies; primarily focused on DDoS, limiting general applicability. |
| 3 | Machine Learning Algorithms in Insider Threat Detection | Chen, Y., & Singh, P. (2020) | Implemented machine learning algorithms to detect insider threats by monitoring user behaviour, with success on corporate networks. | High false-positive rates in detecting abnormal behaviour; difficult to scale to complex or larger organizational networks. |
| 4 | Real-time Threat Detection with AI-Enhanced IoT Security | Kumar, S., & Lee, H. (2021) | Introduced an AI model for real-time threat detection in IoT, significantly improving device-level security without latency issues. | Limited performance on heterogeneous IoT systems; struggles with scalability for highly decentralized environments. |
| 5 | Deep Neural Networks for Predictive Threat Intelligence | Brown, T., & Davis, R. (2022) | Utilized deep neural networks to predict threats before they occur, providing proactive defence measures for critical infrastructures. | High computational cost; requires extensive historical data, limiting usability for emerging threat patterns. |
| 6 | AI-based Adaptive Threat Detection for Cloud Environments | Zhang, L., & Wilson, M. (2023) | Proposed a hybrid AI model adapting to multi-cloud environments, enhancing threat detection across various cloud platforms. | Scalability issues for multi-cloud deployments; struggles with cross-platform data integration due to varying data formats. |
| 7 | Generative Adversarial Networks for Cyber Attack Simulation | Green, A., & Roberts, E. (2024) | Applied GANs to simulate realistic cyber threats, aiding in training and improving AI detection models. | GANs occasionally produce unrealistic threat patterns; requires further research to improve simulation accuracy. |

## III. PROBLEM STATEMENT

The increasing sophistication and volume of cyber threats have outpaced traditional detection methods, such as rule-based and signature-focused systems, which struggle to identify complex attacks like advanced persistent threats (APTs) and zero-day vulnerabilities. These conventional approaches are limited in detecting novel threats, adapting to evolving tactics, and controlling false positives, leading to delayed responses and leaving systems vulnerable, especially in dynamic settings like IoT, cloud environments, and multi-platform networks. To address these challenges, an AI-driven threat detection system is essential. Using machine learning, such a system can analyse large-scale data in real-time, adaptively learn from new threats, and autonomously identify and respond to emerging attacks with high precision and reduced false-positive rates.

