RCHUB: JOURNAL OF COMPUTATIONAL INTELLIGENCE SCIENCE AND ENGINEERING (JCISE)
VOL: 2, ISSUE 2, APRIL-JUNE 2026
RCHUB PUBLISHER
ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/2/003

Review: Artificial intelligence based Cyber threat detection incorporating machine learning algorithm

Spoorthi B S[1], Namana D C[2], Rohan K[3] , Amrutha H P[4]
[1]Department of ECE , Malnad College of Engineering, Hassan
[2]Department of ECE , Malnad College of Engineering, Hassan
[3]Department of ECE , Malnad College of Engineering, Hassan
[4]Department of ECE , Malnad College of Engineering, Hassan

Abstract

Cybersecurity threats have grown more complex and frequent, creating serious risks for organizations, critical infrastructure, and individuals worldwide. Traditional signature-based security tools can no longer effectively identify and deal with advanced, evasive, and quickly changing cyber-attacks, such as zero-day exploits, ransomware, and multi-stage intrusion campaigns. As a result, there is a strong need for real-time cyber threat detection and response systems that adjust dynamically and offer timely, actionable information to security operations teams. This paper provides a detailed review of modern methods that combine machine learning (ML) and open-source intelligence (OSINT) gathered through automated web data scraping. Machine learning offers powerful analysis for spotting both known and unknown threats by recognizing patterns and detecting anomalies in various telemetry data, including network traffic, system logs, and endpoint activities. OSINT enhances these systems by supplying external insights into new vulnerabilities, threat actor tactics, techniques, and procedures (TTPs), as well as real-time cyber threat intelligence shared across open channels like social media, security forums, paste sites, and the dark web[1][2][3].By combining ML-based internal monitoring with continuously updated OSINT feeds, advanced systems improve threat classification accuracy, lower false alarms, and provide contextual information that aids proactive responses. This review looks into the key architectures, machine learning algorithms, and natural language processing techniques for analyzing OSINT, along with illustrative case studies in IoT, finance, and healthcare. It also highlights existing challenges, such as managing data quality, ensuring model robustness, and addressing privacy and compliance issues. It outlines future research directions, focusing on federated learning, explainability, and blockchain-enabled threat intelligence sharing. This paper aims to be a valuable resource for researchers and practitioners seeking more effective, adaptable, and integrated cyber security defence frameworks that can tackle the increasingly sophisticated threat landscape[4].

1. Introduction

The rapid growth of digital infrastructure has exposed organizations to complex cyber threats, including ransomware, phishing, and advanced persistent threats (APTs) that can evade traditional security tools. Real-time detection and response systems powered by machine learning are now crucial for identifying and reducing these threats proactively. By using machine learning's pattern recognition across extensive telemetry data and enhancing it with external threat intelligence gathered through automated web data scraping (OSINT), organizations can significantly improve their cyber defence. This paper examines these integrated methods, emphasizing architectures, machine learning techniques, and intelligence extraction workflows that drive modern cybersecurity operations[1][2][3]. The increasing interconnection of devices, cloud services, and online platforms, along with the growing sophistication of attackers, demands defences that can adapt quickly. Attackers use polymorphic malware, carry out stealthy lateral movements, and exploit weak external collaborations, making it hard for static defences to manage these situations.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/2/003

Therefore, integrating continuous, real-time data analytics through ML and extracting real-world indicators from OSINT is vital for improving detection accuracy and operational response[5][4]. Machine learning algorithms, such as supervised, unsupervised, and deep learning models, have proven effective in analysing complex, high-dimensional security data streams to find patterns that indicate malicious behaviour. At the same time, OSINT from sources like threat intelligence forums, vulnerability repositories, social media chatter, and dark web markets provides valuable context that broadens the visibility of internal monitoring systems. Automated web scraping is crucial for efficiently gathering this data at scale, helping organisations stay ahead of potential threats[3][6]. By combining these complementary capabilities, including internal telemetry analytics and external intelligence gathering, hybrid cyber defence frameworks enhance the speed, accuracy, and contextual relevance of threat alerts. This combination reduces false positives and supports faster, more informed incident responses, which are essential for minimizing attacker dwell time and operational impact[2][7][8].This review explores the latest developments and practical uses of intelligence real-time cyber threat detection and response systems. It details the architectures, machine learning models, OSINT collection processes, and challenges involved. use cases in industrial Io T, finance and healthcare show the applicability and advantages of these technologies. The review concludes with a discussion on research directions aimed at addressing current challenges related to scalability, privacy, and explainability. Our goal is to provide a valuable resource for academics and industry professionals dedicated to enhancing dynamic and intelligence–driven cyber security defence strategies[1][4][9].

