Journal of Universal Computer Science, vol. 31, no. 10 (2025), 1102-1129
submitted: 20/9/2024, accepted: 20/2/2025, appeared: 28/8/2025 CC BY 4.0

Advancing the Threat Intelligence with AI: An Overview, Taxonomy and Roadmap

Igor Tomičić
(Faculty of Organization and Informatics, University of Zagreb, Varaždin, Croatia
https://orcid.org/0000-0002-8626-9507, igor.tomicic@foi.hr)

Petra Grd
(Faculty of Organization and Informatics, University of Zagreb, Varaždin, Croatia
https://orcid.org/0000-0003-3530-5851, petra.grd@foi.hr)

Andrija Bernik
(University North, Varaždin, Croatia
https://orcid.org/0000-0002-2507-9494, abernik@unin.hr)

Abstract: This paper presents a comprehensive analysis of the integration of artificial intelligence (AI) into threat intelligence (TI) systems, focusing on its potential to enhance cybersecurity operations. The paper presents an extensive literature review, covering the current state of AI applications in TI, including machine learning, deep learning, and natural language processing for automating threat detection, classification, and analysis. It outlines the core functions of AI in TI, such as threat detection, correlation, prediction, and automated response, and introduces a detailed taxonomy categorizing AI techniques based on their roles in enhancing TI processes. Additionally, the paper proposes a conceptual workflow for AI-powered TI, illustrating how AI can streamline data collection, threat analysis, and incident response. A roadmap for future research is further provided, highlighting key areas for development, including explainable AI, federated learning, and edge computing. This work contributes to the field by offering a structured framework for integrating AI into TI and identifying critical challenges and future directions in AI-driven cybersecurity.

Keywords: Artificial Intelligence, Cybersecurity, Threat Intelligence, Threat Detection, Incident Response, SOC
Categories: I.2.6, I.2.7, K.6.5, H.3.3, C.2.0, I.5.1
DOI: 10.3897/jucs.137544

1 Introduction

In the face of escalating cyber threats, organizations are increasingly reliant on threat intelligence — a systematic approach to identifying, collecting, processing, and analyzing potential threat data. This process is crucial for understanding specific threats within an organizational context, enabling informed, data-driven, and proactive security decisions. However, the sheer volume of data generated by numerous cyber attacks presents a significant challenge, potentially overwhelming an organization's resources.

The challenge lies not only in the volume of data but also in its complexity and the speed at which it must be analyzed to be effective. Herein lies the potential of AI: its ability to interrogate large datasets, contextualize information, and construct narratives

that are not only coherent but also highly relevant to an organization's unique security needs.

Traditional threat intelligence (TI) without AI relies heavily on manual analysis, rule-based detection systems, and signature-based threat identification, such as SIEM platforms and threat feeds curated by analysts. While these approaches provide structured threat data, they struggle with scalability, real-time adaptability, and detecting novel threats, often leading to alert fatigue, delayed threat response, and high false positive rates. Integrating AI into TI addresses these limitations by automating data correlation, enhancing predictive threat detection, and dynamically adapting to emerging attack patterns, significantly improving both efficiency and accuracy in cybersecurity operations.

Recent research in the field has begun to shed light on the capabilities of AI in enhancing threat intelligence frameworks. Various studies, presented in the following section, discuss the integration of machine learning, deep learning, and natural language processing in automating threat detection, analysis, and response. These technologies can significantly accelerate the identification of emerging threats, refine the accuracy of threat assessments, and facilitate a more dynamic adaptation to the ever-changing cyber threat landscape.

Furthermore, the application of AI in threat intelligence is not merely about automating existing processes; it also involves the creation of more sophisticated, predictive models of threat behavior. This predictive capability allows organizations to shift from a reactive security posture to a more anticipatory stance, potentially identifying and mitigating threats before they materialize.

As this paper deep-dives into the state-of-the-art research in AI development within the threat intelligence domain, it aims to answer critical questions about the efficacy, challenges, and future directions of AI-powered threat intelligence. By analyzing contemporary research and developments, this study seeks to provide a comprehensive overview of how AI can revolutionize the way organizations understand, anticipate, and neutralize cyber threats, thereby fortifying their defenses in an increasingly volatile digital world.

2 Literature Overview

2.1 AI-Based Frameworks for Data Acquisition and Threat Intelligence

Several works propose AI-based frameworks to automate the gathering and analysis of threat intelligence. [Mittal et al., 2019] introduces a system leveraging Vectorized Knowledge Graphs (VKG) for representing cybersecurity information, neural network models to enhance the knowledge base, and a query engine for actionable insights. Experiments show that VKG improves knowledge representation and helps prevent cyber threats. Observing that existing research rarely employs fully automated data acquisition (e.g., Web Scraping, Entity Detection, Sentiment Analysis), [Sufi, 2023] develops a global AI-based system that autonomously collects cyber-attack data and social media posts, then applies CNN and other AI algorithms for real-time threat detection. INTIME [Koloveas et al., 2021] similarly automates data collection (web crawling, scraping, social media monitoring) and ranks content for relevance, then uses ML algorithms (SVM, Random Forest, Naive Bayes, CNN) to produce actionable intelligence. Other approaches focus on NLP for analyzing unstructured threat sources: [Ghazi et al., 2018] achieves around 70% precision in generating comprehensive threat reports, while [Hassan et al., 2019, Aminanto et al., 2019] demonstrate that AI-based techniques can reduce irrelevant alerts, mitigating analyst fatigue.

2.2 Credibility, Data Poisoning, and Pitfalls in ML-Based Security

Given that AI systems ingest data from unverified sources, [Khurana et al., 2019] proposes an ensembled semi-supervised model to assess the credibility of Reddit posts in the cybersecurity domain, reaching a 71.73% accuracy and outperforming random assessments by 21%. Data poisoning threats are highlighted in [Ranade et al., 2021], where a fine-tuned GPT-2 model can produce realistic but fake CTI, underscoring the need for robust defenses against AI-generated misinformation. Further illustrating potential weaknesses in ML-based security, [Quiring et al., 2022] analyzes top-tier security papers and identifies pitfalls such as sampling bias and label inaccuracy, emphasizing that misapplication of ML can lead to unreliable threat intelligence.

2.3 ML-Based Threat Intelligence Sharing and Advanced Representation

Beyond data ingestion, machine learning models themselves can be disseminated as CTI. [Preuveneers and Joosen, 2021] presents a framework integrating ML with platforms like MISP and Cortex, aiming to reduce false positives and adversarial ML threats through shared models protected by Ciphertext-Policy Attribute-Based Encryption. Similarly, [Nguyen et al., 2022] introduces CTI4AI, a prototype system relying on DARPA's GARD toolkit for identifying AI vulnerabilities. It encapsulates threats within a specialized STIX-based object, Artificial Intelligence Threat Information (AITI), for distribution via TAXII.

2.4 Dark Web and Hacker Forums

Mining dark web and hacker forums reveals substantial intelligence on exploits, malware, and emerging tactics. [Zenebe, 2022] uses ML (SVM and ANN) to predict exploit types based on dark web forum posts, finding function-based algorithms more accurate than tree-based ones. [Kadoguchi et al., 2019] extracts threat intelligence by applying doc2vec and an MLP classifier to identify malware offers, while [Deliu et al., 2017] compares CNN and SVM for classifying hacker forum content, concluding that simpler methods like SVM can match CNN's accuracy. [Nunes et al., 2016] uses supervised and semi-supervised learning (Naive Bayes, RF, SVM, Logistic Regression) to detect malicious hacking products and topics in online marketplaces, providing early warnings. Additional studies enhance this approach with topic modeling and clustering. [Hossen et al., 2021] applies ML classifiers and LDA/NMF to hacker forums for multi-class CTI generation, and [Adewopo et al., 2020] combines doc2vec with deep clustering to categorize forum posts without manual labels, aiding proactive defense.

2.5 Threat Intelligence in Industrial Control Systems (ICS)

Industrial environments require specialized defense models. [Dang et al., 2023] employs a deep neural network-based quality assessment to extract high-quality threat intelligence for ICS, using custom matching to forecast attack actions and an attack-defense game theory framework with mixed-strategy Nash equilibrium. A machine learning-based method for detecting Indicators of Compromise (IoCs) in ICS network traffic is presented in [Atluri and Horne, 2021], using nine ML algorithms, including ensemble methods that achieve over 94% testing accuracy. Both studies demonstrate the potential of ML to boost ICS defense through proactive attack prediction.

2.6 Automated CTI Classification, IoT, and Network-Based Threat Detection

Mapping unstructured CTI to structured attack techniques can improve proactive security. [Orbinato et al., 2022] introduces two datasets and assesses ML models (SecureBERT, MLP, SVM, Logistic Regression, CNN), finding SecureBERT most effective for CTI classification. [Dutta and Kant, 2020] argues for integrating AI and ML with traditional signature-based intrusion detection (IDS, SIEM), using Naïve Bayes to gather threat intelligence from dark web sources and honeypots. [Mishra et al., 2022] evaluates SVM, RF, KNN, LR, MLP, NB, and DT for DDoS detection in IoT networks, noting RF's 99.94% accuracy, while [Sowinski-Mydlarz et al., 2021] compares SVM, neural networks, and regression models for intrusion detection through packet analysis, with SVM attaining 92% accuracy. [Liang et al., 2019] applies deep reinforcement learning for efficient packet classification, improving classification time by 18% and reducing memory usage by up to 3×.