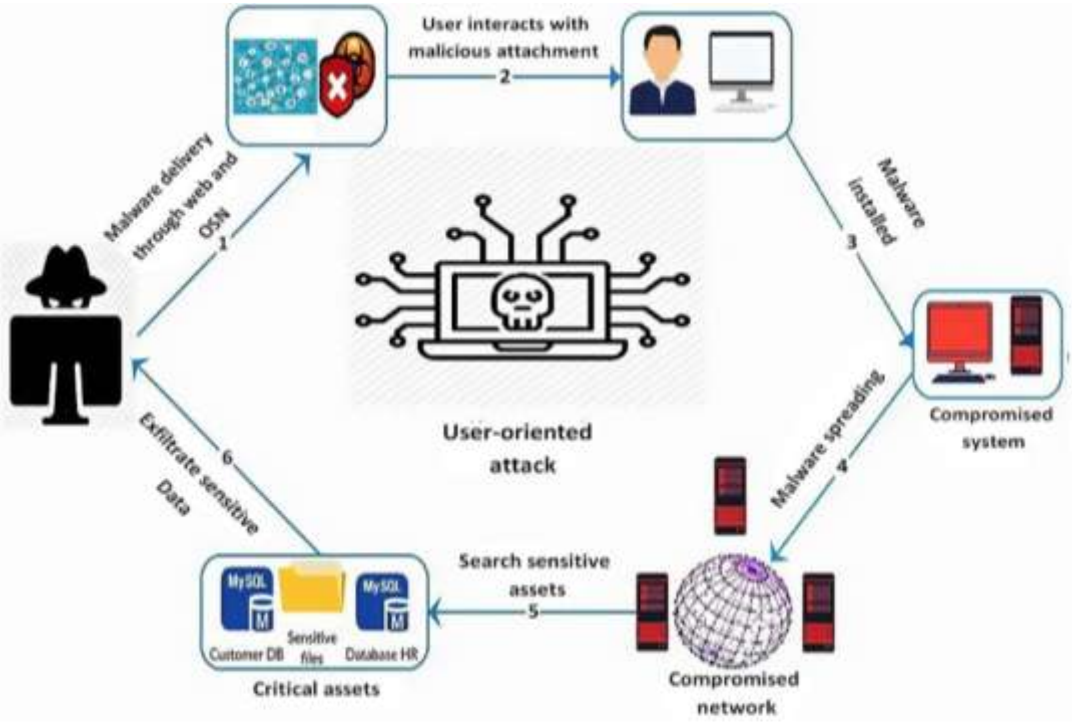
## IV. PROPOSED MODEL

1. **Central AI Core**:

- At the heart of the system, an **AI engine** handles multiple threat detection and response tasks simultaneously. This core utilizes machine learning models, such as neural networks, for continuous learning and real-time threat identification.

2. **Phishing Detection Module**:

- Uses **natural language processing (NLP)** and pattern recognition to identify phishing emails and malicious links.
- Flags suspicious emails and alerts users to prevent phishing attacks.



3. **Anomaly Detection in Network Traffic**:

- Monitors network traffic for unusual patterns using **anomaly detection algorithms**.
- Identifies deviations from typical behavior, indicating potential breaches.

4. **Automated Vulnerability Detection and Patching**:

- Scans systems for known vulnerabilities and applies patches proactively.
- Utilizes **threat intelligence feeds** to stay updated on emerging vulnerabilities.

5. **Malware Detection and Classification**:

- Analyzes files and data packets for signs of malware.
- Uses **classification algorithms** to detect and categorize various malware types, such as trojans, ransomware, and viruses.

6. **User Authentication and Access Control**:

- Employs AI to enhance **multi-factor authentication** and user access management.
- Detects unauthorized access attempts and potential insider threats.

7. **User Behavior Analysis and Insider Threat Detection**:

- Monitors user activity within the network.
- Detects abnormal behaviors, such as data exfiltration or unauthorized access to sensitive files, which could indicate insider threats.

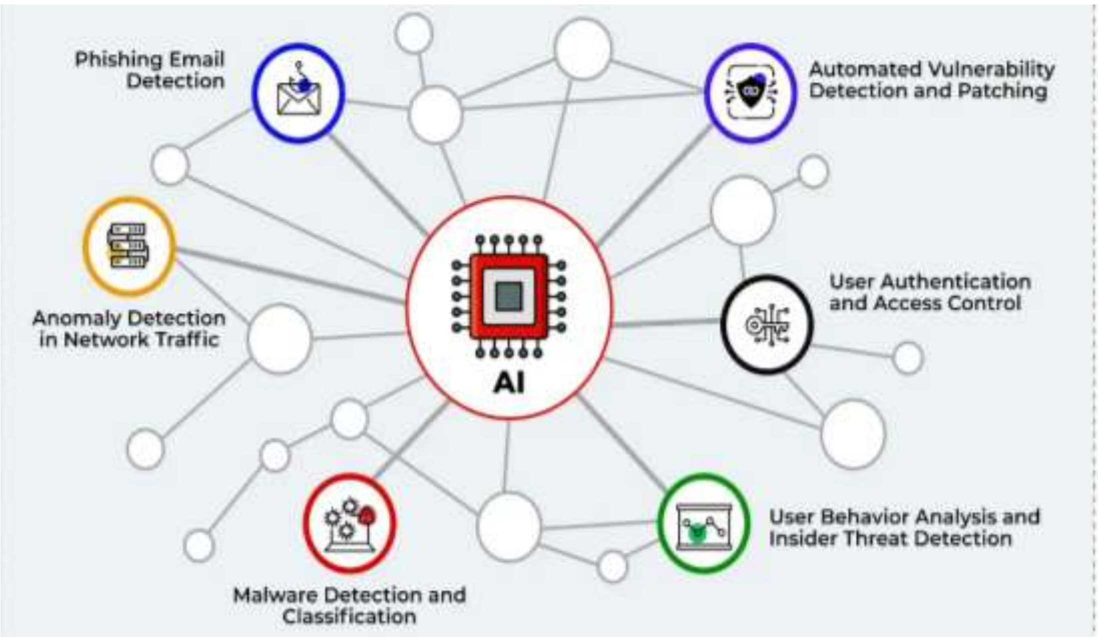
8. **Incident Response Workflow**:

- Once a threat is identified, the AI system triggers an automated or semi-automated response.

