AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

Cyber Threat Hunting: A Proactive Approach to Network Security

Mr. V Koteswara Rao Pokuri, M.Tech, Assistant Professor, Department of MCA, Bapatla Engineering College Bapatla, pvkr415@gmail.com, ORCID: 0009-0009-1860-3073.

Ms. Vangala Deepika , (Reg No:Y25MC23095), Ms.Palla Venkata Triveni, (Reg No: Y25MC23057)
Mr.Ravipati Sasidhar Reddy, (Reg No: Y25MC23068), Mr.Domari Ashok, (Reg No: Y25MC23017),
Department of MCA, Bapatla Engineering College, Bapatla, Andhra Pradesh, India

***Abstract*—The growth of technologies and connected systems has led to more cyber threats targeting organisational networks. Traditional security tools like firewalls and antivirus software mainly react to threats after they happen. Modern cyber attackers use sneaky techniques that can get past these security controls.**

To tackle these challenges, cyber threat hunting has become an approach to cybersecurity. It focuses on finding hidden threats in network environments before they cause harm.

This paper studies cyber threat hunting as an approach to network security. It looks at using analytics and monitoring systems to detect potential security threats. The approach involves monitoring network activities, analysing system logs and looking at network traffic behaviour to identify suspicious patterns.

By using techniques like anomaly detection, threat intelligence analysis and machine learning-based pattern recognition, security analysts can search for threats within the network. Cyber threat hunting is used to find these threats.

The research also explores how modern technologies like machine learning, artificial intelligence and behavioural analytics improve threat detection. These technologies help analyse amounts of network data, making it easier to spot abnormal behavior unauthorized access attempts and potential security breaches. Threat intelligence, cyber threat hunting and proactive hunting strategies work together to detect threats and sophisticated cyber attacks.

Experimental analysis shows that proactive threat hunting improves network security systems. It reduces detection time minimizes security risks and enhances cybersecurity resilience. The proposed framework helps organizations strengthen their security posture by enabling early threat identification and providing insights for incident response teams.

Overall cyber threat hunting is a strategy, for modern cybersecurity defense. It helps organizations move from reactive security practices to an intelligence-driven security model. This model protects network infrastructures from evolving cyber threats using cyber threat hunting.

Keywords: Cyber Threat Hunting, Network Security, Proactive Cyber Defence, Intrusion Detection, Threat Intelligence, Anomaly Detection

…

I. INTRODUCTION

In today's world, companies are using computer networks, cloud systems and online services more and more to run their businesses, communicate and share data. While these new technologies have a lot of benefits, they also make systems vulnerable to cyber threats and security risks. Cyber attacks like malware, phishing and ransomware have become more complicated and harder to find. Traditional cybersecurity methods, such as firewalls and antivirus systems, are designed to respond to known threats. Modern attackers use sneaky techniques that can avoid these defences. This is why companies need to use proactive security strategies.

To deal with these challenges, Cyber Threat Hunting has become an approach to network security. It is an intelligent way to find hidden threats in network environments before they cause serious damage. Cyber Threat Hunting is different from security systems that only respond after an attack is detected. Instead, it focuses on searching for threats within networks. Cyber Threat Hunting teams use analytical techniques, threat intelligence and behavioural analysis to investigate suspicious activities and identify signs of compromise that may not be detected by automated security tools.

Cyber Threat Hunting involves monitoring network traffic, analysing system logs and examining user behaviours to find abnormal patterns that may indicate malicious activities. Security analysts combine data analysis, machine learning techniques and threat intelligence frameworks to detect emerging threats that bypass traditional detection mechanisms. By investigating anomalies and suspicious behaviours, companies can reduce the time attackers spend in their networks and prevent potential security breaches.

In recent years, the use of artificial intelligence, machine learning and big data analytics has made Cyber Threat Hunting more effective. These technologies enable security teams to analyse large amounts of network data, identify complex attack patterns, and detect anomalies in real time. Machine learning models can automatically learn what normal network

Received: 28-02-2026 | Accepted: 02-04-2026 | Published: 19-04-2026 | www.ajaccm.com

behaviour looks like and flag deviations that may indicate intrusions or malicious activities. This allows companies to identify threats early and respond quickly to security incidents.

Another important part of Cyber Threat Hunting is the use of threat intelligence, which provides information about known attack techniques, threat actors and emerging vulnerabilities. By combining threat intelligence with hunting techniques, companies can strengthen their security posture and anticipate potential attacks before they happen. Additionally, Cyber Threat Hunting helps security teams understand attacker behaviour better and develop effective defence strategies.

