International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 6, Nov-Dec-2026, ISSN (Online): 2395-566X

AI-Based Holistic Framework for Cyber Threat Intelligence Management

Gunjal Harshada Rajendra
Department Of Artificial Intelligence And Machine Learning
Sahyadri Valley College Of Engineering And Technology, Affiliated To Sppu, India E-Mail: Harshadagunjal2006@Gmail.Com

Abstract— Cyber Threat Intelligence (CTI) helps organisations understand cyber risks and prepare suitable defensive actions. However, threat information is often collected from many disconnected sources and may contain irrelevant, duplicated, or unverified data. This paper presents a review-oriented study of an AI-based holistic approach to CTI management. It discusses the complete CTI lifecycle, including data collection, filtering, extraction, classification, correlation, enrichment, storage, analysis, and secure sharing. Artificial Intelligence (AI) and Machine Learning (ML) techniques such as Natural Language Processing, Named Entity Recognition, text classification, anomaly detection, and similarity analysis can help convert large volumes of raw information into actionable intelligence. The study also reviews the role of platforms and standards such as MISP, STIX, TAXII, and MITRE ATT&CK; in organising and exchanging threat information. A conceptual framework is described to show how internal and external data sources can be integrated while maintaining privacy, data quality, and analyst oversight. The paper is based on published literature and standards; it does not claim a newly implemented system or measured experimental results. The review highlights that AI can improve the speed and consistency of CTI operations, but reliable deployment requires validation, secure data handling, explainability, and continuous human supervision.

Keywords— Cyber Threat Intelligence, Artificial Intelligence, Machine Learning, Threat Detection, Data Classification, Threat Correlation, STIX, TAXII, MISP.

I. INTRODUCTION

The rapid growth of digital services, cloud platforms, Internet of Things (IoT) devices, and interconnected networks has increased the attack surface of modern organisations. Cyber attackers use techniques such as phishing, malware, credential theft, ransomware, exploitation of vulnerabilities, and supply-chain attacks. Traditional security tools generate large amounts of alerts and logs, but these records do not always explain who is attacking, how the attack is being performed, or what action should be taken.

Cyber Threat Intelligence (CTI) is the process of collecting, processing, analysing, and sharing information about threats, threat actors, vulnerabilities, and attack behaviour. Useful CTI converts raw observations into contextual and actionable knowledge. It supports security teams in prioritising risks, improving detection rules, preparing incident response, and making informed security decisions [1], [2].

An AI-based holistic framework aims to manage the complete CTI lifecycle rather than performing only one task such as indicator collection. AI can assist in filtering irrelevant content, extracting threat entities, identifying relationships between events, and detecting unusual patterns. The objective of this paper is to explain the main components of such a framework, review the enabling technologies, and identify its benefits and limitations.

II. REVIEW OF RELATED WORK

Research on CTI management has explored threat information collection, structured representation, automated sharing, and intelligent analysis. Spyros et al. proposed ThreatWise AI, a holistic framework that integrates collection, extraction, classification, correlation, storage, enrichment, and sharing of CTI. Their work describes the use of internal security data, external web sources, AI/ML methods, and a MISP-based platform [1].

The OASIS Cyber Threat Intelligence standards define STIX as a structured language for representing cyber threat information and TAXII as a protocol for exchanging that information between systems [2], [3]. These standards support machine-readable sharing and interoperability. MITRE ATT&CK; provides a knowledge base of adversary tactics and techniques that can be used to interpret observed behaviour and map events to known attack patterns [4].

Existing studies indicate that automated collection alone is insufficient. Information must be filtered, validated, contextualised, and correlated before it can support operational decisions. AI-based classification and entity extraction can assist analysts, while sharing standards help different security tools exchange consistent information. The reviewed literature therefore supports an integrated lifecycle approach instead of isolated tools.

© 2026 IJSRET

III. RESEARCH METHODOLOGY

This paper follows a literature-review methodology. Published research articles, technical standards, and cybersecurity framework documentation related to CTI management were examined. Priority was given to material describing AI-assisted threat collection, classification, entity extraction, correlation, CTI platforms, and information-sharing standards.

The reviewed material was organised into five themes: (1) CTI sources and collection, (2) AI-based extraction and classification, (3) threat correlation and enrichment, (4) storage and information sharing, and (5) security, challenges, and future scope. The proposed framework in this paper is conceptual and review-based. No new dataset, prototype implementation, or experimental performance values are claimed.

