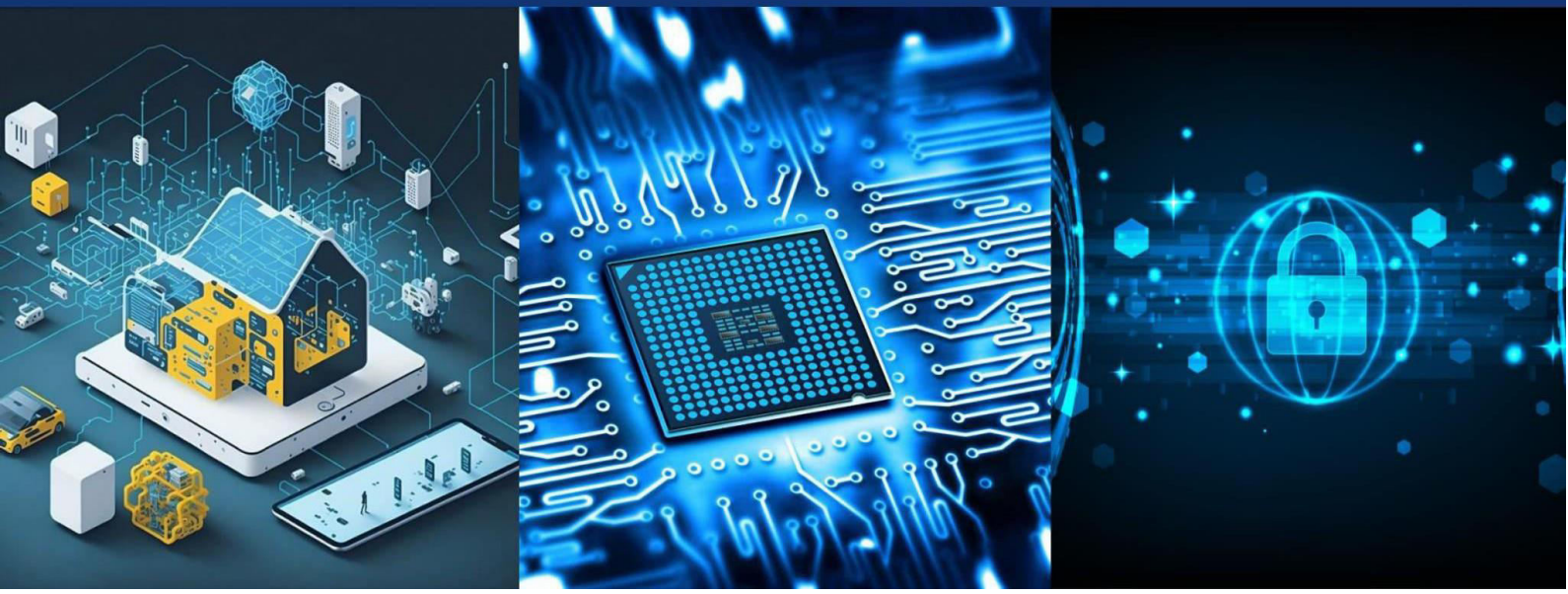
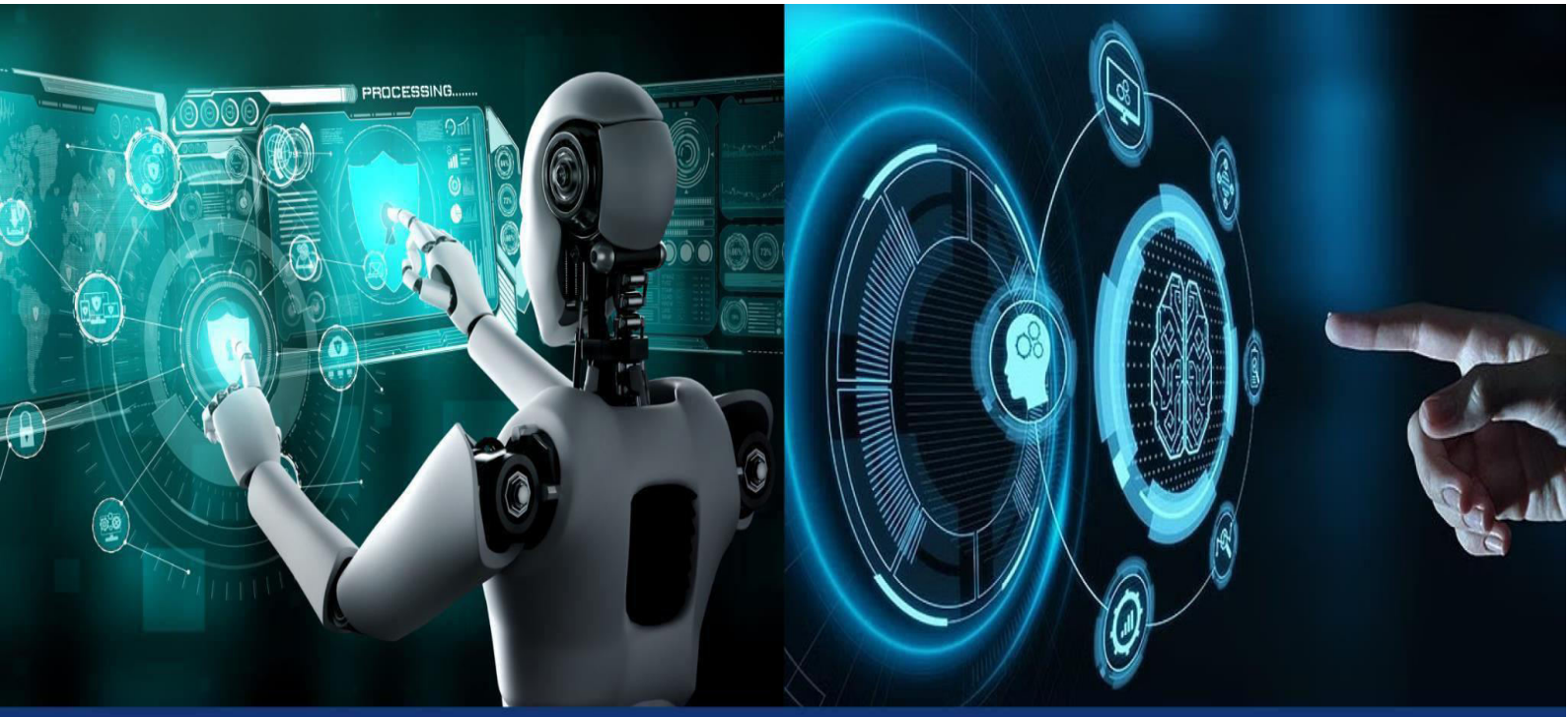
ISSN(O): 2320-9801
ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

