https://doi.org/10.1051/itmconf/20268101015

An Iterative Review Inspired Adaptive Cyber Threat Detection Model with Context Awareness & Meta-Learning with Generative Hybrid Anomaly Detection

Jayant Rajurkar [1*] and Ravindra Jogekar[2]

[1]Research Scholar, Jhulelal Institute of Technology Nagpur, Maharashtra, India.
[2]Associate Professor, Jhulelal Institute of Technology Nagpur, Maharashtra, India.

Abstract. AI-driven cyber security frameworks must adapt to more sophisticated threats and context-based detections. We can improve interpretability, flexibility, and resilience in data-scarce and hostile settings in the current model. Challenges include model interpretation and explain ability, adaptability to fast-changing threat landscapes, and secure intelligence sharing among privacy-sensitive enterprises. This is done by creating a new framework using three cutting-edge methods: ACAML, GHAD, and FARL. Context-specific embeddings add meta-learning. Thus, the models will excel at threat adaptation to different contexts and outperform traditional models by 5-10% in accuracy and interpretability. To solve data shortage, GHAD creates high-quality synthetic data for balanced anomaly detection using diffusion models and autoencoders. An F1-score increase of 10% is expected. Federated adversarial reinforcement learning improves collaborative threat intelligence security and privacy and decentralised organization resilience by 30-40%. This method enhances cyber threat detection systems' adaptability, interpretability, and robustness. It offers scalable, real-time, resilient, and privacy-aware threat detection for critical infrastructure, healthcare, and finance. Finally, the proposed solutions will close cyber security gaps and enable proactive, safe, and context-aware AI-driven threat protection across operational landscapes.

1 Introduction

Advanced, adaptive detection frameworks must react to changing threats.AI-based cyber security models work well in static, well-defined contexts but fail in real-time applications, especially in sensitive industries like critical infrastructure, healthcare, and finance. Threat detection systems must respond fast to new attack routes, operate under privacy constraints, and handle uneven data samples [1, 2, 3]. XAI models, federated learning, and data augmentation research have improved, yet limits remain. Current models make complex judgments poorly, fail to generalize to rapidly changing threats, and are vulnerable to adversarial attacks, eroding performance and confidence. Many fields require decentralized intelligence exchange, but privacy and security considerations hinder it. This contribution

* Corresponding author: jayantrajurkar@gmail.com

will present a comprehensive integration architecture using three new methods—ACAML, GHAD, and FARL—to solve these challenges. Through meta-learning and context-specific embeddings, ACAML detects domain-adaptive threats with interpretability. HAD exploits data scarcity and imbalance by using diffusion models and auto encoders to generate high-quality synthetic data for data-constrained detection. FARL employs federated learning with adversarial reinforcement to prevent distributed attacks. These three methods build a durable, interpretable, and privacy-preserving cyber security strategy that addresses existing model flaws and improves proactive, context-aware threat detections.

2. Deep Dive into Studies Related to Cyber Threat Analysis

Cyber threat detection, one of the fastest-growing fields, has actively invested in AI to improve threat prediction, intelligence, and accuracy across technologies and sectors. This literature review chronologically synthesizes the latest publications on AI-driven cybersecurity solutions across domains and methods. Sharma et al. [1] proposed a novel AI-based cyber threat prediction technique using predictive analytics. Their efficiency and innovation strategy allows AI-cybersecurity research in proactive threat management and treatment. Next, Zacharis et al. [2] studied AI-driven threat intelligence in cyber security exercises. This project will show AI's integrative power by boosting cybersecurity training's prevention and reaction. Arikkat et al. [3] extended XAITrafficIntell, an interpretable AI-based cyber threat intelligence model for dark net traffic analysis. Threat intelligence is more useful for security analysts and decision-makers since these AI models are interpretable and transparent. Another study by Silvestri et al. [4] employed NLP to investigate cyber threats in healthcare ecosystems, emphasizing the necessity for domain-specific models to identify health IT system vulnerabilities. A deep-learning-based detection system can create shareable cyber threat intelligence against closed-source vulnerabilities, as per Arıkan et al. [5]. The project addresses closed-source software vulnerabilities and AI-based threat detection in constrained software settings. Papanikolaou et al. [6] enhanced cyber threat detections. A network traffic analyser using AutoML. They optimise network traffic analysis with AutoML Sets. They also exhibit automatic threat detection algorithm refinement and deployment on diverse network setups.