IoT and WSN-oriented ML solutions are surveyed in [Mamdouh et al., 2018], highlighting SVM's lower complexity for DoS, selective forwarding, and MitM threats. [Raj et al., 2012] uses SVM and NN to detect DoS by analyzing collision and arrival rates, and [Diro and Chilamkurti, 2018] proposes a two-layer deep learning architecture (IoT/fog layers) for decentralized threat detection. [Kaplantzis et al., 2007] focuses on selective forwarding and black hole attacks with a one-class SVM, and [Canedo and Skjellum, 2016] uses ANNs and LSTM for safeguarding node health and communications against MitM. Reinforcement learning techniques also support ongoing threat adaptation [Xiao et al., 2018]. A broad ML-based framework for cybersecurity data science is discussed in [Sarker et al., 2020], recommending incremental and multi-layered learning. For IDS improvement, [Kumar et al., 2012] uses decision trees (C4.5, C5.0) for faster rule matching, while other works compare SVM [Li et al., 2012], KNN [Lin et al., 2015], deep learning [Yin et al., 2017], and ensemble methods [Aburomman and Reaz, 2016].

In addition, [Nazir et al., 2024] describes a framework that integrates blockchain with multiple machine learning models (Random Forest, Decision Tree, Ensemble Learning, LSTM, and CNN) for enhanced IoT security. By fostering a collaborative threat intelligence environment on the IoT23 dataset, it demonstrates improved accuracy and reduced false negatives, highlighting the advantages of jointly leveraging ML and blockchain to strengthen IoT threat detection mechanisms.

2.7 Deep Learning-Enabled Approaches and Specialized Architectures

Deep learning further refines threat detection. [Al-Hawawreh et al., 2020] proposes a Deep Learning-Enabled Threat Intelligence (DLTI) scheme for IoT environments, combining a Deep Stacked Auto-Encoder for pattern extraction and a Gated Recurrent Neural Network for identifying abnormal behaviors. [Rodriguez and Okamura, 2020] focuses on improving real-time data quality through multi-layer keyword filtering, word2vec expansion, and K-means clustering. A machine learning-based tool for attacker identification is explored in [Gossi, 2020], using logistic regression to match new reports with adversary profiles. [Noel, 2021] aligns ML models (Naive Bayes, Logistic Regression, SVC, Random Forest) with MITRE ATT&CK for OSINT-based CTI, reaching 93.65% accuracy. Other work highlights data mining and AI strategies for anomaly detection, including fuzzy logic and K-Means clustering [Gupta et al., 2019]. [Bouchama and Kamal, 2021] also shows improved detection rates using neural networks, SVM, and ensemble algorithms.

Some studies address emerging applications of deep learning and collaborative methods in diverse settings. [Kasman et al., 2023] develops a machine-learning-based sentiment analysis approach to detect cyber threats—particularly Trojan viruses—in news articles, using cosine similarity, TF-IDF, and Bag of Words to build a CTI-driven trend dashboard. Results show growing reports of specific malware incidents, demonstrating the technique's ability to filter real-time threat information.

Further extending deep learning methods to novel environments, [Al-Hawawreh et al., 2024] proposes a threat intelligence framework targeting Ransom Denial of Service (RDoS) in smart satellite-based healthcare networks. By using LSTM for real-time discovery of RDoS behaviors, the model reveals how deep learning can mitigate specialized cyberattacks in emerging network architectures.

2.8 Attack Attribution and Profiling

ML aids attack attribution by reducing manual workload. [Barker, 2020] notes ML's potential for scaling attribution, while [Noor et al., 2019] profiles threat actors using distributional semantics and evaluates multiple classifiers, with Deep Learning Neural Networks achieving 94% accuracy for FinTech threats. Past research on malware-based attribution includes [Rieck et al., 2011, Hodo et al., 2016, Saied et al., 2016, Kang and Kang, 2016], underscoring ML's expanding role in uncovering attackers' strategies.

2.9 Automated IOC Extraction, Correlation, and Next-Generation CTI

Extracting Indicators of Compromise (IOCs) supports rapid response. TIMiner [Zhao et al., 2020] employs a CNN for domain recognition and syntactic methods for IOC extraction, while [Zhu and Dumitras, 2018] combines NLP and multi-class classifiers to categorize thousands of IOCs from security articles. CAVeCTIR [Raptis et al., 2022] applies DBSCAN clustering to correlate CTI reports for connected/autonomous vehicles. [Alsaedi et al., 2022] proposes a two-stage ensemble (Random Forest then MLP) for malicious URL detection, and SeqMask [Ejaz et al., 2022] uses Multi-Instance Learning with semantic attention to identify TTPs without POS tagging. An ontology-based threat analysis integrating Random Forest and Gradient Boosting is offered by [Yeboah-Ofori et al., 2021], achieving about 80% accuracy in supply chain prediction. Meanwhile, [Ranade et al., 2018] introduces an LSTM-based translator for multilingual CTI, surpassing commercial systems in capturing cybersecurity-specific terms.

2.10 LLMs and Large-Scale Cyber Threat Intelligence

Recent works investigate Large Language Models (LLMs) for enhanced CTI. aCTIon [Siracusano et al., 2023] uses GPT-3.5 for entity extraction and relationship identification, and SecurityBERT [Ferrag et al., 2023] adapts BERT for IoT threat detection with privacy-preserving encoding and high attack identification accuracy. AGIR [Perrina et al., 2023] automates CTI reporting by combining template-based NLG with ChatGPT, leveraging STIX graphs to structure threat data. Finally, [Li et al., 2022] presents AttackG, aggregating multiple CTI reports into knowledge graphs to outline attack techniques, and [Kaiser et al., 2023] details AttackDB and the Attack Hypothesis Generator, employing link prediction to infer ATT&CK techniques from observable artifacts.

A further LLM-based contribution, [Kristiansen et al., 2020], introduces CTI-Twitter, which classifies cybersecurity-related tweets using a BERT model alongside LDA or

k-means clustering. This work demonstrates effective filtering and categorization of social media data, thereby expanding the scope of LLMs to real-time threat intelligence from open, user-generated sources.

3 Core Functions of AI in Threat Intelligence

Majority of the existing research seems to suggest that Artificial Intelligence (AI) plays a crucial role in enhancing the capabilities of threat intelligence by automating processes, improving accuracy, and enabling proactive defense mechanisms.

The core functions of AI within the domain of threat intelligence can be categorized into several key areas, each contributing uniquely to the overall cybersecurity posture of organizations and systems (Fig. 1).

3.1 Threat Detection

AI has significantly advanced threat detection by identifying anomalies and malicious activities that traditional methods may overlook. Machine learning algorithms, including Support Vector Machines (SVM), Neural Networks, and ensemble methods, analyze patterns in network traffic, user behavior, and system activities to detect deviations indicative of potential threats.

Various AI techniques have been employed across different domains to enhance cyber threat intelligence. For instance, anomaly detection in network traffic often utilizes ensemble models that combine SVM and k-Nearest Neighbors (k-NN) to improve intrusion detection systems, as demonstrated by Aburomman and Reaz [Aburomman and Reaz, 2016]. Similarly, in Internet of Things (IoT) security, deep learning-based anomaly detection has been effective in protecting resource-constrained devices; Diro and Chilamkurti [Diro and Chilamkurti, 2018] implemented a two-layer deep learning architecture that improved the detection of malicious activities in IoT environments. Beyond these applications, Industrial Control Systems (ICS) also benefit from AI-driven security enhancements—Dang et al. [Dang et al., 2023] developed a model leveraging deep neural networks for high-quality threat intelligence extraction, significantly improving the ability to predict and mitigate cyber attacks.

Across these domains, AI-driven detection mechanisms not only improve the accuracy and efficiency of cyber threat identification but also reduce the burden on human analysts by automating large-scale threat analysis.

3.2 Threat Classification

AI enables the classification of cyber threats into distinct categories, such as malware types, attack techniques, or severity levels, which aids in response prioritization and resource allocation. Machine learning and deep learning models have been widely employed to improve the accuracy and efficiency of threat classification.

One critical application is malicious URL detection, where ensemble learning models have proven effective in distinguishing malicious domains from benign ones. Alsaedi et al. [Alsaedi et al., 2022] developed a two-stage classification system combining Random Forest and Multilayer Perceptron (MLP), significantly reducing false positives and improving detection accuracy. Similarly, deep learning techniques have been explored for automating attack technique mapping, where Orbinato et al. [Orbinato et al., 2022]

utilized various machine learning models, including both traditional algorithms and deep learning approaches, to classify unstructured cyber threat intelligence into specific attack techniques. This approach enhances the efficiency of intelligence processing and cyber threat categorization. Beyond individual attack techniques, cyber threat report analysis has also been enhanced using AI, particularly for extracting and classifying Tactics, Techniques, and Procedures (TTPs). Ejaz et al. [Ejaz et al., 2022] introduced *SeqMask*, a deep learning framework that improves the extraction of TTPs from CTI reports without relying on manual feature engineering, making threat intelligence classification more scalable and automated.

These AI-driven classification methods provide cybersecurity professionals with structured and actionable intelligence, improving threat prioritization and response strategies.