2. Background and Related Work

The cybersecurity landscape has seen significant progress due to the use of machine learning and open-source intelligence (OSINT) techniques. Traditional security measures, which rely on predefined signatures and manual rules, are no longer enough to combat sophisticated cyber threats. These threats are often polymorphic and evolve quickly. Recently, machine learning (ML) has gained popularity because it can recognize patterns and detect anomalies in extensive telemetry data, such as network traffic, end point logs, and user behaviour analytics[1].Supervised learning algorithms, like Random Forest, Support Vector Machines (SVM), and gradient boosting classifiers, are often used to accurately label known malicious activities when trained on well-labelled datasets. On the other hand, unsupervised learning techniques such as clustering and auto encoders, help find new threats by spotting deviations from established baselines. Deep learning architectures that use recurrent (LSTM) and convolutional (CNN) neural networks are particularly good at handling complex data streams over time and space, aiding in more nuanced and scalable intrusion detection[2] .At the same time, OSINT has become a key source of external threat intelligence. This includes publicly available data gathered from social media, vulnerability disclosure platforms like the National Vulnerability Database (NVD), threat actor forums, paste sites and dark web marketplaces. Automatically scraping these varied and often unstructured sources helps security systems stay aware of new vulnerabilities, indicators of campaigns, and attacker Tactics, Techniques, and Procedures (TTPs). To turn this raw data into useful information, natural language processing (NLP) techniques such as named entity recognition, sentiment analysis, and transformer-based models like BERT and GPT are used. This adds semantic understanding to the data hybrid approaches that combine machine learning with continuously updated OSINT feeds have shown improved threat detection accuracy. They provide more context to alerts , reduce false positives, and help detect Advanced Persistent Threats (APTs) and zero-day exploits earlier. While earlier research has focused intensely on individual components, recent systematic surveys show that merging ML and OSINT methods leads to a stronger and more adaptable cybersecurity stance[1]. Despite these advancements, challenges still exist. Issues such as data diversity, understanding how models work, legal limits on data collections, and integrating real-time analytics into operations continue to drive on going research efforts. Digital Manufacturing (DM) is driven by Industry 40 technologies such as Io T ,AI, robotics, and cloud computing. It offers

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/2/003

efficiency and flexibility, but also introduces new cyber security risks. The paper identifies critical vulnerabilities in hybrid manufacturing systems, including attacks on design files (CAD,STL,G-code), machine controllers , sensors, and feedback loops. A threat taxonomy is presented, covering attacks like sabotage, counterfeiting, IP theft, denial-of- service, and side-channel leakage. The authors discuss real-world case studies of attacks, including ransom ware at Honda and firmware attacks on 3D printers. They propose defence strategies that include watermarking, anomaly detection, design obfuscation, and embedded part authentication. Overall, the survey emphasizes that securing DM requires a multi-layered approach. This should combine traditional IT and operational technology security with defences specifically designed for cyber-physical systems[16]. Data mining techniques for proactive cyber security threat detection. It shows how analysing large sets of cyber security data can uncover patterns that indicate possible attacks, including anomalies, intrusion signatures, and harmful behaviours. Key contributions include showcasing the effectiveness of clustering, classification, and association rule mining in detecting threats before they develop into serious breaches. The research also points out the need to combine data-driven methods with current cybersecurity frameworks to improve the accuracy of threat predictions and response times. Overall, the paper emphasizes that using data mining can improve situational awareness and offer a scalable, systematic way to reduce cyber security risks[24].