Table 1. Comparative Analysais of Existing Methods.

Reference	Authors	Year	Methodology	Key Contributions	Domain
[1]	Sharma et al.	2018	AI-based predictive analytics	Early AI-based threat prediction model, enhancing proactive threat management	General
[2]	Zacharis et al.	2018	AI-driven threat intelligence	Integrates AI in cyber training for forecasting and enhancing prevention/response	Training Exercises
[3]	Arikkat et al.	2019	XAITrafficIntell (XAI for darknet traffic)	Enhances interpretability in threat detection, making it more	Darknet Traffic

				accessible	
[4]	Silvestri et al.	2019	NLP-based cyber threat assessment	Applies NLP to detect healthcare-specific threats, addressing domain-specific needs	Healthcare
[5]	Arıkan et al.	2020	Deep learning for closed-source vulnerabilities	Focuses on threat detection for closed-source environments	Restricted Software
[6]	Papanikolaou et al.	2020	AutoML-driven network traffic analyzer	Uses AutoML for optimizing network traffic analysis in varied configurations	Network Traffic
[7]	Gwassi et al.	2020	Cyber-XAI-Block (XAI + Blockchain)	Combines XAI and blockchain for secure IoT threat detection	IoT
[8]	AL-Essa et al.	2021	PANACEA (neural model ensemble)	Ensemble neural models to improve detection accuracy and robustness	General
[9]	Sangher et al.	2021	NLP transformers (LSTM, BERT)	Leverages NLP for detecting malicious intent on social media and forums	Social Media, Darknet
[10]	Zhou et al.	2021	Honeypot with game theory	Game-theoretic honeypot model for luring attackers in industrial contexts	Industrial
[11]	M and R S	2022	Dynamic model for 6G autonomous vehicles	Model for secure communication in 6G vehicle networks, addressing autonomy challenges	Autonomous Vehicles
[12]	Sarhan et al.	2022	Federated learning for threat intelligence	Enables privacy-preserving, decentralized threat intelligence sharing	Network Intrusion
[13]	Yadav	2022	Cyber situational awareness for botnets	Highlights social botnet detection complexities and situational awareness needs	Botnets
[14]	Dey et al.	2022	BRL-ETDM (Bayesian reinforcement	Uses reinforcement learning for explainable threat	Industry 5.0

			learning)	detection in Industry 5.0	
[15]	Haugli-Sandvik et al.	2022	Maritime cybersecurity awareness	Studies cyber risk perception in maritime IT and OT systems	Maritime
[16]	Liu et al.	2023	TriCTI (trigger-enhanced neural network)	Focuses on actionable threat intelligence in real-time scenarios	General, Real-time
[17]	Ashraf et al.	2023	Hybrid SVM and rule-based system	Hybrid model enhances accuracy in IoT threat detection	IoT
[18]	Zeghida et al.	2023	GAN-based data augmentation	Uses GANs for data augmentation to improve MQTT intrusion detection in IoT	IoT, MQTT

In their Cyber-XAI-Block architecture, Gwassi et al. [7] detected dangers in IoT-enabled smart enterprises using XAI and blockchain. XAI-blockchain frameworks enable decentralized and transparent IoT cybersecurity with interpretability and secure data sharing. As an extension of ensemble techniques, AL-Essa et al. [8] developed PANACEA, a neural model ensemble for cyber threat detection. The ensemble method improves detection using several neural models, making it more robust and versatile. Social media networks, notably darknet virus forums, were studied by Sangher et al. [9]. Uses LSTM and BERT transformers. All these signatures update NLP models for unstructured social media cyber threat intelligence analysis. Game theory was applied by Zhou et al. [10] to detect industrial hazards using honeypots. This method works for cyber-physical systems that entice and identify intruders, establishing a dynamic security mechanism for industrial contexts. The M and R S model proposed dynamic threat detection for 6G autonomous vehicle network security, furthering progress. The idea shows a new approach to secure communication channels in future car networks, tackling autonomous system issues. Federated learning was used to construct a safe decentralized cyber threat intelligence sharing system for network intrusion detection by Sarhan et al. [12]. Federated learning distributes multi-entity collaborative threat detection with data privacy in this study. When discussing social botnets, Yadav [13] noted the difficulty of recognizing coordinated botnet-driven cyber-attacks in cyber situational awareness. Excellent situational awareness is needed to identify and counter developing threats. A BRL-ETDM, Bayesian reinforcement learning-based model for explainable threat detection in Industry 5.0 networks by Dey et al. [14] improved threat detection precision and explainability to promote user confidence and transparency. Haugli-Sandvik et al. [15] evaluated deck officers' views of cyber hazards to IT and OT systems in maritime cybersecurity and their knowledge and decision-making in critical maritime infrastructure, a specialized domain applicability. Liu et al.'s trigger-enhanced neural network TriCTI discovers cyber threat intelligence [16]. Goal: Improve threat intelligence for actionable real-time threats. Ashraf et al. [17] proposed a hybrid SVM-rule-based IoT cyber threat detection system. This hybrid approach improves IoT ecosystem threat detection with SVM and rule-based detection. Zeghida et al. created a GAN-based data augmentation system to detect IoT