3.3 Threat Correlation and Contextualization

AI enhances cyber threat intelligence by correlating initially disparate data points and enriching them with contextual information, ultimately creating a comprehensive view of the threat landscape. By identifying relationships between different threat entities, AI-driven models help security analysts understand attack chains and assess the broader impact of emerging threats.

One key approach is the use of knowledge graphs, where AI organizes and links cybersecurity information. Mittal et al. [Mittal et al., 2019] introduced *Vectorized Knowledge Graphs (VKG)*, which allow for structured correlation of threat entities, enabling the derivation of actionable insights from complex data relationships. Similarly, social media intelligence has become an essential component of contextualizing cyber threats. Zhao et al. [Zhao et al., 2020] developed *TIMiner*, an AI-driven framework that extracts and categorizes cyber threat intelligence from social media, associating Indicators of Compromise (IoCs) with specific domains to provide enhanced situational awareness. Beyond individual data sources, AI also contributes to threat intelligence aggregation, where multiple intelligence reports are synthesized into a unified threat context. Li et al. [Li et al., 2022] proposed a technique to construct *Technique Knowledge Graphs (TKGs)*, which summarize attack techniques across multiple cyber threat intelligence reports, improving the ability to correlate and contextualize threats for better operational decision-making.

These AI-driven methods significantly improve cybersecurity operations by linking disparate pieces of intelligence, enabling faster detection, investigation, and mitigation of threats.

3.4 Threat Attribution

AI plays a crucial role in cyber threat attribution by analyzing behavioral patterns, attack signatures, and adversary tactics to identify responsible threat actors. By leveraging machine learning and natural language processing techniques, AI can profile attackers based on past activities and predict potential adversaries.

A fundamental application is threat actor profiling, where AI models extract adversary characteristics from intelligence reports. Noor and Hossain [Noor et al., 2019] developed a machine learning-based approach that employs distributional semantics to classify cyber threat actors with high accuracy, improving intelligence-driven attribution. In addition to profiling known actors, AI facilitates adversary identification from cyber

threat reports by comparing new incidents with historical attack data. Gossi et al. [Gossi, 2020] created a machine learning tool that predicts attackers by calculating the similarity of new threat reports to established adversary profiles, streamlining attribution efforts.

Another approach leverages hacker forum analysis to track underground activities and infer attack responsibility. Hossen et al. [Hossen et al., 2021] employed classification and topic modeling techniques on hacker forum data to generate valuable cyber threat intelligence, linking emerging threats to specific groups and attack campaigns. These AI-powered techniques enhance cyber threat attribution by identifying patterns in attacker behaviors, improving response strategies, and enabling more proactive cybersecurity defense measures.

3.5 Predictive Threat Intelligence

AI-driven predictive analytics enables the anticipation of future threats by analyzing historical data and identifying patterns that may indicate emerging attack vectors. By leveraging machine learning models, organizations can adopt a proactive defense posture, mitigating potential risks before they materialize.

One key application of predictive analytics is future attack forecasting, particularly in Internet of Things (IoT) security. Nazir et al. [Nazir et al., 2024] integrated blockchain technology with machine learning models such as Random Forest and Long Short-Term Memory (LSTM) networks to improve IoT threat prediction. Their approach enhances detection accuracy and facilitates proactive cybersecurity measures. Similarly, predictive AI models have been applied in behavioral forecasting within industrial control systems (ICS), where Dang et al. [Dang et al., 2023] employed deep neural networks to predict attack motives and forecast adversarial actions, strengthening ICS defenses by allowing early threat anticipation. Beyond individual system defenses, cyber supply chain security also benefits from predictive analytics. Yeboah-Ofori et al. [Yeboah-Ofori et al., 2021] developed a model that integrates cyber threat intelligence, ontology, and machine learning to analyze and predict supply chain-related cyber threats with high accuracy. Their approach improves proactive defense strategies by identifying potential vulnerabilities before they are exploited.

3.6 Automated Response and Defense

AI-driven automation enhances cybersecurity by accelerating response actions, reducing reaction times, and alleviating the burden on security teams. Automated systems can dynamically adapt to threats, initiate mitigation strategies, and optimize incident response workflows.

One major application is real-time mitigation, where AI-driven models detect and neutralize threats with minimal human intervention. Al-Sai et al. [Al-Hawawreh et al., 2024] introduced an LSTM-based framework for real-time Ransom Denial of Service (RDoS) threat intelligence modeling in smart satellite-based healthcare networks. Their approach enables automated attack behavior recognition and mitigation, reducing potential service disruptions. In addition, AI can filter and prioritize security alerts, addressing the issue of alert fatigue. Hassan et al. [Hassan et al., 2019] developed an AI-based system that eliminates irrelevant incident reports, allowing security teams to focus on critical threats while automating responses to lower-priority alerts.

Furthermore, AI facilitates incident response automation by integrating machine learning models with cyber threat intelligence platforms. Preuveneers and Joosen [Preuveneers

and Joosen, 2021] proposed a system that enhances threat detection by embedding AI-powered automation into cybersecurity operations, streamlining response actions and improving overall efficiency.

3.7 Learning and Adaptation

AI-driven cybersecurity systems must continuously evolve to counter emerging threats, ensuring long-term resilience against novel attack techniques. By leveraging adaptive learning mechanisms, these models refine their detection capabilities based on new data, real-world feedback, and evolving attack methodologies.

A key aspect of this adaptability is the development of adaptive defense mechanisms that adjust to emerging threats in dynamic environments. Diro and Chilamkurti [Diro and Chilamkurti, 2018] demonstrated the use of deep learning models in IoT networks that continuously refine their anomaly detection capabilities, maintaining high detection rates even as attack patterns evolve. However, to sustain effectiveness, AI models must undergo regular retraining and improvement to mitigate bias, model degradation, and outdated learning representations. Quiring and Rieck [Quiring et al., 2022] emphasized the importance of continuously refining machine learning-based security systems, cautioning against common pitfalls such as overfitting, sampling bias, and flawed evaluation metrics, which can degrade their real-world performance over time. Beyond model retraining, AI-enhanced feedback loops in threat intelligence ensure that cybersecurity systems dynamically integrate new attack data to enhance future predictions. Sarker et al. [Sarker et al., 2020] proposed a multi-layered cybersecurity framework incorporating incremental learning, enabling security mechanisms to dynamically adapt and optimize their responses based on observed threat behaviors.

By reviewing these core functions, it is evident how AI has the potential to significantly enhance threat intelligence processes. Each function leverages AI's strengths in processing vast amounts of data, recognizing patterns, and making informed decisions, rapidly and accurately. The integration of AI into these functions thus seems to improve the efficiency of threat intelligence domain, and enables organizations to adopt a more proactive and resilient cybersecurity posture.

4 Taxonomy of AI Techniques in Threat Intelligence

Building upon the core functions outlined in the previous section, the taxonomy categorizes the specific AI techniques employed in threat intelligence. Each category aligns with the corresponding core function, illustrating how AI methods are applied to fulfill these essential roles in cybersecurity.

4.1 AI Techniques for Threat Detection

Aligned with Threat Detection function, AI techniques have the potential to enhance the ability to identify anomalies and malicious activities within vast datasets.

4.1.1 Machine Learning Algorithms

Machine learning techniques play a crucial role in cyber threat detection, classification, and anomaly detection by leveraging pattern recognition in large datasets. Supervised

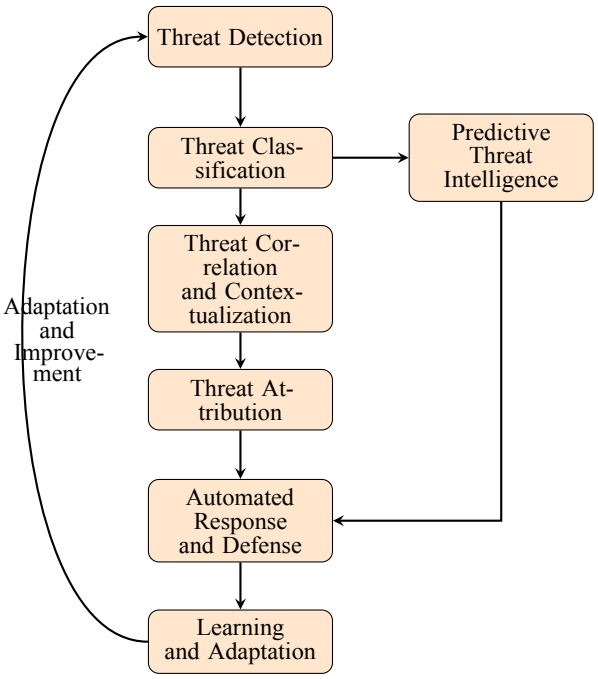

Figure 1: Core Functions of AI in Threat Intelligence

learning models, such as Support Vector Machines (SVM), Random Forests, and Decision Trees, have been widely employed for intrusion detection and network traffic analysis, utilizing labeled datasets to classify threats [Aburomman and Reaz, 2016, Li et al., 2012]. In particular, ensemble learning approaches have demonstrated improved detection accuracy by combining multiple algorithms to compensate for individual model weaknesses. Aburomman and Reaz [Aburomman and Reaz, 2016] showed that hybrid models integrating SVM and k-Nearest Neighbors (k-NN) enhance intrusion detection performance. Other than supervised learning, unsupervised anomaly detection techniques also proved relevant for identifying unknown threats without prior labeling. Clustering algorithms such as K-Means and DBSCAN can detect deviations from normal behavior, flagging potentially malicious activities [Atluri and Horne, 2021].

