

AI-Powered Cyber Threat Detection System

GREESHMA H K , Dr. Md. ISHRAD HUSSAIN B

Student, Department of MCA,UBDTCE, UBDTCE,Davanagere-5770004,Karnataka,India

Assistant Professor, Department of MCA, UBDTCE, Davanagere-5777004, Karnataka,India

ABSTRACT

The widespread adoption of digital technologies across various sectors has increased the risk of cyberattacks targeting computer networks and information systems. Organizations face numerous security challenges, including malware, phishing, ransomware, data breaches, and unauthorized access attempts. Traditional security solutions mainly rely on predefined rules and known attack signatures, making them less effective against emerging and previously unseen threats. As cyber threats become more sophisticated, the demand for intelligent and adaptive security mechanisms continues to grow. This study explores the role of artificial intelligence in cyber threat detection.

INTRODUCTION

Artificial Intelligence has emerged as a powerful technology capable of addressing many of these cybersecurity challenges. By analysing large volumes of data and identifying hidden patterns, AI systems can detect suspicious activities that may indicate potential security threats. Unlike traditional security mechanisms, AI-based solutions can learn from historical data and adapt to changing attack techniques.

This research focuses on understanding how Artificial Intelligence can enhance cyber threat detection capabilities. It examines different machine learning approaches, discusses their applications in cybersecurity, and evaluates their effectiveness in identifying both known and emerging cyber threats.

LITERATURE SURVEY

With the rapid growth of digital technologies, cybersecurity has become an important research area. Traditional security systems were mainly designed to detect attacks by comparing network activities with previously identified threat patterns. Although these methods were effective against known attacks, they often failed to recognize new and sophisticated threats. This limitation encouraged researchers to explore more

advanced approaches for protecting computer networks and information systems.

Artificial Intelligence and Machine Learning have emerged as valuable technologies for improving cyber threat detection. Machine learning models can analyze large volumes of security data and identify suspicious activities that may indicate malicious behaviour. Supervised learning techniques such as Decision Trees, Support Vector Machines, Random Forests, and Naïve Bayes have been widely used to classify network traffic as normal or harmful. These methods have shown promising results in improving detection accuracy and reducing response time.

AI TECHNIQUES FOR CYBER THREAT DETECTION

Machine Learning plays a vital role in modern cyber threat detection systems. It enables computers to learn from historical data and identify suspicious activities without requiring constant human intervention. By examining network traffic, user behaviour, and system logs, machine learning models can recognize patterns associated with cyberattacks and generate timely alerts.

Supervised learning techniques are commonly used to classify network activities as normal or malicious. Algorithms such as Decision Trees, Random Forests, and Support Vector Machines are widely adopted because of their ability to provide accurate threat detection. These models are trained using labeled datasets and can effectively identify known attack patterns.

3.1 Machine Learning in Cybersecurity

Machine Learning is an important component of modern cybersecurity systems. It allows computers to examine large amounts of security-related data and identify patterns associated with malicious activities. By analyzing network traffic, user actions, and system logs, machine learning models can detect potential threats and support faster security responses.

3.2 Supervised Learning Techniques

Supervised learning is commonly used for cyber threat detection because it trains models using labeled datasets containing both normal and malicious activities. Once trained, the model can classify new data and identify potential threats based on learned patterns.

Some widely used supervised learning algorithms include:

Decision Trees: These algorithms use a structured set of rules to classify network activities and identify suspicious behaviour. They are simple to understand and effective for security analysis.

Random Forest: This technique combines multiple decision trees to improve prediction accuracy and reliability. Due to its strong performance and robustness, it is frequently used in intrusion detection systems.

METHODOLOGY

➤ Data Collection

The proposed AI-based cyber threat detection system begins with collecting security-related information from multiple sources. The accuracy of threat detection largely depends on the availability of reliable and up-to-date data. Information is gathered from network devices, security tools, and system monitoring platforms to provide a complete view of network activities.