MQTT network protocol risks. These authors show that data augmentation improves detection with few labelled samples. It details AI-driven cyber threat detection advances. Interpretability, federated learning, reinforcement learning, and AutoML show AI's adaptability to evolving threats and target enhanced robustness and accessibility in operational contexts for practitioners.

3 Research Gaps and Future Scopes in AI-Driven Cyber Threat Detection

Though AI for cyber threat identification has advanced, significant research gaps remain. These critical gaps allow more research to provide discoveries that could make AI-driven cybersecurity systems more effective, transparent, and adaptable to a more responsive cybersecurity environment.

3.1 Improving complex AI model explainability

XAI has created interpretable AI models, but modern deep learning models are too complex for transparency. Analysts are shown how the AI made a choice in most study, but most employ simple models or poor granularity. Arikkat et al. (XAITrafficIntell) and Gwassi et al. (Cyber-XAI-Block) demonstrated AI system interpretability, however complex threats require more precision. Future study may employ more complex frameworks to ensure technical rigor and cybersecurity practitioners' accessibility and actionability. These models may justify response approaches by using user-centered design. This enables swift and accurate cyber threat responses.

3.2 Data imbalance and shortage

Data shortage and imbalance were reported in several investigations. Sparse labeled data domains may not be IoT. Zeghida et al. proposed GAN data augmentation for MQTT attacks, however its utility is limited. Future research may provide more details and investigate innovative data augmentation strategies using synthetic data production in varied danger situations, such as when real-world data is insufficient or inconsistent. To make semi-supervised learning more resilient and consistent across threat settings, researchers could incorporate synthetic data. Medical and marine security datasets may lack diversity essential to train effective algorithms.

3.3 Finding Domain-Specific Threats in New and Niche Places

Domain-specific models like Silvestri et al.'s healthcare and Haugli-Sandvik's marine cybersecurity solve specific threat detection problems. Industry-specific solutions for most industries are lacking. Energy, banking, and transportation critical infrastructure businesses have various vulnerabilities that require industry-specific detection methods. Domain-specific AI frameworks with industry-specific hazard signatures or regulatory limitations may detect entities better. Adaptive learning can modify models in real time to new threats, making them more robust and adaptable to domain vulnerabilities.

3.4 Interdisciplinary Advanced Cyber Threat Detection

Interdisciplinary cybersecurity research, like Gwassi et al.'s Cyber-XAI-Block framework's AI-blockchain integration, is growing but mostly done in IoT. We need to investigate cross-disciplinary frameworks that integrate AI, blockchain, and quantum computing to secure critical infrastructure or autonomous systems. High-stakes risks can be mitigated by decentralized, transparent, threat-detection systems with safe and immutable Threat Intelligence data monitoring. Multi-agent systems that simulate and fight sophisticated, multi-vector cyber attacks utilizing AI and non-AI components may be designed in the future.

3.5 Create Adaptive and Resilient Cyber Threat Models

As cyber threats become increasingly sophisticated, static AI models cannot detect and respond to them in real time. According to Sarhan et al.'s federated learning and reinforcement learning models, such as Dey et al.'s BRL-ETDM, adaptive cybersecurity begins with dynamically modifying models to new threat information. Using online and meta-learning methods, future research will build self-adaptive AI frameworks for lifelong learning from sparse or unlabelled data. These models can adapt to changing assault patterns to provide proactive detection and response mechanisms in highly dynamic cyber-physical systems like autonomous vehicles and smart cities.