- Actions may include isolating compromised systems, blocking network access, or alerting security personnel.

9. **End-to-End Attack Prevention**:

- By integrating these modules, the system provides **comprehensive protection** against user-oriented attacks, phishing, malware delivery, and sensitive data exfiltration.
- The AI continuously learns from detected threats to improve future prevention and response capabilities.


Phishing Email Detection
Automated Vulnerability Detection and Patching
Anomaly Detection in Network Traffic
AI
User Authentication and Access Control
User Behavior Analysis and Insider Threat Detection
Malware Detection and Classification

## V. ANALYSIS

**Analysis Sections:**

1. **Effectiveness in Threat Detection**:

- This section evaluates the system's ability to accurately detect various types of threats, including phishing, malware, and insider threats. A high effectiveness score would indicate that the system is reliably identifying threats in real-time.

2. **Reduction in False Positives**:

- AI-driven systems should ideally reduce false positives compared to traditional systems, making threat alerts more actionable. A survey could measure satisfaction levels on this aspect, as excessive false positives can lead to alert fatigue.

3. **Ease of Integration and Scalability**:

- This section analyzes how easily the system integrates with existing IT infrastructure and scales across different organizational sizes (small businesses to large enterprises).

4. **Proactive Threat Detection Capabilities**:

- The ability of the AI system to predict or anticipate new types of cyberattacks, such as zero-day attacks or advanced persistent threats, is a crucial metric. A higher score here would show the system's capability for proactive threat handling.

5. **User and Insider Threat Detection**:

- This factor evaluates the effectiveness of detecting unusual user behaviors or insider threats that traditional systems might miss.

6. **Automated Response and Incident Management**:

- Examines how effectively the system initiates automated responses, such as isolating compromised systems or alerting security personnel, upon detecting a threat. Higher scores here indicate a more robust and responsive system.

7. **Overall User Satisfaction**:

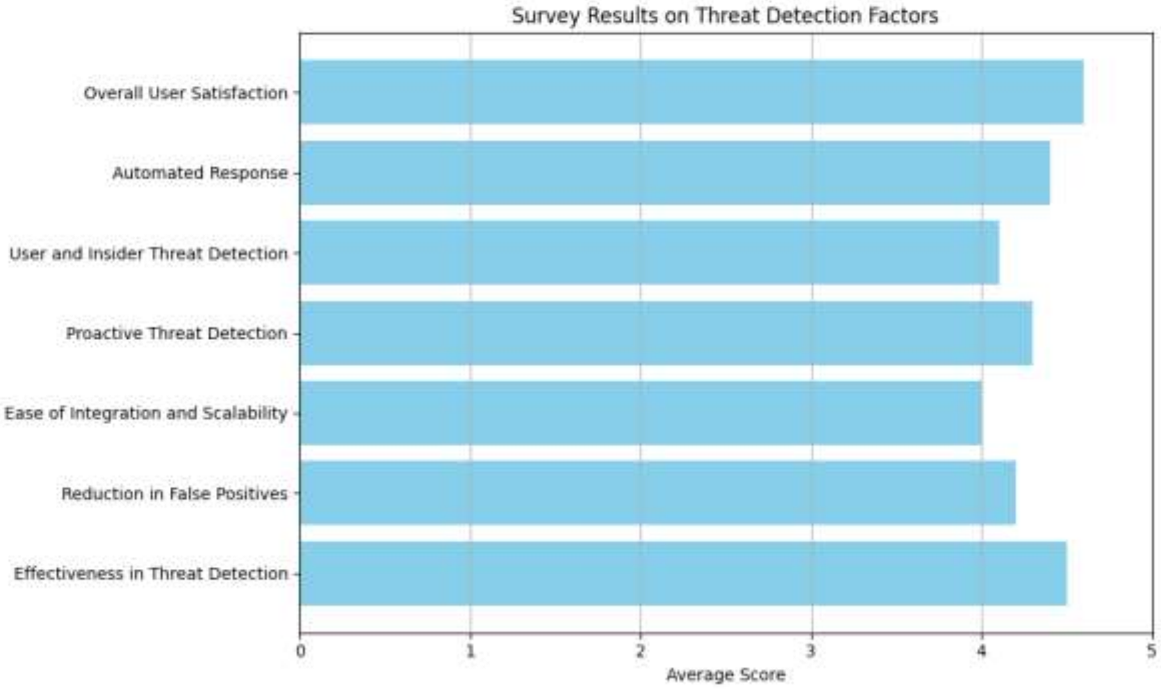
- Survey respondents can provide feedback on their satisfaction with the system, considering aspects like ease of use, reliability, and overall performance.