4.1.2 Deep Learning Models

Deep learning has emerged as an impactful approach for cyber threat intelligence, particularly in intrusion detection, malware classification, and anomaly detection. Convolutional Neural Networks (CNNs) have been extensively applied to analyze network traffic patterns, demonstrating effectiveness in detecting intrusions in IoT environments [Diro and Chilamkurti, 2018, Al-Hawawreh et al., 2020]. By leveraging hierarchical feature extraction, CNNs can recognize subtle attack signatures that traditional machine learning models might overlook. For cyber threats involving sequential patterns, Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks have proven effective in detecting time-dependent attack behaviors [Al-Hawawreh et al., 2024]. These

models process sequential data, allowing them to detect evolving cyber threats and predict adversarial movements over time. In addition to sequence modeling, Deep Belief Networks (DBNs) have been employed in intrusion detection systems for feature extraction and classification [Yin et al., 2017].

As research progresses, deep learning continues to drive innovation in automated threat detection and proactive cybersecurity defense.

4.2 AI Techniques for Threat Classification

Supporting Threat Classification function, AI techniques categorize threats to aid in prioritizing responses.

4.2.1 Supervised Learning for Classification

Supervised learning models are widely used in cyber threat intelligence due to their ability to classify threats based on labeled datasets. These methods are particularly effective in intrusion detection, malware classification, and malicious URL filtering. Naïve Bayes classifiers are commonly applied for spam filtering and URL classification, distinguishing between benign and malicious content with probabilistic modeling [Dutta and Kant, 2020]. Decision tree-based models, such as Random Forests and Gradient Boosting, have demonstrated high accuracy in detecting malicious URLs and classifying various cyberattack types [Alsaedi et al., 2022, Mishra et al., 2022]. Additionally, Support Vector Machines (SVMs) have been used for classifying network intrusions and malware types [Li et al., 2012, Sowinski-Mydlarz et al., 2021].

4.2.2 Deep Learning for Advanced Classification

Deep learning techniques have further expanded cyber threat classification capabilities by automatically extracting complex feature representations from large datasets. Deep Neural Networks (DNNs) have been employed for mapping unstructured threat intelligence to specific attack techniques, improving the ability to categorize emerging cyber threats [Orbinato et al., 2022]. For more structured classification tasks, Multilayer Perceptrons (MLPs) have been integrated into ensemble models for malicious URL detection [Alsaedi et al., 2022]. In cases where sequential attack patterns must be analyzed, Long Short-Term Memory (LSTM) networks have demonstrated effectiveness in predicting and classifying cyber threats over time, capturing temporal dependencies that static models may overlook [Al-Hawawreh et al., 2024].

4.3 AI Techniques for Threat Correlation and Contextualization

In line with Threat Correlation and Contextualization function, AI techniques help in understanding the relationships between threats.

4.3.1 Natural Language Processing (NLP)

Natural Language Processing (NLP) techniques enhance cyber threat intelligence by extracting meaningful information from unstructured text sources such as security reports, blogs, and social media. Entity recognition and extraction methods identify critical

cybersecurity-related entities, including malware names, IP addresses, and vulnerabilities, enabling automated threat intelligence gathering [Ghazi et al., 2018, Koloveas et al., 2021]. Semantic analysis is employed to understand the context and meaning of threat-related communications, allowing for better correlation of attack patterns and intent [Kadoguchi et al., 2019]. These NLP-driven capabilities contribute to more effective and structured cyber threat intelligence, improving the ability to analyze and respond to emerging threats.

4.3.2 Knowledge Graphs and Relationship Modeling

Knowledge graphs play a crucial role in structuring and analyzing cybersecurity information by representing relationships between various threat entities. Vectorized Knowledge Graphs (VKG) provide a structured representation of cybersecurity intelligence, allowing for the correlation and analysis of complex entity relationships [Mittal et al., 2019]. Similarly, Technique Knowledge Graphs (TKGs) are used to aggregate cyber threat intelligence from multiple reports, summarizing known attack techniques and enhancing situational awareness [Li et al., 2022]. AI-driven Indicator of Compromise (IOC) extraction further enriches these knowledge structures by associating threat indicators, such as file hashes and IP addresses, with specific attack campaigns [Zhu and Dumitras, 2018, Zhao et al., 2020].

By integrating NLP techniques with knowledge graph modeling, cybersecurity analysts can improve threat intelligence structuring, entity correlation, and attack attribution, leading to more informed decision-making in cyber defense.

4.4 AI Techniques for Threat Attribution

Supporting the Threat Attribution function, AI techniques assist in identifying the source of cyber-attacks.

4.4.1 Machine Learning for Profiling Threat Actors

Machine learning techniques have been widely applied in cyber threat intelligence to profile adversaries by analyzing threat reports, attack behaviors, and underground activities. Distributional semantics enables the identification of language patterns in cyber threat reports, allowing researchers to profile adversaries based on linguistic and behavioral cues [Noor et al., 2019]. Additionally, similarity calculations are used to compare new threat intelligence reports against known attacker profiles, improving predictive attribution. By measuring the resemblance between emerging threats and historical data, these methods help associate cyber incidents with specific adversary groups [Gossi, 2020]. Classification and topic modeling techniques are applied to hacker forum data, enabling the automated analysis of discussions and marketplace transactions to infer potential threat actor involvement [Hossen et al., 2021].

These profiling techniques contribute to cyber threat attribution by enhancing the ability to identify and link malicious actors based on behavioral indicators and intelligence reports.

4.4.2 Deep Learning for Advanced Attribution

Deep learning models further enhance cyber threat attribution by extracting complex patterns from vast amounts of structured and unstructured data. Deep Neural Networks (DNNs) are leveraged for high-accuracy attribution, identifying adversarial patterns that may not be apparent through traditional statistical methods [Noor et al., 2019]. In addition to classification, Natural Language Generation (NLG) techniques are used to automate the creation of comprehensive threat reports, summarizing key intelligence findings and aiding in adversary identification [Perrina et al., 2023]. By integrating deep learning with automated reporting, cybersecurity analysts can streamline intelligence processing and improve attribution accuracy.

4.5 AI Techniques for Predictive Threat Intelligence

Aligned with the Predictive Threat Intelligence function, AI techniques forecast future threats.

4.5.1 Predictive Modeling and Forecasting

Predictive modeling techniques play a crucial role in cyber threat intelligence by analyzing historical data to anticipate future attack trends. Time series analysis with Long Short-Term Memory (LSTM) networks is used for forecasting cyber threats, leveraging sequential data to identify recurring attack patterns and predict potential future incidents [Nazir et al., 2024, Al-Hawawreh et al., 2024]. Also, reinforcement learning has been applied to enhance adaptive defense strategies, allowing security systems to dynamically respond to predicted attacker behaviors and refine their decision-making processes over time [Diro and Chilamkurti, 2018, Xiao et al., 2018]. In the context of cyber supply chain security, gradient boosting algorithms have been employed to identify vulnerabilities and predict threats, improving risk mitigation efforts in complex and interconnected environments [Yeboah-Ofori et al., 2021].

These predictive modeling approaches enable organizations to shift from reactive to proactive cybersecurity postures, improving threat anticipation and strategic defense planning.

4.5.2 Behavioral Analysis

Understanding adversary behavior is key to predicting and mitigating cyber threats before they materialize. Deep Neural Networks (DNNs) have been applied to analyze attacker motives, helping cybersecurity teams anticipate adversarial intent and develop targeted defensive measures [Dang et al., 2023]. Clustering analysis is used to identify patterns and trends in cyber threat data, enabling security analysts to detect emerging threats based on behavioral similarities between attack incidents [Raptis et al., 2022]. By grouping related threat indicators, clustering techniques assist in refining cyber threat intelligence and strengthening early-warning capabilities.

4.6 AI Techniques for Automated Response and Defense

Corresponding to Automated Response and Defense functions, AI techniques can automate defense mechanisms.

4.6.1 Automation with Machine Learning

Machine learning-driven automation enhances cybersecurity by enabling rapid, AI-powered decision-making in response to emerging threats. One key application is automated incident response, where AI is integrated with Security Orchestration, Automation, and Response (SOAR) systems to initiate defensive actions, reducing response times and minimizing human intervention [Preuveneers and Joosen, 2021].

In addition to direct response actions, AI is also leveraged for alert prioritization, filtering out irrelevant incidents to reduce alert fatigue and enable security teams to focus on critical threats [Hassan et al., 2019, Aminanto et al., 2019]. Furthermore, policy enforcement mechanisms use AI to dynamically update security policies in real time based on detected threats, ensuring that defenses remain adaptive to evolving attack strategies [Atluri and Horne, 2021].

4.6.2 Real-Time Defense Mechanisms

AI-driven real-time defense mechanisms enhance proactive cybersecurity by dynamically responding to threats as they emerge. Anomaly-based blocking enables AI models to detect and immediately neutralize suspicious activities, preventing potential breaches before they escalate [Al-Hawawreh et al., 2024]. Similarly, adaptive security controls allow AI to dynamically adjust defense mechanisms based on evolving threat intelligence, ensuring that security policies and countermeasures remain effective against emerging attack techniques [Diro and Chilamkurti, 2018].