3. Architecture of Integration Detection and Response Systems

Designing systems for real-time cyber threat detection involves a modular setup that supports continuous data collection, processing, analysis, and immediate response. At the core is the data collection and integration layer, which gathers internal telemetry and external OSINT. Internal data sources include network traffic monitors, endpoint detection agents, log aggregators, and behavioural sensors. External OSINT is collected through automated web scraping tools that target threat intelligence forums, social networks, blogs, paste sites, and dark web channels[1] The processing layer readies various data streams by removing noise, standardizing formats, eliminating duplicate records , and applying feature engineering. This includes selecting relevant protocol fields, statistical traffic metrics , or keywords pulled from textual OSINT. Dimensionality reduction methods like Principal Component Analysis (PCA) simplify large data sets, making downstream analysis easier. The analytic core usually combines supervised and unsupervised machine learning models. Supervised classifiers get trained on labelled benign and malicious datasets, while unsupervised methods identify unusual patterns that might indicate new attacks. Deep learning networks handle complex multivariate data , which includes time-series network flows and unstructured OSINT text. Transformer-based NLP models pull out entities and classify threat discussions within the OSINT collection[2][3]. A correlation and fusion module improves accuracy and reduces false positives by cross-checking detections from both internal signals and OSINT-derived indicators. This multi-faceted cross-referencing helps prioritize threats and assess risk. The system's orchestration layer connects with SIEM (Security Information and Event Management) and SOAR (Security Orchestration, Automation, and Response) platforms to enable automated or analyst-led actions like isolating affected hosts, blocking malicious domains or IPs, or starting incident response workflows. Human operators interact with real-time dashboards that display analytics, historical trends, the reasoning behind models, and actionable alerts[4]. Maintaining low latency and high throughput requires scaling these components across distributed architectures using technologies like Apache Kafka, Spark Streaming, or cloud-native serverless frameworks. These designs help keep responsiveness high, which is crucial for minimizing how long attackers remain in the system while handling various, continuous OSINT and network flows in real time.

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/2/003

4. Machine Learning Techniques for Cyber Threat Classification

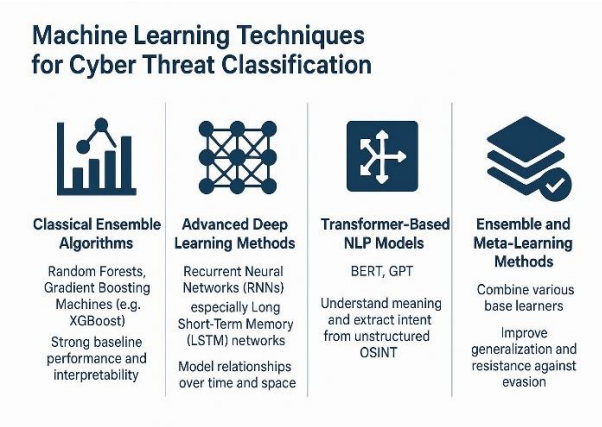

Figure 1. Key machine learning techniques for cyberthreat classification

Machine learning models are essential for threat classification systems. They convert raw security data into useful ratings or labels. Classical ensemble algorithms, like Random Forests and Gradient Boosting Machines (e.g., XGBoost), deliver strong baseline performance and maintain the interpretability needed for audits and compliance. These models effectively manage tabular data that represents session features, endpoint logs, or OSINT-derived metrics. Advanced deep learning methods enhance detection by modelling the relationships in the data over time and space. Recurrent Neural Networks (RNNs), especially Long Short-Term Memory (LSTM) networks, are ideal for analysing network behaviours over time. They help in identifying multi-stage attacks or command-and-control activities early. Convolutional Neural Networks (CNNs) work with structured data, like network traffic matrices or malware binary images. They can capture patterns that traditional methods might miss[2]. Transformer-based NLP models (e.g., BERT, GPT) significantly improve how we process open-source text. These models aid in understanding meaning, profiling threat actors, and extracting intent from unstructured OSINT, such as tweets, dark web posts, or vulnerability descriptions. Fine-tuning these models on large collections of cybersecurity data boosts their accuracy in labeling contextual threat intelligence and detecting threat campaigns. Ensemble and meta-learning methods combine various base learners. This approach improves generalization, lessens the biases of individual models, and enhances resistance against evasion techniques used by threat actors. Continuous retraining based on feedback and new data helps prevent model drift, ensuring effectiveness in changing environments. Explainability techniques (XAI) are increasingly used to help human analysts understand the reasons behind machine learning decisions. This understanding is crucial for building trust, conducting regulatory audits, and responding effectively to incidents[2].

5. Applications and Case Studies

Real-world deployment scenarios provide valuable insights into how integrated machine learning and open-source intelligence systems improve cybersecurity threat detection and response. Various industries and digital ecosystems have tailored these technologies to specific needs, revealing both advantages and challenges in adaptability.