Data sources include:

- Network traffic logs
- Firewall records
- System event logs
- User authentication details
- Application activity records
- Cloud monitoring services

The collected information helps identify suspicious behaviour and supports effective threat analysis.

➤ Data Pre-processing

Before analysis, the collected data must be prepared to ensure consistency and reliability. Security datasets often contain incomplete, duplicate, or unnecessary information that can affect model performance.

The pre-processing stage includes:

- Cleaning inaccurate data
- Removing duplicate records
- Managing missing values
- Reducing unwanted noise
- Normalizing data formats
- Selecting relevant attributes

This process improves data quality and enables machine learning models to produce more accurate results.

➤ Feature Extraction

Feature extraction involves selecting important characteristics from the processed data that can help identify cyber threats. By focusing on relevant features, the system can improve detection efficiency and reduce computational overhead.

Common features used for analysis include:

- Source IP address
- Destination IP address
- Packet size
- Protocol type
- Connection duration
- Login frequency
- Failed login attempts
- Data transfer volume

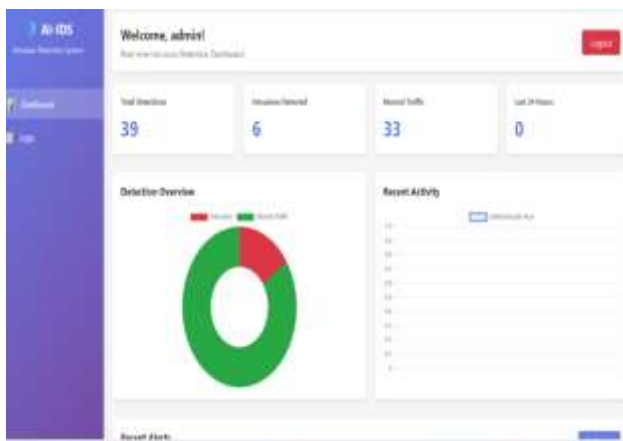
These features are supplied to machine learning models, which analyze them to distinguish normal network behaviour from potentially malicious activities.

RESULTS AND DISCUSSION

The use of Artificial Intelligence in cybersecurity has improved the ability of security systems to identify potential threats within network environments. AI-based solutions can examine large amounts of security data and detect suspicious activities more efficiently than traditional rule-based approaches.

Machine learning models are capable of recognizing patterns associated with malicious behaviour and can support faster threat identification. Research findings indicate that AI-driven intrusion detection systems

provide better performance in detecting cyber threats while improving overall response efficiency. Deep learning techniques are particularly effective in identifying complex attack patterns that may be difficult to recognize using conventional security methods.



CONCLUSION

The increasing number of cyber threats has created a strong need for advanced security solutions capable of protecting modern digital systems. Conventional security methods are often limited in their ability to identify emerging and sophisticated attacks, making intelligent detection mechanisms more important than ever.

The overall analysis shows that AI-based threat detection systems can enhance the identification of malicious activities, support faster decision-making, and improve the efficiency of cybersecurity defenses. Although challenges such as data quality and evolving attack methods continue to exist, future developments in Artificial Intelligence are expected to further improve the effectiveness of cyber threat detection and contribute to a more secure digital environment.

REFERENCES

- [1] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th Edition, Pearson, 2021.
- [2] W. Stallings, Network Security Essentials: Applications and Standards, Pearson Education, 2022.
- [3] V. Kumar and S. Gupta, "Machine Learning Approaches for Intrusion Detection Systems," International Journal of Cyber Security, vol. 15, no. 2, pp. 45–58, 2023.
- [4] A. Sharma and R. Patel, "Artificial Intelligence in Cybersecurity: Opportunities and Challenges," Journal of Information Security Research, vol. 12, no. 1, pp. 23–36, 2024.
- [5] J. Brown, "Deep Learning Techniques for Network Intrusion Detection," IEEE Access, vol. 11, pp. 10215–10230, 2023.