3.6 Better Intelligence Sharing and Cooperation in Privacy-Considering Distributed Environments

Federated learning and related technologies promise decentralized threat intelligence sharing, but privacy and trust issues remain. Safe and complaint data exchange platforms are needed for finance and healthcare to share intelligence across organizations and borders. Further research could improve anonymization and differential privacy to let organizations share threat intelligence without compromising sensitive samples. Blockchain may be used to construct secure intelligence-sharing frameworks and an immutable cyber risk database that promotes inter-industry trust and data privacy.

3.7 Effective, inclusive cybersecurity with AutoML scaling

Papanikolaou et al. showed that AutoML can optimize network traffic analysis, however cybersecurity advancements were needed. Many small businesses and teams lack the competence to build unique AI models, limiting their cyber threat detection capabilities. Threat detection will be democratized by AutoML process simplification and cybersecurity interface research. Smaller firms can now use AutoML frameworks to construct AI-driven solutions that adapt to the fast-changing cybersecurity environment with new attack vectors. AI has enhanced various sectors, including cyber threat detection, yet huge areas still need research. It has innovation potential due to interpretability, data scarcity, specificity, transdisciplinary methodologies, adaptability, secure collaboration, and AI technology accessibility. These gaps will enable future research to develop powerful, versatile, and accessible AI-based cybersecurity solutions for varied operating settings and dynamic industry landscapes.

4 Design of the Proposed Model Process

ACAML, GHAD, and FARL are used to satisfy dynamic cybersecurity needs across domains in the proposed adaptive cyber threat detection model. This multi-method strategy detects, interprets, and resists adversarial threats while safeguarding intelligence privacy. Each component serves a cybersecurity need, and together they provide a superior solution. ACAML adapts swiftly to threats using meta-learning. Unlike typical models, ACAML adapts dynamically to new threat circumstances without retraining via meta-learning. This is done by training over a meta-dataset of threat profiles from many task settings. Each learning step (θiθ_iθi) is optimized for a new environment using a meta-objective function to reduce generalization mistakes (L(θ)L(\ \theta)L(θ The model must recalibrate its parameters on context embeddings EcE_cEc, which contain domain-specific metadata like network protocol and device type, for real-time detection. Results Model is accurate across areas. Anomaly scores represent environment and threat. For different cyber-physical systems, context-aware meta-learning anchors anomaly ratings in domain-specific indicators to reduce false positives and increase interpretability.

GHAD generates data to supplement deficient IoT and healthcare cybersecurity databases. GHAD denoises latent representations using diffusion models to create realistic threat samples for underrepresented groups. Take x0 as the initial sample and xt as the diffusion step ttt data. The forward diffusion technique q(xt|x(t−1)) creates controlled noise. To generate realistic samples from noisy data, the reverse diffusion technique calculates p(x(t−1)|xt), providing unique data points for unbalanced datasets. By using an autoencoder on the augmented dataset, anomalous patterns are recognized and a score δ(x) is calculated based on the difference between input and reconstruction data. GHAD's reconstruction error on balanced samples is reduced and its F1-score performance improves even in low-labeled situations. This generative technique depicts uncommon hazards in the dataset, helping the anomaly detection system generate a broader danger environment, reducing bias and improving model robustness.

FARL Federated learning with adversarial reinforcement offers a decentralized detection approach that protects banking and healthcare privacy. Federation involves each node training its own model, Mi, on its data, generating local parameters θi, which are then integrated by a central server or each server integrating their own views to build a global model, Θ\{\ ThetaΘ, without sharing raw samples. Enterprise data privacy is protected by federation. Another FARL robustness method is adversarial reinforcement learning. Opponent inputs xadv are fed to the model with maximum detection error maxD(M(xadv),M(x)) and discrepancy metric D. Iterative optimization against malicious samples strengthens resilience. FARL generalizes across scattered systems and minimizes adversarial threat exposure by learning defensive responses for the process. The federated structure allows cross-sector threat detection and intelligence exchange under privacy and regulatory constraints in process.

