Open Access Research Journal of
Science and Technology
Journals home page: https://oarjst.com/
ISSN: 2782-9960 (Online)

OARJ OPEN ACCESS RESEARCH JOURNALS

(REVIEW ARTICLE)

# AI-driven threat intelligence for real-time cybersecurity: Frameworks, tools, and future directions

Kelvin Ovabor [1], Ismail Oluwatobiloba Sule-Odu [2,*], Travis Atkison [1], Adetutu Temitope Fabusoro [3] and Joseph Oluwaseun Benedict [4]

[1] *Computer Science, The University of Alabama, Tuscaloosa, Alabama, USA.*
[2] *Computer Science, Maharishi International University (MIU), Fairfield, IA, USA.*
[3] *Education Policy Organization and Leadership, University of Illinois, Urbana Champaign, IL, USA.*
[4] *Information Security and Digital Forensics, University of East London, UK.*

Open Access Research Journal of Science and Technology, 2024, 12(02), 040–048

Publication history: Received on 28 September 2024; revised on 06 November 2024; accepted on 09 November 2024

Article DOI: https://doi.org/10.53022/oarjst.2024.12.2.0135

## Abstract

AI-driven threat intelligence is transforming cybersecurity by enhancing real-time threat detection, analysis, and response capabilities. This paper reviews state-of-the-art AI frameworks, machine learning models, and tools that support threat intelligence, providing a survey of current research in the field and identifying challenges and future directions for real-time cybersecurity. Techniques such as supervised and unsupervised learning, reinforcement learning, and natural language processing (NLP) contribute to the robustness of threat detection, while evolving frameworks and ethics guide AI implementation in security operations. By addressing the increasing sophistication of cyber threats, AI-driven approaches aim to create a proactive, dynamic cybersecurity posture that can keep up with evolving cyber adversaries.

**Keyword:** Artificial Intelligence; Cybersecurity; Machine Learning; Deep Learning

## 1. Introduction

In today's digital landscape, organizations face an unprecedented array of cyber threats. Traditional cybersecurity defenses, largely reactive and manual, are insufficient in countering sophisticated attacks that continuously adapt to bypass defenses [1, 2]. As a result, AI-driven threat intelligence has emerged as a vital strategy in cybersecurity [3], leveraging machine learning, deep learning, and big data analysis to enable rapid, proactive responses to cyber threats [4, 5]. This technology not only strengthens threat detection and prevention but also enables organizations to understand and anticipate potential vulnerabilities.

AI-driven threat intelligence shifts the paradigm from detecting past-known threats to predicting new ones, enabling organizations to preemptively address vulnerabilities and mitigate the impact of attacks. With these advancements [6], AI is poised to become indispensable in cybersecurity, leading to faster, more accurate, and automated threat detection.

### 1.1. Background and Motivation

The necessity of AI-driven threat intelligence is underscored by several key factors:

- **Addressing the Rise of Advanced Persistent Threats (APTs)**: APTs are a class of stealthy and continuous hacking processes that target specific entities to gain intelligence over an extended period [7, 8]. Traditional detection mechanisms are often too rigid to detect the subtle, long-term behavioral anomalies of APTs. AI-

* Corresponding author: Ismail Oluwatobiloba Sule-Odu

Copyright © 2024 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

driven models, however, can continuously learn and adapt, identifying deviations from established behavior patterns indicative of APT activity [9].

- **Managing Volume and Diversity of Threat Data**: Modern networks generate vast quantities of data from devices, applications, and endpoints [10]. This complexity requires systems that can analyze diverse data types (structured and unstructured) in real-time, a task AI is well-suited for with its ability to scale across multiple data sources [11].
- **Overcoming the Limitations of Manual and Rule-based Approaches**: Legacy systems typically rely on manually created rules and static configurations that can be easily circumvented by new or evolving threats [12, 13]. AI-driven systems use dynamic learning and pattern recognition, allowing cybersecurity measures to adapt autonomously and proactively [13].

### 1.2. Scope and Objectives

This paper aims to provide an in-depth overview of AI-driven threat intelligence by focusing on three main objectives:

- **Examine AI frameworks and tools** that support real-time threat intelligence in cybersecurity, evaluating their effectiveness and applicability [14, 15].
- **Survey recent research trends** on machine learning, deep learning, and NLP applications in threat detection, prevention, and response [16].
- **Identify challenges and propose future directions** that can guide improvements in AI-driven threat intelligence systems, with attention to resilience, transparency, and ethical considerations [17].