Industrial Internet of Things (IIoT) Security

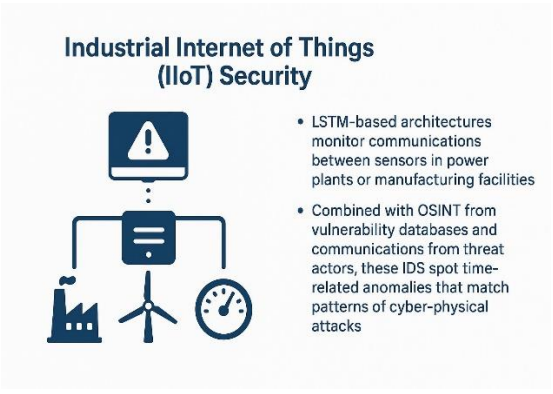

Figure2. LSTM based security architectures, enhanced with OSINT intelligence

In industrial and critical infrastructure settings, IoT devices generate vast amounts of continuous data. Traditional security systems often struggle to monitor this effectively. Using deep learning models in intrusion detection systems (IDS) has significantly improved the detection of unusual

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/2/003

device behaviors that suggest malware infections, misconfigurations, or insider threats. For instance, LSTM-based architectures monitor communications between sensors in power plants or manufacturing facilities. These models can spot time-related anomalies that match patterns of cyber-physical attacks. When combined with open-source intelligence (OSINT) gathered from vulnerability databases and communications from threat actors regarding specific IoT brands or protocols, these detection systems gain insight that helps prioritize patches and respond to threats more quickly[1][2].

Botnet Detection and Domain Name Analysis

Botnets continue to be a serious threat, facilitating large-scale DDoS attacks, spam campaigns, and credential theft. Detecting new botnets often involves identifying dynamically generated domain names used for command and control (C&C). Earlier methods that relied on blacklists faced issues with speed and coverage. New systems combine supervised machine learning models that analyze DNS query logs and domain generation algorithm (DGA) features. These models also leverage natural language processing (NLP) to parse OSINT sources discussing new botnet trends or identified DGAs. This dual approach allows for predicting malicious domains before they are exploited, effectively stopping botnet spread. Case studies in telecommunications networks show that detection accuracy has improved to over 95% with OSINT integration, significantly cutting down on false positives.

Financial Fraud and Insider Threat Detection

Financial institutions confront sophisticated attackers who exploit social engineering and advanced malware to defraud customers and the institutions themselves. Hybrid detection frameworks combine behavioral anomaly detection on transaction data with OSINT-driven threat intelligence that identifies phishing campaigns and credential stuffing attacks on social media. Real-time analysis of suspicious transaction patterns correlates with phishing URLs or leaked credentials flagged from online platforms, enabling timely customer alerts and fraud prevention. Likewise, the mitigation of insider threats benefits from integrated machine learning and OSINT systems that analyze both internal user behavior and external threat communications. These may indicate compromised credentials or collusion attempts. Pilot projects in major banks report faster response times and reduced financial losses, demonstrating the benefits of detection methods enhanced by external intelligence[2].

Healthcare Cyber Defense

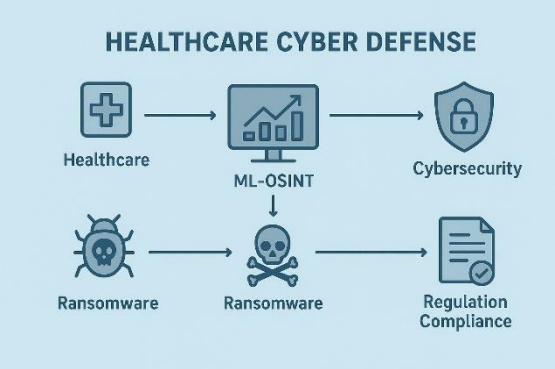

Figure 3. ML-OSINT strengthens healthcare cyber defense by enhancing cybersecurity

Healthcare settings face unique challenges due to the sensitive nature of patient data and a mix of legacy medical devices. Integrated ML-OSINT platforms help identify ransomware campaigns that target healthcare organizations. They correlate endpoint data and network behavior with real-time OSINT analysis of new ransomware signatures and tactics, techniques, and procedures (TTPs) found in threat intelligence feeds and underground markets. Furthermore, these systems help comply with health data regulations by integrating privacy-focused analytics and detecting anomalies. Applications at leading hospitals have successfully prevented costly service outages and data breaches by enabling proactive measures based on timely threat intelligence.