4.7 AI Techniques for Learning and Adaptation

Aligned with Learning and Adaptation functions, AI techniques can ensure that systems remain effective against evolving threats.

4.7.1 Incremental Learning Algorithms

Incremental learning techniques enable AI models to continuously adapt to new threat landscapes by integrating fresh data and refining their decision-making processes. Model retraining is an where AI systems are updated with new threat intelligence to enhance classification accuracy and detection performance over time [Sarker et al., 2020].

Similarly, adaptive deep learning models leverage evolving data patterns to refine their predictive capabilities, allowing them to recognize and respond to previously unseen attack strategies [Diro and Chilamkurti, 2018]. These continuous learning mechanisms ensure that cybersecurity models remain effective against emerging threats without requiring complete retraining from scratch.

4.7.2 Feedback Mechanisms

AI-driven cybersecurity systems incorporate feedback loops to improve accuracy and adaptability in real-world deployments. Human-in-the-loop systems enable analysts to provide corrective feedback, refining AI models to better distinguish between legitimate activity and true threats, thereby reducing false positives [Quiring et al., 2022].

Additionally, monitoring and adjustment mechanisms allow AI systems to assess their own performance and dynamically adjust model parameters to maintain effectiveness in changing environments [Koloveas et al., 2021]. These feedback-driven enhancements ensure that AI-powered cybersecurity remains robust and continuously optimized.

4.8 Adversarial Machine Learning and Defense Mechanisms

Extending beyond the core functions, adversarial machine learning techniques are crucial for protecting AI systems used in threat intelligence.

4.8.1 Detection of Poisoning Attacks

Ensuring the integrity of AI-driven cybersecurity systems requires mechanisms to detect and mitigate poisoning attacks, where adversaries manipulate training data to degrade model performance. Credibility assessment models are employed to evaluate the trustworthiness of incoming data before ingestion, reducing the risk of compromised intelligence affecting AI decision-making [Khurana et al., 2019]. Semi-supervised learning techniques combine labeled and unlabeled data to identify poisoning attempts, leveraging both structured and unstructured information to enhance model robustness against adversarial manipulation [Khurana et al., 2019]. These detection methods play a crucial role in safeguarding AI models from deceptive inputs designed to alter their predictive capabilities.

4.8.2 Robustness Enhancement Techniques

Security measures include protecting AI models through encryption methods such as Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [Preuveneers and Joosen, 2021] and improving model resilience by training them with adversarial examples [Ferrag et al., 2023]. By aligning AI techniques with the core functions of threat intelligence, the proposed taxonomy highlights the specific methods used to enhance cybersecurity operations. Each technique is connected to the functions it serves, demonstrating how AI might contribute to a comprehensive and proactive defense strategy. The integration of various AI methods, from machine learning algorithms to deep learning models and NLP, might enable organizations to effectively detect, classify, correlate, attribute, and respond to cyber threats, while effectively adapting to the ever-evolving threat landscape.

5 A Conceptual Workflow for AI-Powered Threat Intelligence

Building upon the core functions and AI techniques discussed in previous sections, herein we present a conceptual workflow for integrating Artificial Intelligence into the threat intelligence lifecycle (Fig. 3). The workflow illustrates how AI might enhance each stage of threat intelligence process, from data collection to final response.

5.1 Stages of the AI-Powered Threat Intelligence Workflow

The AI-powered threat intelligence workflow consists of seven key stages:

1. **Threat Data Collection**
2. **Data Normalization and Preprocessing**
3. **Threat Detection and Analysis**
4. **Contextual Analysis and Threat Correlation**

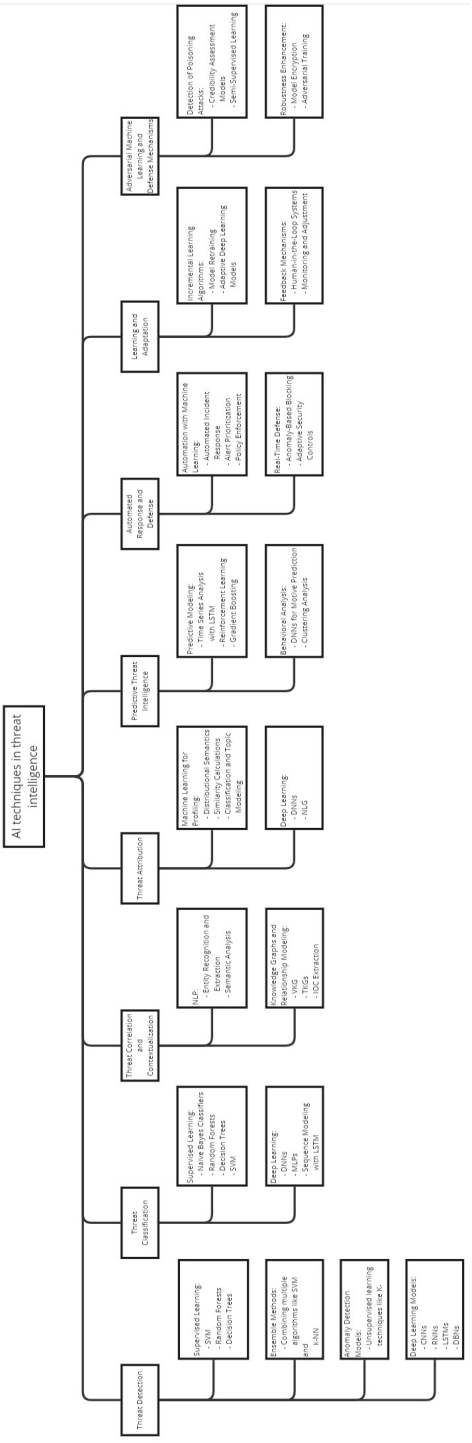

Figure 2: Taxonomy of AI Techniques in Threat Intelligence

5. **Threat Intelligence Synthesis and Prioritization**
6. **Automated Response and Defense**
7. **Learning and Feedback Loop**

Each stage leverages specific AI techniques aligned with the core functions identified in previous sections. The workflow is designed to be iterative and adaptive, incorporating continuous learning to address the evolving cyber threat landscape.

5.1.1 Stage 1: Threat Data Collection

This stage gathers raw threat data from OSINT, dark web forums, social media, and proprietary security feeds. AI-powered web crawlers and scrapers automate data acquisition, while NLP-based entity recognition pinpoints relevant indicators such as malware names and IP addresses. Sentiment analysis models further evaluate the tone of communications, helping to detect potential threats.

5.1.2 Stage 2: Data Normalization and Preprocessing

Collected data is often heterogeneous and unstructured, necessitating conversion into standardized formats (e.g., STIX). Machine learning algorithms then clean and deduplicate datasets, removing duplicates or irrelevant information, while AI-driven feature extraction isolates core attributes for subsequent analysis.

5.1.3 Stage 3: Threat Detection and Analysis

This stage leverages AI to uncover potential threats in the preprocessed data. Unsupervised algorithms detect anomalies by identifying deviations from normal patterns, while supervised classifiers categorize threats (e.g., malware types, attack techniques). Neural networks further analyze complex relationships, providing deep insights into emerging attack patterns.

5.1.4 Stage 4: Contextual Analysis and Threat Correlation

AI then adds context by mapping relationships among threat entities, often via knowledge graphs. Semantic analysis techniques interpret the meaning behind threat data, and AI correlates Indicators of Compromise (IOCs) with known vulnerabilities and tactics, enabling a comprehensive, high-level view of adversarial activity.

5.1.5 Stage 5: Threat Intelligence Synthesis and Prioritization

After analyzing threats, AI systems translate findings into actionable intelligence, assigning risk scores based on severity and likelihood. Predictive analytics forecast possible future attacks by examining historical data and behavior patterns, and threat attribution techniques profile adversaries to prioritize response efforts accordingly.

5.1.6 Stage 6: Automated Response and Defense

The system then automates mitigation strategies, such as blocking malicious IPs or isolating compromised systems. AI filters and prioritizes alerts to reduce analyst workload, and adaptive security controls dynamically adjust policies and defense mechanisms in response to real-time intelligence.

5.1.7 Stage 7: Learning and Feedback Loop

Finally, models learn continuously from fresh data and analyst feedback. AI retrains incrementally on new threat patterns without requiring a complete overhaul, ensuring that detection and defense capabilities evolve in parallel with emerging cyber threats.

5.2 Diagram of the AI-Powered Threat Intelligence Workflow

The workflow diagram in Figure 3 illustrates the sequential stages of the AI-powered threat intelligence process. Arrows indicate the flow of data and feedback loops between stages, emphasizing the iterative nature of the workflow.

- **Data Sources**: OSINT, dark web, social media, vulnerability databases feed into the system.
- **AI-Powered Data Collection**: Automated tools gather and aggregate data.
- **Normalization and Preprocessing**: Data is standardized and cleaned for analysis.
- **Detection and Analysis**: AI models identify threats within the data.
- **Contextualization and Correlation**: AI adds context and correlates data points.
- **Synthesis and Prioritization**: Threats are assessed and prioritized.
- **Automated Response**: Actions are taken to mitigate identified threats.
- **Learning and Feedback**: The system learns and improves over time, adapting to new threats.