The main goal of this research is to explore Cyber Threat Hunting as an approach to network security and analyse its effectiveness in detecting hidden threats in modern network environments. The study looks at Cyber Threat Hunting techniques, data analysis methods and intelligent monitoring systems that can enhance threat detection capabilities. By using Cyber Threat Hunting strategies, companies can significantly improve their ability to detect cyber attacks, reduce response time, and strengthen their overall cybersecurity resilience.

The rest of this paper is organised as follows. Section II reviews related work and existing research on Cyber Threat Hunting and network security. Section III describes the proposed methodology and Cyber Threat Hunting framework. Section IV discusses the results and performance analysis. Finally, Section V concludes the paper and highlights future research directions in proactive cybersecurity defence.

II. LITERATURE SURVEY

The way we communicate and use networks is changing fast. Because of this, cyber threats are getting more complicated and harder to find using security methods. Traditional cybersecurity tools like firewalls and antivirus software mostly look for known threats. However, cyber attackers are continually devising new attack methods, so traditional tools often miss unknown or advanced threats.

This is why researchers are looking for ways to keep networks safe. One of these ways is called cyber threat hunting. It involves looking for hidden threats in network environments.

At first, researchers focused on systems that could detect intruders and prevent them from getting into networks. These systems looked for known attack patterns. They were not very good at finding new or sneaky attacks. So researchers started looking into methods that could detect unusual activities in networks.

Many studies have used anomaly detection techniques to find security threats. These techniques look at network traffic patterns and user behaviour to find activities that're not normal. Machine learning algorithms like Decision Trees and Neural Networks have been used to analyse network data and find activities.

Recent research has also shown that threat intelligence is important for improving cyber threat detection. Threat intelligence is about collecting and analysing information about known cyber threats and vulnerabilities. By using threat intelligence organizations can understand emerging attack patterns. Respond to potential threats.

Another important development in cybersecurity research is the use of behaviour-based threat detection systems. These systems look at user behaviour and network traffic patterns to find actions. They can detect insider threats and abnormal access patterns that traditional security systems may miss.

Some researchers have proposed cyber threat hunting frameworks that combine machine learning, behavioural analysis and threat intelligence. These frameworks involve analysts who actively look for indicators of compromise in network environments. Advanced data analytics tools are used to analyse network data and find patterns associated with cyber attacks.

With these advancements, there are still many challenges in implementing effective cyber threat hunting systems. One of the challenges is the large amount of network data that needs to be analysed. Cyber attackers are also always coming up with ways to attack, and skilled security analysts are needed to interpret threat intelligence.

This research focuses on Cyber Threat Hunting as a way to proactively keep networks safe. It combines monitoring systems, anomaly detection techniques and threat intelligence analysis to improve threat detection capabilities. The goal is to help organisations detect threats, reduce the time attackers spend in networks, and make their cybersecurity stronger.

The proposed approach uses Cyber Threat Hunting to enhance network security. It uses monitoring systems to analyse network data and find suspicious activities. It also uses anomaly detection techniques to find patterns in network traffic. By combining these methods with threat intelligence analysis organizations can detect cyber threats effectively.

Overall, Cyber Threat Hunting is a development in cybersecurity research. It provides an approach to network security, and it can help organisations detect and respond to cyber threats more effectively. By using Cyber Threat Hunting organizations can reduce the risk of cyber attacks. Make their networks more secure.

III. ALGORITHM

The proposed algorithm focuses on proactively identifying hidden cyber threats within network environments by analysing network traffic, system logs, and behavioural patterns. The algorithm integrates threat intelligence, anomaly detection, and machine learning techniques to detect suspicious activities before they evolve into serious cyber attacks.

Algorithm: Proactive Cyber Threat Hunting Framework

Input: Network dataset D containing system logs, network traffic data, user activity records, and threat intelligence information.

Output: Detection of potential cyber threats and classification of network behavior as *Normal Activity* or *Malicious Activity*.

Step 1: Data Collection: Network data is continuously collected from multiple sources including:

- Network traffic logs
- System event logs
- Firewall logs
- User authentication records
- Endpoint activity logs

The collected dataset can be represented as:

$$D = \{N, L, U\} \tag{1}$$

where N represents network traffic data, L represents system log data, and U represents user activity information.