These applications highlight the benefits of combining internal analytics with OSINT to improve accuracy, decrease detection time, and create more effective mitigation strategies. Despite specific adaptations to various domains, challenges such as data variety, understanding detection

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/2/003

outputs, and integration complexity continue to exist.

6. Challenges and Limitations

While using machine learning and OSINT in cybersecurity is powerful, some ongoing challenges and limitations affect how systems are designed, deployed, and work effectively.

Data Quality and Volume Management

The amount of OSINT data online is enormous. It includes reliable indicators from trusted sources and large volumes of noisy, unclear, or misleading information. Extracting useful intelligence from this "information overload" needs advanced filtering and prioritization algorithms. False positives from unverified or duplicate OSINT can overwhelm alert systems and operators. Cleaning, removing duplicates, and scoring the relevance of scraped data are necessary but hard to achieve at scale, especially in near-real-time environments [3].

Adversarial Evasion and Model Drift

Attackers constantly change their tactics to evade detection. They alter malware signatures, use encryption or obfuscation, and apply adversarial machine learning techniques to confuse detection models. This ongoing struggle requires regular updates to ML models, constant training against adversarial threats, and using multiple approaches for better strength. However, retraining needs labeled data, which is hard to find for new or stealthy threats, and there is a risk of overfitting. Rapidly changing attack methods can cause models to drift, decreasing detection accuracy over time unless managed proactively.

Privacy, Legal, and Ethical Constraints

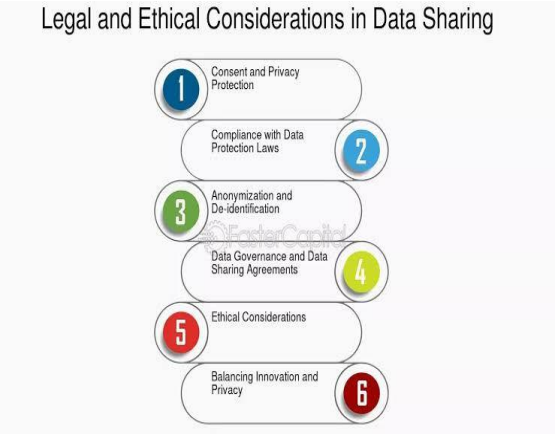

Figure 4. Legal and Ethical considerations in data sharing

Collecting, storing, and analyzing security data and OSINT raises significant privacy and legal issues. Web scraping can conflict with data usage rules, service terms, or laws like GDPR in Europe. Compliance requires careful data storage, anonymization, and secure handling, creating logistical and cost challenges. Finding a balance between useful threat intelligence and privacy rights is still a struggle. Ethical concerns also arise in reducing false accusations or harm from automated systems, especially in environments with multiple stakeholders like cloud services or critical infrastructure[3].

Explainability and Analyst Trust

Deep learning models at the heart of modern detection systems often work as "black boxes." This makes it tough for human analysts to understand or validate their decisions. The lack of clear explanations for flagged threats can quickly weaken analyst confidence and hinder investigations or regulatory checks. Explainable AI (XAI) techniques seek to fill these gaps but are still developing in cybersecurity and can impact performance. Creating systems that achieve high detection accuracy while offering clear reasoning is essential for their acceptance and effectiveness[4].

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/2/003

Integration Complexity and Operational Overhead

Setting up integrated ML-OSINT systems within existing infrastructure, various endpoints, cloud setups, and different threat intelligence platforms is complex. Ensuring smooth operation, speedy data flow, scalable computing, and real-time coordination requires a lot of engineering work, resource investment, and collaboration across teams. Smaller organizations often lack the expertise and budget to implement these advanced detection technologies.

7. Future Research Directions

As cyber threats become more complex and widespread, the field of real-time cyber threat detection and response must evolve by addressing current limitations and exploring new methods. Several promising research areas stand out for their potential to improve system capabilities, resilience, and usability.

Federated Learning for Privacy-Preserving Collaboration

Federated learning allows multiple organizations or distributed network nodes to collaboratively train machine learning models without sharing raw data. This approach is especially promising for cybersecurity, where sharing sensitive telemetry and threat intelligence is restricted due to privacy laws and competition. By sharing model parameters or aggregated gradients instead of actual datasets, federated learning helps increase the diversity of training data, enhancing model generalization while maintaining confidentiality. Research continues to focus on improving communication efficiency, model convergence, and adversarial robustness in federated systems designed for cyber threat detection.