## 2. AI Frameworks and Models for Real-time Threat Intelligence

AI-driven threat intelligence utilizes various machine learning models to detect and respond to threats dynamically. The following sections discuss the types of machine learning models applied in cybersecurity and their specific applications in identifying, classifying, and mitigating cyber threats.

### 2.1. Supervised Learning Models

Supervised learning models require labeled datasets to train algorithms in classifying threats accurately:

- **Model Training on Labeled Threat Data**: Supervised learning models learn from historical data by associating specific inputs with known outcomes. This is particularly effective in identifying types of malware or phishing attacks, where existing attack signatures are available [18, 19].
- **Applications in Malware and Phishing Detection**: Techniques like decision trees, support vector machines (SVMs), and neural networks are commonly used. For instance, neural networks can analyze a phishing email's content and sender information, learning to flag emails with suspicious characteristics based on prior examples [20].

### 2.2. Unsupervised and Semi-supervised Learning Models

Unsupervised models play a crucial role in anomaly detection, a cornerstone of cybersecurity applications:

- **Clustering and Anomaly Detection**: With unsupervised models, threat detection becomes more flexible, as these models are not restricted to labeled datasets. For example, clustering algorithms identify outliers within network traffic, helping detect patterns indicative of cyber-attacks [18, 21].
- **Semi-supervised Learning with Limited Labeled Data**: Often, cybersecurity data lacks comprehensive labeling. Semi-supervised learning allows models to learn from a small set of labeled data combined with a larger volume of unlabeled data, thereby improving detection capabilities for unknown threats [22, 23].

### 2.3. Reinforcement Learning

Reinforcement learning (RL) supports real-time, adaptive responses by learning from environmental feedback:

- **Adaptive Security Policies**: RL algorithms can autonomously refine policies based on success metrics (rewards), optimizing response strategies to contain threats effectively [6, 24].
- **SIEM System Integration**: In Security Information and Event Management (SIEM) systems, RL-based automation can prioritize alerts, automate threat responses, and refine defense mechanisms over time, enabling continuous improvement in threat response [25, 26].

### 2.4. Natural Language Processing (NLP)

NLP allows for interpreting unstructured data, such as threat reports, social media, and cybersecurity forums:

- **Text Mining for Threat Intelligence**: NLP-based text mining extracts threat information from textual data, identifying keywords and entities related to potential attacks [27, 28].
- **Contextual Threat Analysis**: NLP enhances the contextual analysis of threats by interpreting intent and relevance, which is crucial in threat intelligence operations to discern between benign and malicious activities [29, 30].

### 2.5. Deep Learning Techniques

Deep learning's multi-layered architecture enables it to detect intricate threat patterns:

- **Applications in Fraud Prevention and Predictive Analytics**: Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) help in recognizing complex fraud patterns, while Generative Adversarial Networks (GANs) simulate potential threats, improving the resilience of defense mechanisms [31, 32].
- **Pattern Recognition for Unknown Threats**: Deep learning models' ability to identify anomalies and previously unseen threats has become essential in detecting zero-day vulnerabilities and other novel attack forms[33].

## 3. Tools and Frameworks in AI-driven Threat Intelligence

Several tools and platforms integrate AI with cybersecurity operations, automating threat intelligence and facilitating real-time responses.

### 3.1. IBM QRadar Advisor with Watson

IBM QRadar Advisor uses IBM Watson's cognitive abilities to analyze unstructured data and enhance threat detection:

- **NLP for Threat Contextualization**: QRadar Advisor processes security reports, social media, and threat intelligence feeds to provide contextual analysis, enabling security teams to prioritize significant threats [34, 35].
- **Enhanced Anomaly Detection**: Using machine learning, QRadar analyzes large volumes of security logs to detect unusual behavior indicative of security breaches [36].

### 3.2. Microsoft Azure Sentinel

Azure Sentinel is a scalable, cloud-based SIEM that uses machine learning for multi-cloud threat detection:

- **Scalable Data Analysis**: Azure Sentinel can process diverse datasets across cloud environments, applying machine learning to detect potential threats in real time [37, 38].
- **Integration with Microsoft's Security Ecosystem**: Azure Sentinel's integration with Microsoft's security resources enables it to provide comprehensive threat intelligence by leveraging global datasets, facilitating more accurate and timely responses [39].