1. Ai-Based Holistic Cti Framework

A holistic CTI framework combines multiple stages into one connected workflow. The system receives information from internal and external sources, processes the data using rule-based and AI-based methods, stores structured intelligence, and shares validated results with authorised security teams and partner organisations.

2. Data Collection

Internal sources include firewall logs, server and application logs, endpoint detection alerts, IDS/IPS events, SIEM records, and honeypot activity. External sources include CERT/CSIRT advisories, vulnerability databases, threat feeds, security blogs, malware repositories, and relevant public reports. Combining both source types provides local context as well as information about the wider threat landscape [1].

3. Data Filtering And Privacy Protection

Collected data may contain duplicated records, unrelated content, and personally identifiable information (PII). Pre-processing removes noise, normalises formats, checks timestamps, and applies privacy rules. Access to sensitive information should be restricted, and PII should be minimised or removed when it is not necessary for cybersecurity analysis.

4. Ai-Based Extraction And Classification

Natural Language Processing (NLP) can identify threat-related content in reports, advisories, and online discussions. Named Entity Recognition (NER) can extract entities such as IP addresses, domain names, file hashes, malware names, threat actors, and vulnerabilities. Machine-learning classifiers can label documents as CTI-related, general cybersecurity information, or irrelevant content. Multi-label classification can further associate intelligence with sectors such as healthcare, finance, energy, or transportation [1].

5. Correlation And Enrichment

Correlation links indicators and events that may belong to the same campaign or attacker activity. Simple correlation can identify repeated values, such as a common IP address or domain. Advanced correlation can compare multiple attributes, text similarity, timing, and behavioural features. AI-based anomaly detection can highlight unusual activity for analyst review. Enrichment adds context such as related malware, known vulnerabilities, threat actor information, and mapped MITRE ATT&CK; techniques.

6. Storage And Knowledge Management

A CTI repository stores validated indicators, reports, relationships, confidence levels, timestamps, and source references. Platforms such as MISP can support collection, correlation, event management, and sharing. Structured records improve searchability, reduce duplication, and help analysts trace the origin of an intelligence item [1], [5].

7. Sharing And Response

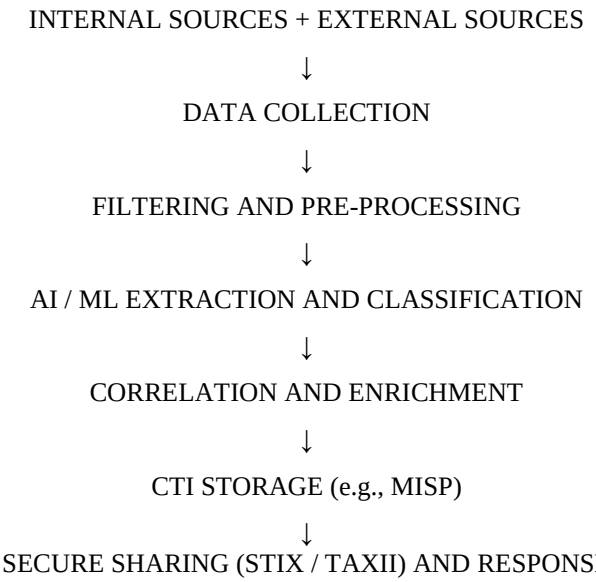


Fig. 1. Conceptual workflow of an AI-based holistic CTI management framework.

Validated intelligence can be shared with internal security tools, incident response teams, and trusted external partners. STIX provides a structured way to represent CTI, while TAXII supports its exchange through standardised services [2], [3]. Sharing policies should define permitted recipients,

© 2026 IJSRET

sensitivity labels, retention periods, and approval requirements. Relevant indicators and techniques can then support detection rules, blocking decisions, vulnerability prioritisation, and incident response.

IV. KEY AI AND CYBERSECURITY TECHNOLOGIES

1. Natural Language Processing
NLP processes unstructured text from advisories, reports, and threat feeds. It helps identify relevant sentences, classify documents, and extract security-related entities. Transformer-based language models can capture context, but their outputs must be checked for incorrect or misleading interpretations.

2. Named Entity Recognition
NER identifies and categorises important terms in text, including malware families, organisations, vulnerabilities, IP addresses, and domains. Extracted entities can be converted into structured CTI records and linked with existing knowledge.