Blockchain-Enabled Cyber Threat Intelligence (CTI) Sharing

The decentralized and unchangeable nature of blockchain technology provides a secure and trustworthy method for sharing cyber threat intelligence. Blockchain can ensure the provenance, auditability, and tamper-resistance of CTI shared across organizations and sectors. Combining blockchain with OSINT sharing platforms builds trust in the authenticity and integrity of shared intelligence, reduces duplication, and prevents misinformation. Research questions focus on scalability, privacy protection on public ledgers, and integration with real-time detection systems.

Automated Threat Action and TTP Extraction

Extracting detailed attack tactics, techniques, and procedures (TTPs) from various OSINT sources requires significant effort. Multimodal machine learning models that combine text, image, and network data show promise for automated TTP extraction and contextual threat action classification. Transformer architectures fine-tuned on cybersecurity-specific datasets improve the mapping of unstructured intelligence into structured actionable formats, speeding up incident response processes. Improving these models' ability to generalize across new threat campaigns is a key research challenge.

Explainable AI (XAI) for Cybersecurity

Despite the strengths of deep learning, the lack of transparency reduces analyst trust and complicates regulatory compliance. Developing AI models that provide interpretable explanations—such as feature attributions, attention visualizations, or simplified surrogate models—will enhance collaboration between humans and AI. Research in XAI for cybersecurity must find a balance between explainability, computational efficiency, and detection performance. User-focused evaluations to measure the effectiveness of explanations for incident responders are essential for practical adoption[1].

Adaptive and Autonomous Security Orchestration

Future systems will need to adapt dynamically to changing threats through autonomous security orchestration platforms that can make real-time decisions. By combining adaptive machine learning models with SOAR technologies, these platforms will automate detection, validation, and response actions seamlessly, reducing the need for human

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/2/003

intervention and speeding up mitigation. Including threat intelligence updates from OSINT feeds directly in orchestration policies will support context-aware, risk-based security automation. Research into safe and auditable autonomous decision frameworks is crucial to avoid unintended outcomes.

Additional Directions

Emerging research is also exploring how quantum computing can enhance cryptography to secure telemetry, strengthen adversarial machine learning defenses, and improve cross-domain cybersecurity intelligence sharing frameworks. Integrating IoT, cloud-native, and industrial control systems security under unified ML-OSINT detection frameworks addresses the growing complexity of digital infrastructures [2].

8. Conclusion

This review looked at real-time cyber threat detection and response systems that use machine learning and open-source intelligence gathered through automated web data scraping. Using internal telemetry analytics combined with regularly updated external intelligence leads to significant improvements in early threat detection, better classification accuracy, rich situational awareness, and faster response times. Different machine learning methods, including classical ensemble algorithms, deep learning models, and transformer-based natural language processing, work together to process large and varied security data. Real-world examples from industrial IoT, telecommunications, financial services, and healthcare show how hybrid ML-OSINT frameworks can boost effectiveness. However, ongoing issues related to data handling, adaptability to threats, privacy laws, explainability, and operational integration require ongoing focus and new ideas. In the future, promising research areas like federated learning, blockchain-based threat intelligence sharing, automated TTP extraction, explainable AI, and autonomous response orchestration are set to advance the next generation of cyber defense. By adopting these innovations and tackling current challenges, the cybersecurity community can develop more resilient, flexible, and trustworthy real-time detection and response systems needed to protect the increasingly complex digital environment. Ultimately, effective cyber defense depends on combining the strengths of data-driven machine learning with actionable threat intelligence from open-source sources. This evolving approach provides a strong method to tackle the rising and sophisticated cyber threats facing modern organizations and critical infrastructure.

References

[1.] Alshuaibi, M. Almaayah, and A. Ali, "Machine Learning for Cybersecurity Issues: A Systematic Review," Journal of Cyber Security and Risk Auditing, vol. 1, 2025, pp. 36, 46. DOI: 10.63180/jcsra.thestap.2025.1.4.

[2.] R. Kaur, "Artificial Intelligence for Cybersecurity: Literature Review and Future Directions," Journal of Network and Computer Applications, vol. 212, 2023, article 103484.

[3.] Aldhaheri et al., "Deep Learning for Cyber Threat Detection in IoT Networks: A Review," IEEE Internet of Things Journal, 2024.