### 3.3. Darktrace

Darktrace's self-learning AI autonomously identifies and mitigates cyber threats by continuously adapting to network behavior:

- **Unsupervised Learning for Novel Threats**: Darktrace employs unsupervised models to autonomously detect deviations from typical behavior, making it effective for discovering previously unknown threats [40, 41].
- **Real-time Threat Detection and Response**: Darktrace's ability to respond to threats as they emerge helps organizations address zero-day vulnerabilities more effectively [42, 43].

### 3.4. FireEye Threat Intelligence Platform

FireEye's threat intelligence platform combines machine learning and threat data sharing for advanced threat detection:

- **Malware and Intrusion Detection**: FireEye's platform applies machine learning to enhance malware detection accuracy, aiding in the identification of sophisticated attack techniques [44].
- **Collaborative Data Sharing**: Through shared threat intelligence, FireEye's platform allows organizations to leverage collective insights, strengthening defenses across the cybersecurity landscape [45].

## 4. Survey of Research in AI-driven Threat Intelligence

This section surveys recent advancements in research related to AI applications in threat intelligence.

### 4.1. Research on Predictive Analytics and Threat Detection

Predictive models provide a proactive approach to threat intelligence:

- **Techniques for Threat Scoring**: Researchers are developing algorithms that assign risk scores to potential threats, allowing security teams to prioritize mitigation efforts based on threat severity [46-48].
- **Machine Learning in Threat Vector Prediction**: Studies focus on how machine learning can predict likely attack vectors by analyzing historical data, enhancing organizational preparedness [49-51].

### 4.2. Studies on NLP in Cybersecurity

NLP is critical in analyzing unstructured data sources for threat detection:

- **Text Mining Innovations**: Recent studies focus on text mining to extract insights from open-source intelligence, such as threat data from forums, social media, and reports [27, 52, 53].
- **Multilingual NLP for Global Threat Monitoring**: Research is being conducted to adapt NLP for multilingual threat detection, essential for international organizations dealing with global cyber threats [54-57].

### 4.3. Research on Anomaly Detection in Network Security

Anomaly detection remains a pivotal aspect of AI-driven threat intelligence:

- **Clustering Techniques**: Clustering methods, such as k-means and DBSCAN, identify patterns in network traffic, enabling real-time threat detection [58, 59].
- **Deep Learning for Real-time Anomaly Detection**: Deep learning models are increasingly applied to detect high-dimensional anomalies within large network environments [60].

### 4.4. Adversarial AI in Cybersecurity

Adversarial AI is both a tool and a threat to cybersecurity:

- **Evasion Tactics and Defense Mechanisms**: Research explores adversarial AI that creates inputs to deceive AI models, while also developing defense mechanisms to counter these tactics [61, 62].
- **Enhancing Model Robustness**: Defensive techniques, such as adversarial training, are being explored to make models more resistant to deception by adversarial samples.

### 4.5. Reinforcement Learning Applications

Reinforcement learning has demonstrated potential in automating threat responses:

- **Decision-making Automation**: RL models optimize security responses by learning from past decisions, effectively automating the prioritization and response process [61].
- **Case Studies in SIEM Systems**: Research highlights RL's success in enhancing SIEM automation by adapting to evolving threats and optimizing response strategies [63, 64].

## 5. Challenges and Limitations of AI-driven Threat Intelligence

While AI-driven threat intelligence offers numerous benefits, it also faces challenges.

### 5.1. Data Quality and Availability

Data quality is a critical factor for AI model accuracy:

- **Challenges in Data Labeling and Collection**: Collecting labeled data for cybersecurity is difficult and costly, resulting in models that may lack robustness [23].
- **Imbalanced Data Challenges**: In cybersecurity, benign data often far exceeds malicious samples, leading to models that may struggle with accurate threat detection [65].

### 5.2. Adversarial Attacks

AI models are vulnerable to adversarial attacks:

- **Impact of Adversarial Samples**: Attackers can use adversarial inputs to bypass AI-driven security measures, leading to false negatives in threat detection [66].
- **Mitigating Adversarial Vulnerabilities**: Techniques such as adversarial training help models withstand evasion attempts by adversaries [66].