Step 2: Data Preprocessing: Before analysis, the collected data must be cleaned and structured. The preprocessing process includes:

- Removing duplicate or incomplete records
- Normalising network data formats
- Filtering irrelevant events from log data
- Converting textual logs into structured feature representations

Step 3: Feature Extraction: Important security features are extracted from network data, including:

- Packet size and traffic volume
- Source and destination IP addresses
- Protocol types
- Login frequency
- Failed authentication attempts
- User access patterns

The feature vector can be represented as:

$$F = \{f_1, f_2, f_3, \ldots, f_n\} \tag{2}$$

where each f_i represents a network behaviour attribute.

Step 4: Threat Intelligence Integration: Threat intelligence databases are integrated to identify known malicious entities. These databases contain information such as:

- Known malicious IP addresses
- Malware signatures
- Indicators of Compromise (IOCs)

This step allows the system to correlate observed activities with known cyber threats.

Step 5: Anomaly Detection: Machine learning models analyse the extracted features to identify abnormal network behaviours. The prediction function can be represented as:

$$Y = f(F) \tag{3}$$

where F represents the feature vector and Y represents the predicted network behaviour.

If the predicted behaviour deviates significantly from normal patterns, the system flags it as suspicious activity.

Step 6: Threat Correlation and Analysis: Suspicious events are correlated across multiple data sources such as network logs, system logs, and user activity records. This correlation helps identify multi-stage cyber attacks and coordinated malicious activities.

Step 7: Threat Classification: Detected anomalies are classified into different threat categories, including:

- Malware activity
- Unauthorised access attempts
- Insider threats
- Distributed Denial of Service (DDoS) attacks
- Data exfiltration attempts

Step 8: Alert Generation and Response: If malicious activity is detected, the system performs the following actions:

- Generate real-time security alerts
- Notify security analysts or automated defense systems
- Trigger incident response mechanisms

Step 9: Performance Evaluation: The performance of the threat hunting system is evaluated using standard classification metrics.

Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

Precision

$$Precision = \frac{TP}{TP + FP} \tag{5}$$

Recall

$$Recall = \frac{TP}{TP + FN} \tag{6}$$

F1 Score

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{7}$$

Received: 28-02-2026 | Accepted: 02-04-2026 | Published: 19-04-2026 | www.ajaccm.com

where TP , TN , FP , and FN represent true positives, true negatives, false positives, and false negatives, respectively.

The proposed algorithm enables proactive identification of hidden cyber threats, reduces attacker dwell time within networks, and strengthens overall network security.

IV. METHODOLOGY

The methodology of this research focuses on developing a proactive cyber threat hunting framework that enables organisations to detect hidden threats within network environments before they cause significant damage. The proposed methodology integrates network monitoring, log analysis, threat intelligence, anomaly detection, and machine learning techniques to identify suspicious activities and potential cyber attacks. The overall framework consists of several stages, including data collection, preprocessing, feature extraction, anomaly detection, threat correlation, and threat classification.

A. Data Collection

The first stage involves collecting data from multiple sources within the network environment. Modern organisations generate large volumes of data through network devices, servers, and security systems. These data sources provide valuable insights into system activities and network behaviour.

The collected data typically includes:

- Network traffic logs
- Firewall and intrusion detection system logs
- System event logs
- User authentication records
- Endpoint activity data

These datasets help security analysts monitor network activities and identify potential indicators of compromise (IOCs).

B. Data Preprocessing

Raw network data often contains incomplete records, redundant information, and irrelevant events. Therefore, preprocessing is necessary to improve data quality and prepare the dataset for analysis.

The preprocessing process includes:

- Removing duplicate or corrupted records
- Normalising network traffic data
- Filtering irrelevant log entries
- Structuring unorganised log data into analyzable formats

This step ensures that the dataset is clean and suitable for further analysis.

C. Feature Extraction

Feature extraction is performed to identify important attributes that represent network behaviour. These features help distinguish between normal network activity and malicious behaviour.

Common extracted features include:

- Source and destination IP addresses
- Packet size and traffic volume
- Protocol types
- Login frequency and authentication failures
- Data transfer patterns
- Network session duration

These features are represented as a feature vector:

$$F = \{f_1, f_2, f_3, \ldots, f_n\} \quad (8)$$

where f_1, f_2, ..., f_n represent different network activity attributes.

D. Threat Intelligence Integration

Threat intelligence plays a critical role in proactive cyber threat hunting. External threat intelligence sources provide information about known cyber threats, attack techniques, malicious IP addresses, and malware signatures.

By integrating threat intelligence with network monitoring systems, organisations can correlate observed network events with known attack indicators, enabling faster detection of potential threats.

E. Anomaly Detection

Anomaly detection techniques are used to identify unusual network behaviour that may indicate malicious activity. Machine learning algorithms analyse the extracted features and learn patterns associated with normal network operations.