[4.] F. Sufi, Z. Li, and R. Magalhães, "An Innovative GPT-Based Open-Source Intelligence Using Multidimensional Cyber Threat Features," ScienceDirect, 2024.

[5.] X. Zhang et al., "EX-Action: Automated Threat Action Extraction Using BERT," 2021.

[6.] M. Saeed et al., "A Systematic Literature Review on Cyber Threat Intelligence for Organizational Cybersecurity Resilience," Sensors, 2023.

[7.] H. Moraliyage et al., "Explainable Deep Learning for Onion Service Typing," IEEE Transactions on Information Forensics and Security, 2022.

[8.] S. Khan et al., "Anomaly Detection with Machine Learning in Cybersecurity," IEEE Transactions on Network and Service Management, 2022.

[9.] P. Koloveas et al., "Crawler and Dark Web Cyber Threat Intelligence Harvesting

ISSN: 3107-8168
DOI: https://doi.org/10.65725/JCISE/2/2/003

Architectures," Cybersecurity Informatics Conference, 2023.

[10.] S. Suryotrisongko, "Botnet Domain Generation Algorithm Detection with NLP and ML," 2022.

[11.] Mishra et al., "Machine Learning for Anomaly Detection in IoT Using MQTT Traffic," 2022.

[12.] Alsaedi et al., "CTI-Based Malicious URL Detection Using Ensemble Learning," 2022.

[13.] L. Gong and J. Lee, "BLOCIS: Blockchain Framework for Cyber Threat Intelligence Sharing," 2022.

[14.] K.D.O. Ofoegbu et al., "Real-Time Cybersecurity Threat Detection Using Machine Learning and Big Data Analytics," CSIT Research Journal, 2023.

[15.] M. Ejaz et al., "Machine Learning for Cyber Threat Intelligence Data Visualization," 2021.

[16.] P. Mahesh, "A survey of cybersecurity of digital manufacturing," Proceedings of the IEEE, vol. 109, no. 4, pp. 495, 516, Apr. 2021

[17.] M. V. Carriegos, "On aggregation and prediction of cybersecurity incident reports," IEEE Access, vol. 9, 2021

[18.] M. Sánchez-Paniagua, "Phishing URL detection: A real-case scenario through login URLs," IEEE Access, vol. 10, pp. 60696, 60710, 2022

[19.] P. Kyranoudi, "Sectoral cybersecurity skills gap: The case of maritime cybersecurity certification training," in Proc. 2024 IEEE Int. Conf. Eng., Technol. Innov. (ICE/ITMC), Funchal, Portugal, 2024, pp. 1, 8, doi: 10.1109/ICEITMC61174.2024.10705118

[20.] Sangwan, "Human factors in cybersecurity awareness," in Proc. 2024 Int. Conf. Intell. Syst. Cybersecurity (ISCS), Noida, India, 2024

[21.] R. Baskaran, Transforming Cybersecurity with AI: A Revolutionary Approach. Piscataway, NJ, USA: IEEE, 2025, doi: 10.1109/9781394220298

[22.] S. Vongsuvat, "Cybersecurity Threat Detection Analysis via Exploratory Data Analysis," 2024

[23.] B. Bokan and J. Santos, "Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures," in *Proc. 2021 Systems and Information Engineering Design Symposium (SIEDS)*, 2021

[24.] P. Kaushik, "Leveraging Data Mining for Cybersecurity Threat Detection," in *Proc. 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N)*, 2024

[25.] T. Rains and T. Youngblood, "Cybersecurity Threats, Malware Trends, and Strategies: Discover Risk Mitigation Strategies for Modern Threats to Your Organization." Packt Publishing, 2023

[26.] M. Aljaramiz, M. K, "Deep Learning-Driven Cybersecurity Threat Detection and Mitigation in Saudi Arabia Healthcare System," 2025

[27.] D. Sridevi, "Detecting Insider Threats in Cybersecurity Using Machine Learning and Deep Learning Techniques," 2023

[28.] T. Desai and R. K. Pal, "Machine Learning in Cybersecurity: A Review of Threat Detection, Prevention, and Response Strategies," 2025

[29.] H. Janardhanan, "A Reinforcement Learning Approach to Cybersecurity: Deep Q-Networks for Threat Modeling," in *Proc. 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS)*, 2025

[30.] T. R. Gadad, V. R., Y. B. K., and Y. H. Singh, "Machine Learning in Cybersecurity: Threat Detection and Response," 2025