### 5.3. Interpretability and Transparency

The complexity of AI models can hinder interpretability:

- **Challenges in Model Explainability**: As deep learning models grow more complex, explaining decisions to non-technical stakeholders becomes difficult, impacting trust [67].
- **Efforts to Improve Explainability**: Techniques like SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-Agnostic Explanations) aim to make AI decisions more understandable [68].

### 5.4. Ethical and Privacy Concerns

The ethical use of AI in threat intelligence is a significant concern:

- **Balancing Privacy and Threat Monitoring**: Ensuring privacy while monitoring for threats requires careful management of data collection practices.
- **Ethical Implications of Automated Intelligence**: Unregulated AI-driven intelligence gathering raises concerns over potential abuses, emphasizing the need for ethical frameworks.

## 6. Future Directions

### 6.1. Enhanced Real-time Analytics

Advancements in real-time analytics promise greater scalability and privacy:

- **Federated Learning**: Federated learning enables models to train on decentralized data sources, enhancing privacy in real-time analytics.
- **Edge Computing for Scalable Analysis**: Lightweight models for edge devices reduce latency, allowing for faster localized threat detection.

### 6.2. Quantum Computing in Cybersecurity

Quantum computing presents new possibilities and challenges for cybersecurity:

- **Quantum-enhanced Encryption**: Quantum algorithms can secure data more effectively, but also pose threats to existing encryption methods.
- **Research into Quantum-resistant Algorithms**: Quantum-resistant encryption is essential to safeguard data as quantum computing advances.

### 6.3. Multimodal Threat Intelligence

Combining various data sources allows for more comprehensive threat intelligence:

- **Holistic Data Analysis**: Multimodal approaches offer a fuller picture by integrating data from multiple sources, strengthening threat assessment accuracy.

### 6.4. AI Ethics and Governance Frameworks

Establishing ethical standards for AI in cybersecurity will ensure responsible use:

- **Transparency and Fairness Standards**: Ethical frameworks guide the responsible implementation of AI, fostering trust and accountability in cybersecurity applications.

## 7. Conclusion

AI-driven threat intelligence is revolutionizing cybersecurity by providing advanced capabilities for real-time detection and response to ever-evolving cyber threats. By analyzing vast amounts of data and identifying patterns that indicate malicious activities, AI enhances the speed and precision of threat detection, enabling organizations to mitigate risks proactively. Moreover, AI can automate incident response, reducing the burden on security teams and ensuring timely intervention to prevent potential breaches.

Despite these advantages, significant challenges remain. Issues such as data quality can impact the effectiveness of AI models, as inaccurate or biased datasets may lead to false positives or missed threats. Additionally, the interpretability of AI decisions poses a challenge, as the "black box" nature of many AI algorithms can make it difficult for cybersecurity professionals to understand or justify AI-driven actions. Ethical considerations, including privacy concerns and the risk of algorithmic bias, further complicate the deployment of AI in security operations.

Looking ahead, emerging technologies such as federated learning and quantum computing hold great promise for enhancing the resilience and efficiency of AI in cybersecurity. Federated learning allows for decentralized training of AI models across multiple devices, improving data privacy while enabling the development of robust models that learn from diverse, distributed datasets. Quantum computing, on the other hand, has the potential to revolutionize cryptography and data processing, offering unprecedented computational power to tackle complex security challenges. As these advancements mature, they will play a critical role in creating adaptive and robust cybersecurity frameworks, making AI an indispensable tool in the defense against increasingly sophisticated cyber threats.

## Compliance with ethical standards

### *Disclosure of conflict of interest*

No conflict of interest to be disclosed.

## References

[1] AL-Hawamleh, A., *Cyber resilience framework: Strengthening defenses and enhancing continuity in business security.* International Journal of Computing and Digital Systems, 2024. **15**(1): p. 1315-1331.

[2] Burton, S.L., *The Rise and Advancement: Intelligent Cybersecurity Markets*, in *Pioneering Paradigms in Organizational Research and Consulting Interventions: A Multidisciplinary Approach*. 2024, IGI Global. p. 259-302.