5.3 Integration with Organizational Security Infrastructure

This AI-powered threat intelligence workflow can integrate seamlessly with existing security infrastructure. It augments Security Information and Event Management (SIEM) solutions by offering advanced analytics and reducing false positives, while Security Orchestration, Automation, and Response (SOAR) platforms benefit from AI-driven automated responses, cutting incident resolution times. Additionally, collaboration tools like MISP support the sharing of threat intelligence across organizations.

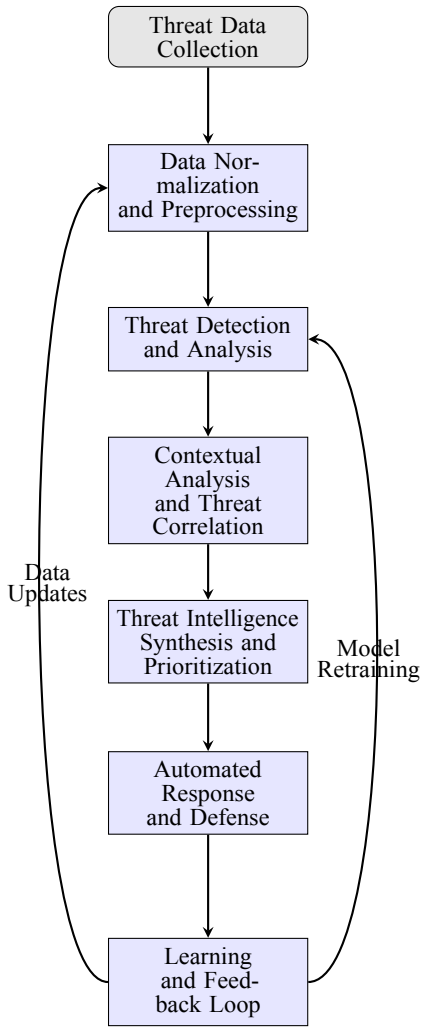

Figure 3: Conceptual Workflow for AI-Powered Threat Intelligence

5.4 Benefits of the AI-Powered Workflow

- **Scalability**: AI handles large volumes of data efficiently, enabling organizations to scale their threat intelligence efforts
- **Proactive Defense**: Predictive analytics allow systems to anticipate and mitigate threats before they materialize
- **Resource Optimization**: Automation reduces the workload on security teams, allowing them to focus on strategic tasks
- **Learning and Improvement**: The feedback loop ensures the system adapts to new threats, maintaining effectiveness over time

5.5 Challenges and Considerations

Implementing an AI-powered threat intelligence workflow presents several challenges:

- *Data Quality*: Ensuring the accuracy and relevance of collected data is critical [Rodriguez and Okamura, 2020].
- *Model Interpretability*: Complex AI models may lack transparency, making it difficult for analysts to trust their outputs.
- *Adversarial Attacks*: AI models themselves may become targets for manipulation [Khurana et al., 2019].
- *Integration Complexity*: Aligning AI systems with existing infrastructure requires careful planning and execution.

5.6 Recommendations for Implementation

Organizations should prioritize solid data management practices (e.g., validation and standardization) to ensure robust AI models. Explainable AI (XAI) mechanisms foster transparency and trust in model outputs, while adversarial training and model hardening counter potential attacks. Effective deployment also involves integrating these systems with established security tools and ensuring personnel receive ongoing AI-related training.

6 Future Directions and Recommendations for AI-Powered Threat Intelligence

The integration of Artificial Intelligence (AI) into the threat intelligence process has the potential to significantly enhance the capabilities of cybersecurity operations. However, as cyber threats continue to evolve, there is a need to advance AI methodologies and address emerging challenges. This section outlines potential future directions, provides recommendations for enhancing AI-powered threat intelligence, and proposes a roadmap for research and development.

6.1 Advancements in AI Technologies for Threat Intelligence

6.1.1 Explainable AI (XAI)

One of the pressing challenges in adopting AI for threat intelligence is the lack of transparency in decision-making processes of complex models, particularly deep learning algorithms. Explainable AI (XAI) seeks to address this by making AI models more interpretable and their decisions more understandable to human analysts.

Future Direction & Recommendation: Enhance AI model interpretability in threat detection by incorporating Explainable AI (XAI) techniques. Developing models with built-in explanation capabilities will help security analysts understand decision-making processes, increasing trust and improving response effectiveness.

6.1.2 Adversarial Robustness and Defense Mechanisms

As AI models become integral to threat intelligence, they themselves become targets for adversarial attacks, including model evasion and poisoning attacks [Khurana et al., 2019]. Enhancing the robustness of AI models against such attacks is crucial.

Future Direction & Recommendation: Advance adversarial machine learning research to develop AI models resilient to manipulation by incorporating adversarial training techniques and robust optimization methods. Regular security assessments should be conducted to detect adversarial inputs and mitigate vulnerabilities.

6.1.3 Integration of Large Language Models (LLMs)

Recent advancements in natural language processing (NLP), particularly with large language models like GPT and BERT, have shown significant promise in processing unstructured text data [Siracusano et al., 2023]. These models might significantly enhance the extraction and analysis of threat intelligence from textual sources.

Future Direction & Recommendation: Utilize Large Language Models (LLMs) for more accurate and efficient processing of unstructured threat intelligence data, such as security reports and dark web communications. Fine-tuning LLMs on cybersecurity-specific datasets will enhance their performance in tasks like entity recognition, sentiment analysis, and context understanding.

6.1.4 Federated Learning for Collaborative Threat Intelligence

Data privacy concerns and the need for collaborative defense strategies highlight the importance of federated learning, where AI models are trained across multiple decentralized devices or servers holding local data samples without exchanging them [Yang et al., 2019].

Future Direction & Recommendation: Utilize federated learning to enhance collaborative AI model improvement in threat intelligence while preserving data privacy. Developing frameworks that address challenges like data heterogeneity and secure model aggregation will ensure effective deployment in cybersecurity contexts.

6.1.5 Real-time Threat Intelligence and Edge Computing

With the proliferation of IoT devices and edge computing, there is a need for AI models that can operate efficiently in real-time and on resource-constrained devices [Diro and Chilamkurti, 2018].

Future Direction & Recommendation: Develop lightweight AI models for real-time threat detection at the edge, minimizing latency and enhancing response times. Optimizing algorithms through model compression and knowledge distillation will enable efficient deployment on resource-constrained devices while maintaining performance. intain performance while reducing computational requirements.

6.2 Recommendations for Enhancing AI-Powered Threat Intelligence

6.2.1 Data Quality and Standardization

High-quality data is the foundation of effective AI models. Ensuring the accuracy, relevance, and standardization of threat intelligence data is essential.

Recommendation: Implement comprehensive data validation and cleansing processes. Adopt standardized formats like STIX for representing threat intelligence, facilitating interoperability and data sharing [Zhu and Dumitras, 2018].

6.2.2 Ethical Considerations and Bias Mitigation

AI models can inadvertently incorporate biases present in the training data, leading to skewed results and unfair practices.

Recommendation: Conduct regular audits of AI models to identify and mitigate biases. Ensure that ethical considerations are integrated into the AI development lifecycle, promoting fairness and accountability.

6.2.3 Learning and Skill Development

The dynamic nature of cyber threats necessitates continuous learning, not just for AI models but also for the professionals managing them.

Recommendation: Provide ongoing training for cybersecurity personnel in AI and machine learning concepts. Foster a culture of continuous learning to keep pace with technological advancements.

6.2.4 Collaboration Between Academia and Industry

Bridging the gap between theoretical research and practical application can accelerate innovation in AI-powered threat intelligence.

Recommendation: Encourage partnerships between academic institutions and industry practitioners. Support collaborative projects and knowledge exchange to translate research findings into operational tools.

6.3 Roadmap for Future Research and Development

Short-Term Goals (1-2 Years):

- *Enhance Model Interpretability*: Integrate XAI methods into existing AI models for threat intelligence to improve transparency.
- *Strengthen Adversarial Defenses*: Develop and implement robust adversarial training techniques to protect AI models.
- *Optimize Data Practices*: Standardize data formats and improve data sharing mechanisms while ensuring privacy and compliance.

Medium-Term Goals (3-5 Years):

- *Adopt Advanced NLP Techniques*: Fully integrate LLMs into threat intelligence workflows for superior processing of unstructured data.
- *Expand Federated Learning Applications*: Establish federated learning frameworks for collaborative threat intelligence across organizations.
- *Promote Ethical AI Development*: Implement comprehensive policies for ethical AI use, addressing bias and fairness.

Long-Term Goals (5+ Years):

- *Innovate in Edge AI*: Develop sophisticated AI models capable of real-time threat intelligence on edge devices and IoT networks.
- *Advance Autonomous Threat Response*: Create AI systems with higher levels of autonomy for threat detection and response, minimizing human intervention.
- *Foster Global Collaboration*: Establish international coalitions for sharing threat intelligence and AI advancements, enhancing global cybersecurity resilience.

6.4 Challenges and Considerations

While AI-driven threat intelligence brings notable benefits, it also raises crucial concerns. Balancing data sharing with privacy demands robust encryption and access controls, and the shortage of professionals trained in both AI and cybersecurity intensifies the skill gap. Compliance with legal regulations remains vital for avoiding liabilities when deploying AI solutions.