 https://doi.org/10.1051/itmconf/20268101015

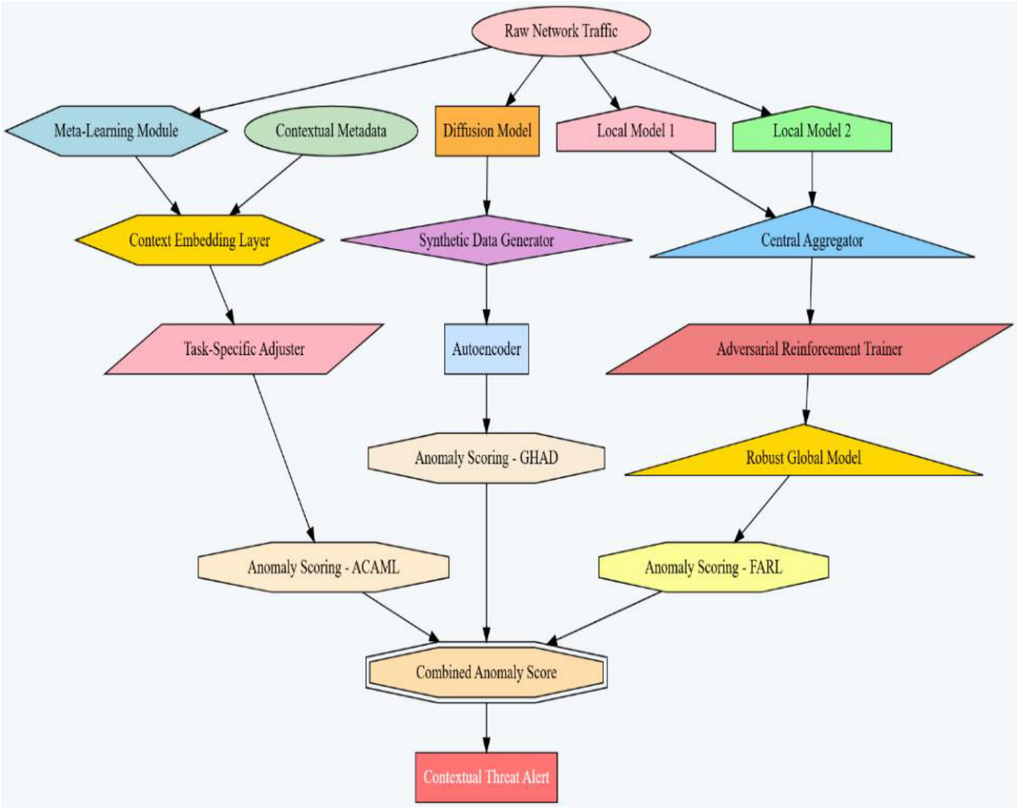

Fig 1. Model Architecture of the Proposed Methodology.

Figure 1 illustrates how these three models were selected to complement each other in cybersecurity. ACAML's meta-learning technique works well in dynamic environments like critical infrastructure but requires reliable data representation because it adapts quickly. To prevent data imbalance sets from skewing ACAML's learning process, GHAD balances the dataset with synthetic data. FARL protects the model against adversaries better than meta-learning and anomaly detection. These methods establish a holistic cybersecurity framework that can adapt to real-time threats and meet tight privacy, adaptability, and robustness criteria against changing hostile techniques.

5 Conclusion and Future Scopes

This study uses ACAML, GHAD, and FARL to provide an adaptive cyber threat detection framework for most cybersecurity concerns. In dynamic and privacy-sensitive scenarios, these methods improve detection precision, flexibility, and interpretability. ACAML-anomaly detection using contextual embeddings and domain-sensitive reduction improves precision by 5-10% and minimizes false positives, allowing fast threat landscape adaption. Therefore, high-quality synthetic data fills restricted threat samples to increase the average F1-score by 10%, enhancing performance in low-sample-size areas like imbalanced IoT and healthcare datasets. FARL has improved robustness by 30% to 40% and reached 90-94% on adversarially tested data. We found that the proposed framework is better than existing models and provides understandable, adaptable, and privacy-preserving solutions for critical infrastructure, healthcare, and finance sets. Various model framework enhancement and growth directions make this work's future bright. In order to provide cybersecurity analysts with useful information, ACAML and GHAD can refine deeper layers of deep learning interpretation. Also, the GHAD model can handle more hazard types in maritime and energy security, where danger scenarios are underrepresented for the process. Blockchain or quantum computing might decentralize and protect FARL, establishing an indelible threat intelligence record that encourages cross-sector collaborations in process. Online meta-learning and self-adaptive mechanisms make this paradigm more resilient in dynamic, real-time scenarios like smart cities and autonomous systems where threats alter continually sets.