[3] Alesinloye, T., et al., *THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENHANCING CYBERSECURITY FOR FINTECH APPLICATIONS: A COMPREHENSIVE REVIEW.* INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING AND TECHNOLOGY (IJCET), 2024. **15**(5): p. 38-44.

[4] Nassar, A. and M. Kamal, *Machine Learning and Big Data analytics for Cybersecurity Threat Detection: A Holistic review of techniques and case studies.* Journal of Artificial Intelligence and Machine Learning in Management, 2021. **5**(1): p. 51-63.

[5] Chen, X.-W. and X. Lin, *Big data deep learning: challenges and perspectives.* IEEE access, 2014. **2**: p. 514-525.

[6] Arulkumaran, K., et al., *Deep reinforcement learning: A brief survey.* IEEE Signal Processing Magazine, 2017. **34**(6): p. 26-38.

[7] Mahboubi, A., et al., *Evolving techniques in cyber threat hunting: A systematic review.* Journal of Network and Computer Applications, 2024: p. 104004.

[8] Che Mat, N.I., et al., *A systematic literature review on advanced persistent threat behaviors and its detection strategy.* Journal of Cybersecurity, 2024. **10**(1): p. tyad023.

[9] Rayhan, A., *Cybersecurity in the Digital Age: Assessing Threats and Strengthening Defenses.*

[10] Gharaibeh, A., et al., *Smart cities: A survey on data management, security, and enabling technologies.* IEEE Communications Surveys & Tutorials, 2017. **19**(4): p. 2456-2501.

[11] Chen, C.P. and C.-Y. Zhang, *Data-intensive applications, challenges, techniques and technologies: A survey on Big Data.* Information sciences, 2014. **275**: p. 314-347.

[12] Anvaari, M., *A Rule-based Framework for Enhancing Architectural Decision Guidance.* 2016.

[13] Fickas, S., *Design issues in a rule-based system.* ACM SIGPLAN Notices, 1985. **20**(7): p. 208-215.

[14] Adeoye, I., *Leveraging Artificial Intelligence and Machine Learning for Real-Time Threat Intelligence: Enhancing Incident Response Capabilities.* 2023.

[15] Rehman, F. and S. Hashmi, *Enhancing Cloud Security: A Comprehensive Framework for Real-Time Detection Analysis and Cyber Threat Intelligence Sharing.* Advances in Science, Technology and Engineering Systems Journal, 2023. **8**(6): p. 107-119.

[16] Mihalcea, R., H. Liu, and H. Lieberman. *NLP (natural language processing) for NLP (natural language programming)*. in *Computational Linguistics and Intelligent Text Processing: 7th International Conference, CICLing 2006, Mexico City, Mexico, February 19-25, 2006. Proceedings 7*. 2006. Springer.

[17] Hassan, M., L.A.-R. Aziz, and Y. Andriansyah, *The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance.* Reviews of Contemporary Business Analytics, 2023. **6**(1): p. 110-132.

[18] Laskov, P., et al. *Learning intrusion detection: supervised or unsupervised?* in *Image Analysis and Processing–ICIAP 2005: 13th International Conference, Cagliari, Italy, September 6-8, 2005. Proceedings 13*. 2005. Springer.

[19] Mebawondu, J.O., et al., *Network intrusion detection system using supervised learning paradigm.* Scientific African, 2020. **9**: p. e00497.

[20] Kayode-Ajala, O., *Applying Machine Learning Algorithms for Detecting Phishing Websites: Applications of SVM, KNN, Decision Trees, and Random Forests.* International Journal of Information and Cybersecurity, 2022. **6**(1): p. 43-61.

[21] Eskin, E., et al., *A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data.* Applications of data mining in computer security, 2002: p. 77-101.

[22] Mvula, P.K., et al., *A Survey on the Applications of Semi-supervised Learning to Cyber-security.* ACM Computing Surveys, 2024. **56**(10): p. 1-41.

[23] Anagnostopoulos, C., *Weakly supervised learning: how to engineer labels for machine learning in cyber-security*, in *Data Science for Cyber-Security*. 2019, World Scientific. p. 195-226.

[24] Gopireddy, R.R., *Reinforcement Learning for Cyber Defense: Adaptive and Autonomous Security Systems.* European Journal of Advances in Engineering and Technology, 2023. **10**(10): p. 102-105.