7 Conclusion, Limitations, and Future Research

7.1 Conclusion

In this paper, we have presented a comprehensive exploration of the integration of Artificial Intelligence into threat intelligence processes within the cybersecurity domain. We outlined a conceptual workflow that demonstrates how AI enhances each stage of the threat intelligence lifecycle, from data collection and preprocessing to threat detection, analysis, and automated response. The core functions of AI in threat intelligence were identified and elaborated upon, including threat detection, classification, correlation, attribution, predictive intelligence, and continuous learning. Additionally, we provided a taxonomy of AI techniques applicable to threat intelligence, categorizing them based on their roles and functionalities.

The integration of AI into threat intelligence seems to offer significant benefits, including improved scalability, proactive defense capabilities, optimized resource allocation, and adaptation to evolving threats.

7.2 Limitations of the Study

Despite the comprehensive approach taken in this study, several limitations exist. Firstly, the rapidly evolving nature of AI and cybersecurity means that new techniques and threats emerge continuously, potentially rendering some aspects of this study outdated over time. Secondly, the implementation of AI in threat intelligence poses challenges such as data privacy concerns, the need for high-quality data, model interpretability issues, and vulnerability to adversarial attacks. While these challenges were acknowledged, in-depth exploration of mitigation strategies was beyond the scope of this paper.

Moreover, the practical deployment of AI systems in organizational environments may face integration complexities with existing infrastructures, and the effectiveness of AI models can vary depending on the specific context and data available. Finally, the study primarily focuses on conceptual frameworks and does not include empirical validation through case studies or experimental results, which could provide additional insights into the practical effectiveness of the proposed approaches.

7.3 Future Research

Future research directions might include:

- **Empirical Validation -** Conducting case studies and experiments to evaluate the practical effectiveness of AI techniques in real-world threat intelligence operations.
- **Advanced AI Models -** Exploring the application of advanced AI models, such as reinforcement learning and federated learning, to enhance threat intelligence processes while addressing data privacy concerns.
- **Explainable AI (XAI) -** Developing and integrating XAI methods to improve the interpretability and trustworthiness of AI models used in threat intelligence, enabling security analysts to better understand and validate AI-driven insights.
- **Adversarial Robustness -** Investigating strategies to protect AI models against adversarial attacks, including adversarial training and the development of robust model architectures.
- **Integration Strategies -** Studying methodologies for seamless integration of AI systems with existing cybersecurity infrastructures, including SIEM and SOAR platforms, to maximize the benefits of AI-enhanced threat intelligence.
- **Ethical and Legal Considerations -** Examining the ethical and legal implications of using AI in threat intelligence, particularly concerning data privacy, surveillance, and compliance with regulations.

By addressing these areas, future research can contribute to the advancement of AI-powered threat intelligence, overcoming current limitations and enhancing cybersecurity defenses against increasingly sophisticated cyber threats.

References

[Aburomman and Reaz, 2016] Aburomman, A. A. and Reaz, M. B. I. (2016). A novel svm-knn-pso ensemble method for intrusion detection system. *Applied Soft Computing*, 38:360–372.

[Adewopo et al., 2020] Adewopo, V., Gonen, B., and Adewopo, F. (2020). Exploring open source information for cyber threat intelligence. In *2020 IEEE International Conference on Big Data (Big Data)*, pages 2232–2241. IEEE.

[Al-Hawawreh et al., 2020] Al-Hawawreh, M., Moustafa, N., Garg, S., and Hossain, M. S. (2020). Deep learning-enabled threat intelligence scheme in the internet of things networks. *IEEE Transactions on Network Science and Engineering*, 8(4):2968–2981.

[Al-Hawawreh et al., 2024] Al-Hawawreh, M., Moustafa, N., and Slay, J. (2024). A threat intelligence framework for protecting smart satellite-based healthcare networks. *Neural Computing and Applications*, 36(1):15–35.

[Alsaedi et al., 2022] Alsaedi, M., Ghaleb, F. A., Saeed, F., Ahmad, J., and Alasli, M. (2022). Cyber threat intelligence-based malicious url detection model using ensemble learning. *Sensors*, 22(9):3373.

[Aminanto et al., 2019] Aminanto, M. E., Zhu, L., Ban, T., Isawa, R., Takahashi, T., and Inoue, D. (2019). Automated threat-alert screening for battling alert fatigue with temporal isolation forest. In *2019 17th International Conference on Privacy, Security and Trust (PST)*, pages 1–3. IEEE.

[Atluri and Horne, 2021] Atluri, V. and Horne, J. (2021). A machine learning based threat intelligence framework for industrial control system network traffic indicators of compromise. In *SoutheastCon 2021*, pages 1–5. IEEE.

[Barker, 2020] Barker, C. (2020). Applications of machine learning to threat intelligence, intrusion detection and malware.

[Bouchama and Kamal, 2021] Bouchama, F. and Kamal, M. (2021). Enhancing cyber threat detection through machine learning-based behavioral modeling of network traffic patterns. *International Journal of Business Intelligence and Big Data Analytics*, 4(9):1–9.

[Canedo and Skjellum, 2016] Canedo, J. and Skjellum, A. (2016). Using machine learning to secure iot systems. In *2016 14th annual conference on privacy, security and trust (PST)*, pages 219–222. IEEE.

[Dang et al., 2023] Dang, F., Yan, L., Li, S., and Jia, Z. (2023). Research on threat intelligence detection model based on deep neural network. In Kong, X., editor, *Second International Conference on Electronic Information Engineering, Big Data, and Computer Technology (EIBDCT 2023)*, volume 12642, page 126422S. International Society for Optics and Photonics, SPIE.

[Deliu et al., 2017] Deliu, I., Leichter, C., and Franke, K. (2017). Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks. In *2017 IEEE International Conference on Big Data (Big Data)*, pages 3648–3656. IEEE.

[Diro and Chilamkurti, 2018] Diro, A. A. and Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for internet of things. *Future Generation Computer Systems*, 82:761–768.

[Dutta and Kant, 2020] Dutta, A. and Kant, S. (2020). An overview of cyber threat intelligence platform and role of artificial intelligence and machine learning. In *Information Systems Security: 16th International Conference, ICISS 2020, Jammu, India, December 16–20, 2020, Proceedings 16*, pages 81–86. Springer.

[Ejaz et al., 2022] Ejaz, S., Noor, U., and Rashid, Z. (2022). Visualizing interesting patterns in cyber threat intelligence using machine learning techniques. *Cybernetics and Information Technologies*, 22(2):96–113.

[Ferrag et al., 2023] Ferrag, M. A., Ndhlovu, M., Tihanyi, N., Cordeiro, L. C., Debbah, M., and Lestable, T. (2023). Revolutionizing cyber threat detection with large language models. *arXiv preprint arXiv:2306.14263*.

[Ghazi et al., 2018] Ghazi, Y., Anwar, Z., Mumtaz, R., Saleem, S., and Tahir, A. (2018). A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources. In *2018 International Conference on Frontiers of Information Technology (FIT)*, pages 129–134. IEEE.

[Gossi, 2020] Gossi, C. (2020). Identifying attackers by using machine learning on unstructured cyber threat intelligence.

[Gupta et al., 2019] Gupta, S., Sabitha, A. S., and Punhani, R. (2019). Cyber security threat intelligence using data mining techniques and artificial intelligence. *Int. J. Recent Technol. Eng*, 8:6133–6140.

[Hassan et al., 2019] Hassan, W. U., Guo, S., Li, D., Chen, Z., Jee, K., Li, Z., and Bates, A. (2019). Nodoze: Combatting threat alert fatigue with automated provenance triage. In *network and distributed systems security symposium*.

[Hodo et al., 2016] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.-L., Iorkyase, E., Tachtatzis, C., and Atkinson, R. (2016). Threat analysis of iot networks using artificial neural network intrusion detection system. In *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, pages 1–6. IEEE.

[Hossen et al., 2021] Hossen, M. I., Islam, A., Anowar, F., Ahmed, E., and Rahman, M. M. (2021). Generating cyber threat intelligence to discover potential security threats using classifica-

tion and topic modeling. In *Cyber Security Using Modern Technologies*, pages 141–153. CRC Press.

[Kadoguchi et al., 2019] Kadoguchi, M., Hayashi, S., Hashimoto, M., and Otsuka, A. (2019). Exploring the dark web for cyber threat intelligence using machine leaning. In *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 200–202. IEEE.

[Kaiser et al., 2023] Kaiser, F. K., Dardik, U., Elitzur, A., Zilberman, P., Daniel, N., Wiens, M., Schultmann, F., Elovici, Y., and Puzis, R. (2023). Attack hypotheses generation based on threat intelligence knowledge graph. *IEEE Transactions on Dependable and Secure Computing*.

[Kang and Kang, 2016] Kang, M.-J. and Kang, J.-W. (2016). Intrusion detection system using deep neural network for in-vehicle network security. *PloS one*, 11(6):e0155781.

[Kaplantzis et al., 2007] Kaplantzis, S., Shilton, A., Mani, N., and Sekercioglu, Y. A. (2007). Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In *2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information*, pages 335–340. IEEE.