The prediction model can be represented as:

$$Y = f(F) \quad (9)$$

where F represents the feature vector and Y represents the predicted network behaviour.

If the observed behaviour significantly deviates from the learned normal patterns, the system flags it as suspicious activity.

F. Threat Correlation and Investigation

Suspicious activities detected by anomaly detection models are correlated across multiple data sources such as network logs, system logs, and user activity records. This correlation helps identify complex attack patterns and multi-stage cyber

attacks.

Security analysts analyze these correlated events to determine whether the detected anomalies represent genuine cyber threats or false positives.

G. Threat Classification

Once suspicious activities are confirmed, they are classified into different
categories of cyber threats such as:

- Malware infections
- Unauthorized access attempts
- Insider threats
- Distributed Denial of Service (DDoS) attacks
- Data exfiltration attempts

This classification helps security teams prioritise responses and implement appropriate mitigation strategies.

H. Response and Mitigation

After identifying a potential cyber threat, the system generates alerts and triggers incident response procedures. Security teams can take actions
such as:

- Blocking malicious IP addresses
- Isolating compromised systems
- Updating security policies
- Deploying patches or malware removal tools

These responses help prevent further damage and strengthen the overall security posture of the network.

I. Performance Evaluation

The effectiveness of the proposed threat hunting framework is evaluated using performance metrics such as accuracy, precision, recall, and F1-score. These metrics measure the system's ability to correctly detect cyber threats while minimising false positives.

Overall, the proposed methodology enables organisations to transition from reactive cybersecurity practices to a proactive security model, allowing early detection of cyber threats and improving the resilience of the network infrastructures.

V. RESULT ANALYSIS

This section presents the experimental evaluation of the proposed Cyber Threat Hunting framework, which aims to proactively detect malicious activities within network environments. The primary objective of the evaluation is to analyse the effectiveness of the proposed approach in identifying hidden cyber threats through continuous monitoring, anomaly detection, and threat intelligence integration. The system analyses network traffic logs, system event logs, firewall records, and user activity data to identify

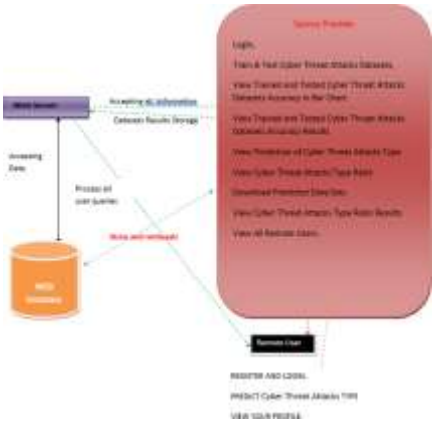

Fig. 1. Architecture Overview

abnormal behaviours that may indicate potential cyber attacks.

To evaluate the performance of the proposed framework, a dataset containing both normal network activities and malicious attack patterns was used. The dataset was divided into two parts: training data (80%) for model learning and testing data (20%) for evaluating detection performance. Various features such as network traffic volume, login frequency, packet size, protocol types, failed authentication attempts, and unusual access patterns were extracted and analysed. These features help distinguish between legitimate user behaviour and malicious activities.

A. Model Performance Evaluation

The performance of the cyber threat hunting framework was evaluated using several standard metrics, including accuracy, precision, recall, and F1-score. These metrics provide a comprehensive understanding of how effectively the system can detect cyber threats while minimising false alarms. The results demonstrate that the proposed framework is capable of identifying suspicious network activities with high accuracy.

The integration of anomaly detection techniques and threat intelligence data significantly improves the detection capability of the system. Anomaly detection helps identify unusual network behaviours that deviate from normal patterns, while threat intelligence provides information about known attack signatures, malicious IP addresses, and indicators of compromise. By combining these techniques, the system can detect both known and unknown threats within the network environment.

B. Accuracy Analysis

Accuracy measures the proportion of correctly classified events among all analysed network activities. It is calculated as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (10)$$

where TP (True Positive) represents correctly detected cyber attacks, TN (True Negative) represents correctly identified normal activities, FP (False Positive) represents normal activities incorrectly flagged as attacks, and FN (False Negative) represents malicious activities that were not detected by the system.

Experimental analysis indicates that the proposed cyber threat hunting model achieves high accuracy in detecting malicious network behaviours, demonstrating its effectiveness in distinguishing between legitimate and suspicious activities.