[25] Rani, R., G. Epiphaniou, and C. Maple. *Reinforcement learning-based alert prioritisation in security operation centre: A framework for enhancing cybersecurity in the digital economy*. in *International Conference on AI and the Digital Economy (CADE 2023)*. 2023. IET.

[26] Banik, S. and S.S.M. Dandyala, *Reinforcement Learning for Adaptive Cybersecurity.* International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 2022. **13**(1): p. 366-382.

[27] Rahman, M.R., R. Mahdavi-Hezaveh, and L. Williams. *A literature review on mining cyberthreat intelligence from unstructured texts*. in *2020 International Conference on Data Mining Workshops (ICDMW)*. 2020. IEEE.

[28] Arazzi, M., et al., *NLP-Based Techniques for Cyber Threat Intelligence.* arXiv preprint arXiv:2311.08807, 2023.

[29] Gutiérrez, L.F. and A. Namin, *Contextminer: Mining contextual features for conceptualizing knowledge in security texts.* IEEE Access, 2022. **10**: p. 85891-85904.

[30] Mulugu, N., *AUTOMATED EMERGING CYBER THREAT IDENTIFICATION AND PROFILING BASED ON NATURAL LANGUAGE PROCESSING.*

[31] Sheth, H.S.K., A. Ilavarasi, and A.K. Tyagi. *Deep Learning, blockchain based multi-layered Authentication and Security Architectures*. in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*. 2022. IEEE.

[32] Sharma, R., K. Mehta, and P. Sharma, Role of Artificial Intelligence and Machine Learning in Fraud Detection and Prevention, in Risks and Challenges of AI-Driven Finance: Bias, Ethics, and Security. 2024, IGI Global. p. 90-120.

[33] Goodfellow, I., Deep Learning. 2016: MIT Press.

[34] Vähäkainu, P. and M. Lehto, Use of artificial intelligence in a cybersecurity environment, in Artificial intelligence and cybersecurity: Theory and applications. 2022, Springer. p. 3-27.

[35] Tan, E., A conceptual model of the use of AI and blockchain for open government data governance in the public sector. 2021, DIGI4FED Consortium. Retrieved from: https://soc. kuleuven. be/io/digi4fed ….

[36] Page, A., et al., SIEM+: Harnessing Machine Learning for Advanced Anomaly Detection in Cybersecurity Software.

[37] Diogenes, Y., N. DiCola, and T. Turpijn, Microsoft Azure Sentinel: Planning and implementing Microsoft's cloud-native SIEM solution. 2022: Microsoft Press.

[38] Peiris, C., B. Pillai, and A. Kudrati, Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks. 2021: John Wiley & Sons.

[39] Borra, P., Microsoft Azure Networking: Empowering Cloud Connectivity and Security. International Journal of Advanced Research in Science, Communication and Technology (IJARSCT) Volume, 2024. 4.

[40] Crawford, J., *The impact of artificial intelligence on autonomous cyber defense*. 2017, Utica College.

[41] BABS, M.-P.B., *Artificial Intelligence in Cyber security and Network security.*

[42] Tayyab, M., et al., *AI-Powered Threat Detection in Business Environments: Strategies and Best Practices*, in *Generative AI for Web Engineering Models*. 2025, IGI Global. p. 379-436.

[43] Ok, E., *Artificial Intelligence and Cybersecurity: Strengthening Defenses in the Digital Age.*

[44] Nasser, Y. and M. Nassar, *Toward Hardware-Assisted Malware Detection Utilizing Explainable Machine Learning: A Survey.* IEEE Access, 2023. **11**: p. 131273-131288.

[45] Brown, S., J. Gommers, and O. Serrano. *From cyber security information sharing to threat management*. in *Proceedings of the 2nd ACM workshop on information sharing and collaborative security*. 2015.

[46] Stergiopoulos, G., P. Dedousis, and D. Gritzalis, *Automatic analysis of attack graphs for risk mitigation and prioritization on large-scale and complex networks in Industry 4.0.* International Journal of Information Security, 2022. **21**(1): p. 37-59.

[47] Sancho, J.C., et al., *New approach for threat classification and security risk estimations based on security event management.* Future Generation Computer Systems, 2020. **113**: p. 488-505.