[Kasman et al., 2023] Kasman, S., Utomo, S. D., et al. (2023). Machine learning sentiment analysis in cyber threat intelligence recommendation system. *International Journal on Information and Communication Technology (IJoICT)*, 9(2):75–85.

[Khurana et al., 2019] Khurana, N., Mittal, S., Piplai, A., and Joshi, A. (2019). Preventing poisoning attacks on ai based threat intelligence systems. In *2019 IEEE 29th International Workshop on Machine Learning for Signal Processing (MLSP)*, pages 1–6. IEEE.

[Koloveas et al., 2021] Koloveas, P., Chantzios, T., Alevizopoulou, S., Skiadopoulos, S., and Tryfonopoulos, C. (2021). intime: A machine learning-based framework for gathering and leveraging web data to cyber-threat intelligence. *Electronics*, 10(7):818.

[Kristiansen et al., 2020] Kristiansen, L.-M., Agarwal, V., Franke, K., and Shah, R. S. (2020). Cti-twitter: gathering cyber threat intelligence from twitter using integrated supervised and unsupervised learning. In *2020 IEEE International Conference on Big Data (Big Data)*, pages 2299–2308. IEEE.

[Kumar et al., 2012] Kumar, M., Hanumanthappa, M., and Kumar, T. S. (2012). Intrusion detection system using decision tree algorithm. In *2012 IEEE 14th international conference on communication technology*, pages 629–634. IEEE.

[Li et al., 2012] Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., and Dai, K. (2012). An efficient intrusion detection system based on support vector machines and gradually feature removal method. *Expert systems with applications*, 39(1):424–430.

[Li et al., 2022] Li, Z., Zeng, J., Chen, Y., and Liang, Z. (2022). Attackg: Constructing technique knowledge graph from cyber threat intelligence reports. In *European Symposium on Research in Computer Security*, pages 589–609. Springer.

[Liang et al., 2019] Liang, E., Zhu, H., Jin, X., and Stoica, I. (2019). Neural packet classification. In *Proceedings of the ACM Special Interest Group on Data Communication*, pages 256–269.

[Lin et al., 2015] Lin, W.-C., Ke, S.-W., and Tsai, C.-F. (2015). Cann: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-based systems*, 78:13–21.

[Mamdouh et al., 2018] Mamdouh, M., Elrukhsi, M. A., and Khattab, A. (2018). Securing the internet of things and wireless sensor networks via machine learning: A survey. In *2018 International Conference on Computer and Applications (ICCA)*, pages 215–218. IEEE.

[Mishra et al., 2022] Mishra, S., Albarakati, A., and Sharma, S. K. (2022). Cyber threat intelligence for iot using machine learning. *Processes*, 10(12):2673.

[Mittal et al., 2019] Mittal, S., Joshi, A., and Finin, T. (2019). Cyber-all-intel: An ai for security related threat intelligence. *arXiv preprint arXiv:1905.02895*.

[Nazir et al., 2024] Nazir, A., He, J., Zhu, N., Wajahat, A., Ullah, F., Qureshi, S., Ma, X., and Pathan, M. S. (2024). Collaborative threat intelligence: Enhancing iot security through blockchain and machine learning integration. *Journal of King Saud University-Computer and Information Sciences*, page 101939.

[Nguyen et al., 2022] Nguyen, C., Morgan, C., and Mittal, S. (2022). Poster cti4ai: Threat intelligence generation and sharing after red teaming ai models. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 3431–3433.

[Noel, 2021] Noel, L. (2021). Redai: A machine learning approach to cyber threat intelligence.

[Noor et al., 2019] Noor, U., Anwar, Z., Malik, A. W., Khan, S., and Saleem, S. (2019). A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories. *Future Generation Computer Systems*, 95:467–487.

[Nunes et al., 2016] Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., Robertson, J., Shakarian, J., Thart, A., and Shakarian, P. (2016). Darknet and deepnet mining for proactive cybersecurity threat intelligence. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, pages 7–12. IEEE.

[Orbinato et al., 2022] Orbinato, V., Barbaraci, M., Natella, R., and Cotroneo, D. (2022). Automatic mapping of unstructured cyber threat intelligence: An experimental study:(practical experience report). In *2022 IEEE 33rd International Symposium on Software Reliability Engineering (ISSRE)*, pages 181–192. IEEE.

[Perrina et al., 2023] Perrina, F., Marchiori, F., Conti, M., and Verde, N. V. (2023). Agir: Automating cyber threat intelligence reporting with natural language generation. In *2023 IEEE International Conference on Big Data (BigData)*, pages 3053–3062. IEEE.

[Preuveneers and Joosen, 2021] Preuveneers, D. and Joosen, W. (2021). Sharing machine learning models as indicators of compromise for cyber threat intelligence. *Journal of Cybersecurity and Privacy*, 1(1):140–163.

[Quiring et al., 2022] Quiring, E., Pendlebury, F., Warnecke, A., Pierazzi, F., Wressnegger, C., Cavallaro, L., and Rieck, K. (2022). Dos and don'ts of machine learning in computer security. In *31st USENIX Security Symposium (USENIX Security 22), USENIX Association, Boston, MA*.

[Raj et al., 2012] Raj, A. B., Ramesh, M. V., Kulkarni, R. V., and Hemalatha, T. (2012). Security enhancement in wireless sensor networks using machine learning. In *2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems*, pages 1264–1269. IEEE.

[Ranade et al., 2018] Ranade, P., Mittal, S., Joshi, A., and Joshi, K. (2018). Using deep neural networks to translate multi-lingual threat intelligence. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*, pages 238–243. IEEE.

[Ranade et al., 2021] Ranade, P., Piplai, A., Mittal, S., Joshi, A., and Finin, T. (2021). Generating fake cyber threat intelligence using transformer-based models. In *2021 International Joint Conference on Neural Networks (IJCNN)*, pages 1–9. IEEE.

[Raptis et al., 2022] Raptis, G. E., Katsini, C., Alexakos, C., Kalogeras, A., and Serpanos, D. (2022). Cavectir: Matching cyber threat intelligence reports on connected and autonomous vehicles using machine learning. *Applied Sciences*, 12(22):11631.

[Rieck et al., 2011] Rieck, K., Trinius, P., Willems, C., and Holz, T. (2011). Automatic analysis of malware behavior using machine learning. *Journal of computer security*, 19(4):639–668.

[Rodriguez and Okamura, 2020] Rodriguez, A. and Okamura, K. (2020). Enhancing data quality in real-time threat intelligence systems using machine learning. *Social Network Analysis and Mining*, 10:1–22.

[Saied et al., 2016] Saied, A., Overill, R. E., and Radzik, T. (2016). Detection of known and unknown ddos attacks using artificial neural networks. *Neurocomputing*, 172:385–393.

[Sarker et al., 2020] Sarker, I. H., Kayes, A., Badsha, S., Alqahtani, H., Watters, P., and Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. *Journal of Big data*, 7:1–29.

[Siracusano et al., 2023] Siracusano, G., Sanvito, D., Gonzalez, R., Srinivasan, M., Kamatchi, S., Takahashi, W., Kawakita, M., Kakumaru, T., and Bifulco, R. (2023). Time for action: Automated analysis of cyber threat intelligence in the wild. *arXiv preprint arXiv:2307.10214*.

[Sowinski-Mydlarz et al., 2021] Sowinski-Mydlarz, V., Li, J., Ouazzane, K., Vassilev, V., et al. (2021). Threat intelligence using machine learning packet dissection. *Transactions on Computational Science and Computational Intelligence*.

[Sufi, 2023] Sufi, F. (2023). A global cyber-threat intelligence system with artificial intelligence and convolutional neural network. *Decision Analytics Journal*, 9:100364.

[Xiao et al., 2018] Xiao, L., Wan, X., Dai, C., Du, X., Chen, X., and Guizani, M. (2018). Security in mobile edge caching with reinforcement learning. *IEEE Wireless Communications*, 25(3):116–122.

[Yang et al., 2019] Yang, Q., Liu, Y., Chen, T., and Tong, Y. (2019). Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 10(2):1–19.

[Yeboah-Ofori et al., 2021] Yeboah-Ofori, A., Mouratidis, H., Ismai, U., Islam, S., and Papastergiou, S. (2021). Cyber supply chain threat analysis and prediction using machine learning and ontology. In *Artificial Intelligence Applications and Innovations: 17th IFIP WG 12.5 International Conference, AIAI 2021, Hersonissos, Crete, Greece, June 25–27, 2021, Proceedings 17*, pages 518–530. Springer.

[Yin et al., 2017] Yin, C., Zhu, Y., Fei, J., and He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *Ieee Access*, 5:21954–21961.

[Zenebe, 2022] Zenebe, A. (2022). Cyber threat intelligence discovery using machine learning from the dark web. *Communications of the IIMA*, 20(2).

[Zhao et al., 2020] Zhao, J., Yan, Q., Li, J., Shao, M., He, Z., and Li, B. (2020). Timiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data. *Computers & Security*, 95:101867.

[Zhu and Dumitras, 2018] Zhu, Z. and Dumitras, T. (2018). Chainsmith: Automatically learning the semantics of malicious campaigns by mining threat intelligence reports. In *2018 IEEE European symposium on security and privacy (EuroS&P)*, pages 458–472. IEEE.