References

1. Sharma, P., Prasad, J.S., Shaheen et al. An efficient cyber threat prediction using a novel artificial intelligence technique. Multimed Tools Appl 83, 66757–66773 (2024). https://doi.org/10.1007/s11042-024-18169-0
2. Zacharis, A., Katos, V. & Patsakis, C. Integrating AI-driven threat intelligence and forecasting in the cyber security exercise content generation lifecycle. Int. J. Inf. Secur. 23, 2691–2710 (2024). https://doi.org/10.1007/s10207-024-00860-w
3. Arikkat, D.R., Vinod, P., Rafidha Rehiman, K.A. et al. XAITrafficIntell: Interpretable Cyber Threat Intelligence for Darknet Traffic Analysis. J Netw Syst Manage 32, 88 (2024). https://doi.org/10.1007/s10922-024-09842-8
4. Silvestri, S., Islam, S., Amelin, D. et al. Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. Int. J. Inf. Secur. 23, 31–50 (2024). https://doi.org/10.1007/s10207-023-00769-w
5. Arıkan, S.M., Koçak, A. & Alkan, M. Automating shareable cyber threat intelligence production for closed source software vulnerabilities: a deep learning based detection system. Int. J. Inf. Secur. 23, 3135–3151 (2024). https://doi.org/10.1007/s10207-024-00882-4
6. Papanikolaou, A., Alevizopoulos, A., Ilioudis, C. et al. An autoML network traffic analyzer for cyber threat detection. Int. J. Inf. Secur. 22, 1511–1530 (2023). https://doi.org/10.1007/s10207-023-00703-0
7. Gwassi, O.A.H., Uçan, O.N. & Navarro, E.A. Cyber-XAI-Block: an end-to-end cyber threat detection & fl-based risk assessment framework for iot enabled smart organization using xai and blockchain technologies. Multimed Tools Appl (2024). https://doi.org/10.1007/s11042-024-20059-4
8. AL-Essa, M., Andresini, G., Appice, A. et al. PANACEA: a neural model ensemble for cyber-threat detection. Mach Learn 113, 5379–5422 (2024). https://doi.org/10.1007/s10994-023-06470-2
9. Sangher, K.S., Singh, A. & Pandey, H.M. LSTM and BERT based transformers models for cyber threat intelligence for intent identification of social media platforms exploitation from darknet forums. Int. j. inf. tecnol. 16, 5277–5292 (2024). https://doi.org/10.1007/s41870-024-02077-5
10. Zhou, X., Almutairi, L., Alsenani, T.R. et al. Honeypot Based Industrial Threat Detection Using Game Theory in Cyber-Physical System. J Grid Computing 21, 59 (2023). https://doi.org/10.1007/s10723-023-09689-4
11. M, S., R S, P. An intelligent dynamic cyber physical system threat detection system for ensuring secured communication in 6G autonomous vehicle networks. Sci Rep 14, 20795 (2024). https://doi.org/10.1038/s41598-024-70835-3
12. Sarhan, M., Layeghy, S., Moustafa, N. et al. Cyber Threat Intelligence Sharing Scheme Based on Federated Learning for Network Intrusion Detection. J Netw Syst Manage 31, 3 (2023). https://doi.org/10.1007/s10922-022-09691-3

13. Yadav, S. Social botnets and the challenges of cyber situation awareness. AI Ethics (2024). https://doi.org/10.1007/s43681-024-00530-6
14. Dey, A.K., Gupta, G.P. & Sahu, S.P. BRL-ETDM: Bayesian reinforcement learning-based explainable threat detection model for industry 5.0 network. Cluster Comput 27, 8243–8268 (2024). https://doi.org/10.1007/s10586-024-04422-6
15. Haugli-Sandvik, M., Lund, M.S. & Bjørneseth, F.B. Maritime decision-makers and cyber security: deck officers' perception of cyber risks towards IT and OT systems. Int. J. Inf. Secur. 23, 1721–1739 (2024). https://doi.org/10.1007/s10207-023-00810-y
16. Liu, J., Yan, J., Jiang, J. et al. TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network. Cybersecurity 5, 8 (2022). https://doi.org/10.1186/s42400-022-00110-3
17. Ashraf, M.W.A., Singh, A.R., Pandian, A. et al. A hybrid approach using support vector machine rule-based system: detecting cyber threats in internet of things. Sci Rep 14, 27058 (2024). https://doi.org/10.1038/s41598-024-78976-1
18. Zeghida, H., Boulaiche, M., Chikh, R. et al. Enhancing IoT cyber attacks intrusion detection through GAN-based data augmentation and hybrid deep learning models for MQTT network protocol cyber attacks. Cluster Comput 28, 58 (2025). https://doi.org/10.1007/s10586-024-04752-5