[48] Ganin, A.A., et al., *Multicriteria decision framework for cybersecurity risk assessment and management.* Risk Analysis, 2020. **40**(1): p. 183-199.

[49] Shah, V., *Machine learning algorithms for cybersecurity: Detecting and preventing threats.* Revista Espanola de Documentacion Cientifica, 2021. **15**(4): p. 42-66.

[50] Yeboah-Ofori, A., et al., *Cyber threat predictive analytics for improving cyber supply chain security.* IEEE Access, 2021. **9**: p. 94318-94337.

[51] Ajala, O.A., et al., *Review of AI and machine learning applications to predict and Thwart cyber-attacks in real-time.* Magna Scientia Advanced Research and Reviews, 2024. **10**(1): p. 312-320.

[52] Hoppa, M.A., et al., *Twitterosint: Automated open source intelligence collection, analysis & visualization tool.* Annual Review of Cybertherapy And Telemedicine 2019, 2019. **121**.

[53] Adewopo, V., B. Gonen, and F. Adewopo. *Exploring open source information for cyber threat intelligence*. in *2020 IEEE International Conference on Big Data (Big Data)*. 2020. IEEE.

[54] Silvestri, S., et al., *Cyber threat assessment and management for securing healthcare ecosystems using natural language processing.* International Journal of Information Security, 2024. **23**(1): p. 31-50.

[55] Florea, M., et al., *Complex project to develop real tools for identifying and countering terrorism: real-time early detection and alert system for online terrorist content based on natural language processing, social network analysis, artificial intelligence and complex event processing*, in *Challenges in cybersecurity and privacy-the European research landscape*. 2022, River Publishers. p. 181-206.

[56] Rozlomii, I., et al. *Data Protection in the Utilization of Natural Language Processors for Trend Analysis and Public Opinion: ryptographic Aspect*. in *Proceedings of the 2nd International Workshop on Social Communication and Information Activity in Digital Humanities (SCIA-2023)*. 2023.

[57] Mnassri, K., et al., *A survey on multi-lingual offensive language detection.* PeerJ Computer Science, 2024. **10**: p. e1934.

[58] Rashid, U., et al., *Anomaly Detection using Clustering (K-Means with DBSCAN) and SMO.* Journal of Computing & Biomedical Informatics, 2024. **7**(02).

[59] Nalavade, K. and B. Meshram, Evaluation of k-means clustering for effective intrusion detection and prevention in massive network traffic data. International Journal of Computer Applications, 2014. 96(7).

[60] Thudumu, S., et al., A comprehensive survey of anomaly detection techniques for high dimensional big data. Journal of Big Data, 2020. 7: p. 1-30.

[61] Nguyen, T.T. and V.J. Reddi, Deep reinforcement learning for cyber security. IEEE Transactions on Neural Networks and Learning Systems, 2021. 34(8): p. 3779-3795.

[62] Hossain, M.T., R. Afrin, and M.A.-A. Biswas, A Review on Attacks against Artificial Intelligence (AI) and Their Defence Image Recognition and Generation Machine Learning, Artificial Intelligence. Control Systems and Optimization Letters, 2024. 2(1): p. 52-59.

[63] Wei, W. and L. Liu, Robust deep learning ensemble against deception. IEEE Transactions on Dependable and Secure Computing, 2020. 18(4): p. 1513-1527.

[64] Banik, S. and S.S.M. Dandyala, Adversarial Attacks Against ML Models. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 2020. 11(1): p. 205-229.

[65] Al-Shehari, T. and R.A. Alsowail, Random resampling algorithms for addressing the imbalanced dataset classes in insider threat detection. International Journal of Information Security, 2023. 22(3): p. 611-629.

[66] Hoang, V.-T., et al., Security risks and countermeasures of adversarial attacks on AI-driven applications in 6G networks: A survey. Journal of Network and Computer Applications, 2024: p. 104031.

[67] Elahi, M.M., A user-centric exploration of transparency, explanations, and trust in multi-model and single-model decision support systems. 2023, Brunel University London.

[68] Vimbi, V., N. Shaffi, and M. Mahmud, Interpreting artificial intelligence models: a systematic review on the application of LIME and SHAP in Alzheimer's disease detection. Brain Informatics, 2024. **11**(1): p. 10.