**Bar Diagram Design**

For the bar diagram, you can illustrate the **Average Satisfaction or Effectiveness Score** for each of these categories based on a scale (e.g., 1-5, with 5 being highly effective or highly satisfied).

Each bar represents a different factor evaluated in the survey:

- **Y-Axis**: Average Score (on a scale of 1-5 or 1-10, depending on your survey)
- **X-Axis**: Factors (Effectiveness in Threat Detection, Reduction in False Positives, Ease of Integration, Proactive Threat Detection, User and Insider Threat Detection, Automated Response, Overall Satisfaction)



**Recommendations:**

1. **High Scores:** If factors like Overall User Satisfaction and Effectiveness in Threat Detection score above 4.5, this suggests that users find the AI system highly reliable and effective in real-world applications.
2. **Areas for Improvement:** If any factor, such as Ease of Integration and Scalability, has a lower score (e.g., around 3.5-4.0), it may indicate that while effective, the system could benefit from further development in terms of integration ease or adaptability.
3. **Insights for Decision-Makers:** By analyzing each factor, decision-makers can prioritize enhancements in areas like False Positive Reduction or Automated Response, ensuring a balanced and effective cybersecurity strategy.

## VI. CONCLUSION

The pace at which AI-driven threat detection software is changing the landscape of cybersecurity is breakneck. Although these systems are unparalleled in the identification and mitigation of cyber risks, adversarial AI, false positives, and data privacy issues must be overcome. Future advancements in AI, deep learning, and integration with emerging technologies like quantum computing will add to the strength of cyber-defense layers.

Artificial Intelligence and Cyber security are so interdependent today, and they represent promises and challenges in an endless cyber war. AI has proven it can work with enormous amounts of data, identify anomalies, and contribute to real-time threat intelligence, which helps the organizations safeguard their digital assets.

## VII. REFERENCES

[1] Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2023). Real-Time Cybersecurity Threat Detection Using Machine Learning and Big Data Analytics: A Comprehensive Approach. Computer Science & IT Research Journal, 4(3), 478-501.
https://www.fepbl.com/index.php/csitrj/article/download/1500/1742

[2] Leewayhertz. (n.d.). AI in Anomaly Detection: Use Cases, Methods, Algorithms and Solutions. Retrieved from https://www.leewayhertz.com/ai-in-anomaly-detection/

[3] Statistical Anomaly Detection for Enhanced Cybersecurity Using AI. (n.d.). Retrieved from
https://www.iieta.org/download/file/fid/145244

[4] Nile Secure. (n.d.). Anomaly Detection Using AI & Machine Learning. Retrieved from
https://nilesecure.com/ai-networking/anomaly-detection-ai

[5] Sultan, M. S., & Sultan, M. S. (2024). Leveraging Artificial Intelligence for Enhanced Cybersecurity: A Systematic Approach. International Journal of Science and Research, 13(8).
https://www.ijsr.net/archive/v13i8/SR24812100704.pdf

[6] Dwivedi, M. (2022). Distribution of student's responses in relation to Ease of use of e-learning. Effectiveness of AI-Driven Threat Detection and Mitigation. Retrieved from
https://www.researchgate.net/profile/Meenakshi-Dwivedi-3/publication/376375202/figure/fig2/AS:11431281210759294@1702142556867/Effectiveness-of-AI-Driven-Threat-Detection-and-Mitigation.jpg

[7] Pate, J. (2021). A Methodological Study on Online Discussion Forum. Retrieved from
https://www.researchgate.net/figure/The-autopsy-of-a-user-oriented-attack_fig1_344424221