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



Impact Factor: 8.771 **Volume 14, Issue 1, January 2026**

© 2026 IJIRCCE | Volume 14, Issue 1, January 2026| DOI:10.15680/IJIRCCE.2026.1401086

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

Automated Cyber Threat Intelligence using Artificial Intelligence

Mrs. Sujata Sachin Albhar

Assistant Professor, MCA, Siddhant Institute of Computer Application, Sudumbare Pune, India

ABSTRACT: The rapid expansion of digital systems has significantly increased exposure to cyber threats. Conventional security mechanisms often struggle to detect modern, sophisticated attacks in a timely manner. This research proposes an automated Cyber Threat Intelligence (CTI) system that leverages Artificial Intelligence (AI) to enhance threat detection, analysis, and response.

The suggested framework integrates machine learning, deep learning, and natural language processing techniques to support the complete lifecycle of threat intelligence—from data collection to automated mitigation. Convolutional Neural Networks are used to identify patterns in network traffic, Long Short-Term Memory models help detect abnormal behavioral sequences, and transformer-based models analyze unstructured threat information.

Experimental evaluation conducted on widely accepted cybersecurity datasets demonstrates strong performance, achieving detection accuracy close to 97% while improving precision and recall compared to traditional models. The study also considers scalability and real-time deployment challenges in enterprise environments. Overall, the research highlights the potential of AI-driven automation in strengthening cybersecurity defenses and minimizing response time.

KEYWORDS: Cyber Threat Intelligence, Artificial Intelligence, Machine Learning, Deep Learning, Network Security, Threat Detection.

I. INTRODUCTION

The dependence on digital technologies has grown rapidly across industries, making cyber security a critical concern for organizations worldwide. Modern cyber attacks are becoming more advanced, including ransomware, phishing campaigns, zero-day vulnerabilities, and advanced persistent threats. These attacks can lead to financial losses, data breaches, and operational disruptions.

Traditional cyber threat intelligence methods rely heavily on manual analysis performed by security professionals. Analysts must gather data from multiple sources such as system logs, threat feeds, and security reports. However, the enormous volume of data generated daily makes manual processing inefficient and prone to delays.

Artificial Intelligence offers a promising solution by enabling automated threat detection and faster decision-making. AI-based systems can analyze large datasets, recognize hidden patterns, and respond to threats in real time.

This research introduces an AI-driven CTI framework designed to automate major intelligence processes, including:

- Collecting threat data from multiple sources
- Cleaning and preparing data for analysis
- Detecting malicious activities
- Correlating related threats
- Generating automated responses

Objectives of the Study

- To design a scalable architecture for automated cyber threat intelligence.
- To improve detection accuracy using AI techniques.
- To evaluate the framework using benchmark datasets.
- To explore future possibilities for intelligent cyber security systems.

© 2026 IJIRCCE | Volume 14, Issue 1, January 2026| DOI:10.15680/IJIRCCE.2026.1401086

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

II. RELATED WORK

Researchers have increasingly explored the role of AI in cyber security. Early studies focused primarily on intrusion detection systems that applied machine learning algorithms such as Support Vector Machines and Random Forests to identify abnormal network behavior. While these methods improved detection rates, they often produced high false alarms in dynamic environments.

Deep learning approaches later gained popularity due to their ability to process complex data. Convolutional Neural Networks have been applied to malware detection, while recurrent neural networks have proven effective in analyzing sequential network activities. Similarly, natural language processing models have been used to extract useful intelligence from security reports.

Despite these advancements, many existing solutions address isolated tasks rather than providing a unified intelligence system. Few frameworks combine detection, correlation, and automated response into a single architecture. This research attempts to bridge that gap by proposing an integrated AI-based CTI model.

III. PROPOSED ARCHITECTURE

The proposed system follows a modular architecture that supports flexibility and scalability. It consists of five primary components:

3.1 Data Collection Module

This module gathers threat-related information from diverse sources such as network logs, threat intelligence platforms, open-source databases, and security reports. High-throughput tools ensure that large volumes of data can be processed efficiently.

3.2 Data Preprocessing Module

Raw data often contains inconsistencies and irrelevant information. Therefore, preprocessing techniques such as normalization, noise removal, and feature extraction are applied. Text data is tokenized and converted into embeddings, while network packets are transformed into structured features.

3.3 AI-Based Detection Module

This is the core of the framework. Multiple AI models operate together:

- **CNN:** Extracts spatial patterns from network traffic.
- **LSTM:** Detects unusual sequences that may indicate attacks.
- **NLP Models:** Classify textual threat reports.

Combining these models increases reliability and reduces detection errors.

3.4 Threat Correlation Module

Detected threats are analyzed to identify relationships between events. Graph-based techniques help uncover attack chains, enabling better situational awareness.

3.5 Automated Response Module

Once a threat is confirmed, the system can trigger alerts, update firewall rules, or recommend mitigation strategies. Human oversight remains available for critical decisions.

The framework is implemented using Python-based libraries and can be deployed in cloud environments for large-scale operations.