C. Precision and Recall Analysis

Precision and recall are important metrics for evaluating the reliability of threat detection systems.

$$Precision = \frac{TP}{TP + FP} \quad (11)$$

$$Recall = \frac{TP}{TP + FN} \quad (12)$$

Precision measures the proportion of detected threats that are actually malicious, while recall measures the system's ability to detect all existing cyber threats in the network. The results show that the proposed system maintains high precision and recall values, indicating a strong capability to detect cyber threats while reducing false alarms.

D. F1 Score Evaluation

The F1-score combines precision and recall into a single metric that reflects the overall detection performance of the model.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (13)$$

A higher F1-score indicates better balance between detecting threats and minimising incorrect detections. The proposed cyber threat hunting framework achieves a high F1-score, demonstrating the effectiveness of the combined anomaly detection and threat intelligence approach.

E. Detection of Advanced Cyber Threats

One of the key advantages of the proposed framework is its ability to detect advanced cyber threats such as insider attacks, unauthorised access attempts, malware activities, and distributed denial-of-service (DDoS) attacks. By analysing network behaviour patterns and correlating events from multiple sources, the system can identify suspicious activities that may remain hidden from traditional security tools.

Threat correlation techniques allow the system to detect multi-stage attacks, where attackers perform several actions over time to compromise a network. By analysing relationships between different events, the system provides deeper insights into potential attack scenarios
.

F. Comparative Analysis

A comparative analysis between the proposed cyber threat hunting framework and traditional reactive security mechanisms, such as signature-based intrusion detection systems, shows that the proposed approach provides significantly improved detection capabilities. Traditional systems mainly detect known threats, whereas the proposed framework can detect previously unknown threats and abnormal behaviours through anomaly detection and proactive investigation.

G. Overall System Effectiveness

The experimental results demonstrate that the proposed cyber threat hunting approach enhances network security by enabling early detection of cyber threats and reducing the time attackers remain undetected within a network. Continuous monitoring, intelligent analysis of network logs, and integration of threat intelligence help security teams quickly identify suspicious activities and take preventive actions.

Overall, the results confirm that cyber threat hunting is an effective proactive cybersecurity strategy that improves threat detection accuracy, reduces false alarms, and strengthens the resilience of modern network infrastructures against evolving cyber attacks.

Visualization and Output:

Fig. 2. wed page

VI. CONCLUSION

In this survey, we provided a detailed review of the most significant works on CTI mining that have been published so far. In our paper, we proposed a classification scheme for organizing and categorizing existing research

Fig. 3. login page

Fig. 4. value

works on the basis of the purposes of CTI knowledge acquisition, and we highlighted the methodology adopted by the existing studies. In accordance with the proposed classification scheme, we thoroughly review and discuss current works, including cybersecurity related entities and events, cyber attack tactics, techniques and procedures, profiles of hackers, indicators of compromise, vulnerability exploits and malware implementation, and threat hunting. Furthermore, we discussed current challenges and promising future research directions. Over the past several decades, there has been tremendous interest in CTI mining, specifically for proactive cybersecurity defense. Many people have come to the attention that an enormous number of new techniques and models are developed every year. Hopefully, this survey helps readers understand the critical aspects of this field, clarifies the most notable advances, and sheds light on future research.

REFERENCES

[1]] Liu, Jieling, et al. ”Deception Maze: A Stackelberg Game-Theoretic Defense Mechanism for Intranet Threats.” ICC 2021-IEEE International Conference on Communications. IEEE, 2021.

[2] Wang, Xiaoyu, et al. ”MAAC: Novel alert correlation method to detect multi-step attack.” 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, 2021.

[3] Liu, Zhijie, Chongjun Wang, and Shifu Chen. ”Correlating multi-step attack and constructing attack scenarios based on attack pattern modeling.” 2008 International Conference on Information Security and Assurance (ISA 2008). IEEE, 2008.

[4] Stafford, V. A. ”Zero trust architecture.” NIST special publication 800 (2020): 207.

[5] Chen, Ping, Lieven Desmet, and Christophe Huygens. ”A study on advanced persistent threats.” Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15. Springer Berlin Heidelberg, 2014.

Fig. 5. Prediced value

[6] Cho, Byeong-joo, Jang-ho Yun, and Kyeong-ho Lee. ”Study of effectiveness for the network separation policy of financial companies.” Journal of the Korea Institute of Information Security Cryptology 25.1 (2015): 181-195.

[7] Bagui, Sikha, et al. ”Detecting reconnaissance and discovery tactics from the MITRE ATTCK framework in Zeek Conn Logs using Spark’s machine learning in the big data framework.” Sensors 22.20 (2022): 7999.