3. Machine Learning Classification
Supervised models can classify documents or events using labelled examples. Unsupervised methods can group similar reports or detect patterns without relying on a complete set of labels. Model selection depends on data quality, available training examples, and the cost of false alerts.

4. Anomaly Detection And Similarity Analysis
Anomaly detection identifies activity that differs from normal system behaviour. Similarity analysis compares reports or indicators to find repeated or related threat information. These techniques can reduce manual effort, but unusual activity does not automatically prove that an attack has occurred.

V. APPLICATIONS OF AI-BASED CTI

1. Enterprise Security Operations
Security Operations Centres (SOCs) can use enriched CTI to prioritise alerts, identify related incidents, and improve the context available to analysts.

2.Critical Infrastructure Protection
Energy, transport, healthcare, and industrial organisations can combine operational logs with external threat intelligence to understand risks to essential services.

3. Financial Services
Banks and financial platforms can use threat feeds and behavioural analytics to investigate phishing infrastructure, malware campaigns, and suspicious access patterns.

4. Incident Response And Vulnerability Management
CTI can help response teams identify affected assets, understand attacker techniques, prioritise exposed vulnerabilities, and select suitable containment actions.

VI. BENEFITS AND CHALLENGES

1. Benefits
An integrated framework can reduce manual collection and repetitive analysis. AI-based classification and extraction can process large volumes of information, while correlation adds context to isolated indicators. Standardised formats can improve interoperability and support faster information exchange. A shared CTI repository also helps teams maintain a common understanding of threats.

2. Challenges
The quality of AI output depends on the quality, freshness, and representativeness of training and source data. False positives may overload analysts, while false negatives may hide relevant threats. Adversaries can change infrastructure and behaviour to evade detection. Data sharing raises privacy, confidentiality, and trust concerns. Integration across different tools, formats, and organisations can also be difficult. Human review, explainability, access control, and secure updates remain important requirements.

3. Future Scope
Future work can explore explainable AI to make threat classifications and correlations easier to understand. Privacy-preserving collaboration may allow organisations to share useful intelligence without exposing unnecessary sensitive data. Graph-based learning can help model relationships among threat actors, infrastructure, malware, and campaigns. Continual learning may help systems adapt to changing attack patterns, provided that model drift and poisoning risks are carefully managed. Further research is also needed on reliable evaluation metrics, interoperability, multilingual threat reports, and analyst-centred interfaces.

VII. CONCLUSION

AI-based holistic Cyber Threat Intelligence management provides an integrated way to transform large volumes of security information into structured and actionable knowledge. The lifecycle includes collection, filtering, extraction, classification, correlation, enrichment, storage,

© 2026 IJSRET

and secure sharing. NLP, NER, machine learning, and anomaly detection can assist analysts in identifying relevant information and connecting related threat events. Standards such as STIX and TAXII and platforms such as MISP support consistent representation and exchange of intelligence. However, AI should support rather than replace security experts. Data quality, privacy, explainability, validation, and human oversight are essential for building a trustworthy CTI management process. This paper is a literature-based review and does not claim experimental validation of a new system.

REFERENCES

1. A. Spyros, I. Koritsas, A. Papoutsis, P. Panagiotou, D. Chatzakou, D. Kavallieros, T. Tsirika, S. Vrochidis, and I. Kompatsiaris, "AI-Based Holistic Framework for Cyber Threat Intelligence Management," IEEE Access, vol. 13, pp. 20820–20846, 2025, doi: 10.1109/ACCESS.2025.3533084.
2. OASIS Open, "STIX Version 2.1," OASIS Committee Specification 03, 21 May 2021. [Online]. Available: https://docs.oasis-open.org/cti/stix/v2.1/cs03/stix-v2.1-cs03.html
3. OASIS Open, "TAXII Version 2.1," OASIS Cyber Threat Intelligence Technical Committee. [Online]. Available: https://oasis-open.github.io/cti-documentation/
4. MITRE, "MITRE ATT&CK;: Knowledge Base of Adversary Tactics and Techniques." [Online]. Available: https://attack.mitre.org/
5. MISP Project, "MISP—Open Source Threat Intelligence Platform." [Online]. Available: https://www.misp-project.org/
6. Cybersecurity and Infrastructure Security Agency (CISA), "Automated Indicator Sharing (AIS) 2.0 Submission Guide," 2023..

© 2026 IJSRET