IV. MATHEMATICAL MODEL

Let the collected dataset be represented as **D**, containing multiple threat instances. A feature extraction function transforms raw data into a structured feature space suitable for machine learning models.

The classifier predicts whether an activity is malicious or normal. A sigmoid function converts model outputs into probability scores, enabling binary classification.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

To improve prediction quality, the system minimizes binary cross-entropy loss during training. Optimization algorithms such as Adam help adjust model parameters efficiently. Techniques like dropout are applied to prevent overfitting, ensuring that the model performs well on unseen data.

Additionally, focal loss is incorporated to address class imbalance, a common issue where malicious samples are fewer than normal ones.

V. DATASET DESCRIPTION

The framework is evaluated using two widely recognized datasets:

- **CICIDS2017:** Contains millions of network records representing real-world attack scenarios.
- **UNSW-NB15:** Includes modern attack simulations with multiple network features.

Data Preparation Steps:

- Scaling numerical values for consistency
- Removing outliers
- Reducing dimensionality using Principal Component Analysis
- Balancing classes through oversampling

The dataset is divided into training, validation, and testing subsets to ensure reliable evaluation.

VI. EVALUATION METRICS

System performance is measured using standard classification metrics:

- **Accuracy:** Overall correctness of predictions
- **Precision:** Reliability of detected threats
- **Recall:** Ability to identify actual attacks
- **F1-Score:** Balance between precision and recall
- **Latency:** Time required to detect threats

These metrics provide a comprehensive understanding of the model's effectiveness.

VII. RESULTS AND DISCUSSION

Experimental testing indicates that the proposed AI-based CTI framework performs better than several traditional models.

Model	Accuracy	Precision	Recall	Latency
SVM	88%	0.86	0.85	Higher
Random Forest	91%	0.89	0.90	Moderate
LSTM	94%	0.93	0.92	Lower
Proposed AI-CTI	**97%**	**0.96**	**0.97**	**Very Low**

The improvement is largely due to multi-model integration and better handling of complex attack patterns. Reduced latency also makes the system suitable for real-time deployment.

Limitations

- Dataset bias may affect generalization.
- Deep learning models require significant computational resources.

Nevertheless, the results confirm the effectiveness of AI in automated threat intelligence.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

VIII. CONCLUSION AND FUTURE WORK

This research demonstrates that integrating Artificial Intelligence into cyber threat intelligence significantly improves detection capability, operational speed, and scalability. The proposed framework successfully automates key intelligence processes and outperforms conventional techniques.

Future Enhancements:

- Incorporating explainable AI to improve transparency
- Enabling secure intelligence sharing through federated learning
- Exploring blockchain for tamper-proof threat storage
- Developing quantum-resistant security mechanisms

AI-driven cybersecurity solutions are expected to play a vital role in protecting digital infrastructure against evolving threats.

REFERENCES

[1] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.
[2] M. Conti, T. D. Nguyen, and B. Crispo, "Cyber threat intelligence," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2921-2956, 2018.
[3] NIST, "Guide to Cyber Threat Intelligence," Special Publication 800-150, 2022.
[4] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy*, 2018, pp. 108-116.
[5] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems," in *Proc. Mil. Commun. Inf. Syst. Conf.*, 2015, pp. 1-6.
[6] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Comput. Secur.*, vol. 28, no. 1-2, pp. 18-28, 2009.
[7] J. Kim, S. Kim, H. Kim, and M. Kim, "CNN-based malware detection using malware images," in *Proc. Int. Conf. Inf. Secur. Appl.*, 2016, pp. 71-76.
[8] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954-21961, 2017.
[9] G. Husari, E. Al-Shaer, M. Ahmed, B. Chu, and X. Niu, "TTPDrill: Automatic and accurate extraction of threat actions from unstructured text of CTI sources," in *Proc. 33rd Annu. Comput. Secur. Appl. Conf.*, 2018, pp. 103-115.
[10] T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," *IEEE Signal Process. Mag.*, vol. 37, no. 3, pp. 50-60, 2020.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details