ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a1

Al-Noor Journal for Information Technology and Cybersecurity

https://jncs.alnoor.edu.iq/

Learning to Secure: A Survey on Meta-Learning Approaches in Cyber Threat Detection and Response

[1]Balqees Talal Hasan1, [1]Zaid J. Al-Araji

[1]Department of Computer Networks and Internet, College of Information Technology, Ninevah University, Ninevah 41001, Iraq.

Article information

Article history:
Received: August, 18,2025
Revised: August, 31,2025
Accepted: September, 22, 2025

Keywords:
Meta-Learning
Cybersecurity
IDS
Threat Detection
Few-Shot Learning

Correspondence:

Zaid J. Al-Araji
zaid.jasim@uoninevah.edu.iq

Abstract

The increasing sophistication and dynamism of cyber threats demand security systems that can adapt rapidly to new and evolving attack patterns. Meta-learning, or "learning to learn," offers a promising paradigm for enhancing the adaptability and generalization of machine learning models in cybersecurity contexts. This survey presents a review of recent research on meta-learning approaches applied to cyber threat detection and response, with a particular focus on intrusion detection systems, malware classification, phishing detection, anomaly detection, and adversarial defense. We categorize existing methods into optimization-based, metric-based, and model-based meta-learning, and examine their strengths in few-shot learning, task generalization, and robustness under domain shifts. Furthermore, we identify key challenges, including the lack of standardized benchmarks, computational overhead, explainability limitations, and vulnerability to adversarial attacks. By synthesizing recent advances and outlining open research questions, this paper aims to guide future developments in adaptive, intelligent cybersecurity systems by using meta-learning to enhance the attack detection or even to protect the systems.

DOI: https://doi.org/10.69513/jncs.v2.i2.a1

1. Introduction

The exponential growth of digital infrastructure, coupled with the increasing sophistication of cyber-attacks, has made cybersecurity a critical domain of global concern [1,2]. As modern systems, including Internet of Things (IoT), Industrial IoT (IIoT), and cloud-native architectures—become more interconnected, they are simultaneously exposed to a wider array of attack vectors, including malware, ransomware, zero-day exploits, phishing campaigns, and advanced persistent threats (APTs) [3,4]. Traditional security mechanisms, such as rule-based systems and static machine learning models, have shown efficacy in known attack scenarios but often fail to generalize or adapt when confronted with novel or evolving threats, particularly in dynamic or adversarial environments [5,6].

Recent advances in machine learning (ML) have contributed significantly to threat detection and response tasks, including intrusion detection systems (IDS), malware classification, and anomaly detection. However, conventional ML models typically rely on large volumes of labeled data, are computationally intensive to retrain, and often perform poorly in low-data or few-shot scenarios [7]. These limitations pose significant obstacles in cybersecurity, where real-time decision-making and adaptability are paramount.

Meta-learning, or "learning to learn," offers a promising solution to these challenges by enabling models to quickly adapt to new tasks using knowledge acquired from related tasks during a meta-training phase. In contrast to standard ML paradigms, meta-learning models are designed to generalize across task distributions and require only a few labeled examples to fine-tune on unseen data—making them especially suited for zero-day attack detection, few-shot malware classification, and cross-domain anomaly detection[8,9]. Techniques such as Model-Agnostic Meta-Learning (MAML),

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a1

Prototypical Networks, and Siamese Neural Networks have shown notable performance improvements in security-sensitive domains, including IoT networks and mobile cyber-defense environments [10,11].

Despite these advances, the integration of meta-learning into cybersecurity is still in its early stages and faces several open challenges. These include the lack of standardized benchmarks, computational complexity in real-time settings, interpretability concerns, and vulnerability to adversarial manipulation [12,13]. Moreover, the growing need for privacy-preserving learning has spurred research into federated meta-learning, which combines the benefits of distributed learning and rapid task adaptation [14].

This paper provides a comprehensive survey of recent research on meta-learning applications in cyber threat detection and response. We aim to:

- Present foundational concepts in both cybersecurity and meta-learning.
- Classify meta-learning algorithms used in security into optimization-based, metric-based, and model-based methods.
- Review state-of-the-art applications in intrusion detection, malware analysis, anomaly detection, and adversarial defense.
- Identify key limitations and challenges, such as generalization, scalability, and robustness.

By reviewing and analyzing the intersection of meta-learning and cybersecurity, this survey will serve as a resource for researchers and practitioners working to develop adaptive, intelligent, and robust threat detection systems.

The remainder of this survey is organized as follows: Section 2 explains the background and preliminaries of meta-learning. Section 3 demonstrates Meta-Learning in Cybersecurity. Section 4 explains Applications of Meta-Learning in Cyber Threat Detection, while Section 5 describes Meta-Learning Methods and Frameworks in Use, and Section 6 explains and list Challenges and Limitations and Section 7 explains the Conclusion.

2. Background and Preliminaries

This section establishes the foundational concepts essential for understanding how meta-learning techniques are increasingly applied within cyber threat detection and response systems. We first review the evolving cybersecurity landscape and then introduce meta-learning fundamentals.

2.1 Cyber Threat Detection and Response

Increasing interconnectivity across digital infrastructures has elevated the prevalence and sophistication of cyber threats—including intrusion attempts, malware, phishing, insider attacks, and adversarial exploits. Traditional security mechanisms rely heavily on static rules or conventional machine learning (ML) models trained on large, labeled datasets and thus struggle when facing novel or low-prevalence attacks [4,15].

Threat detection involves identifying malicious or anomalous behavior within data streams, systems, or networks. Common techniques include signature-based detection and statistical anomaly detection [16]. More recently, supervised ML classifiers have been applied; however, their efficacy diminishes when data are scarce (e.g., zero-day attacks), imbalanced, or high-dimensional [14,17]. Threat response, on the other hand, refers to actions such as alert generation, enforcement of security policies, or automated model adaptation. Effective response mechanisms must rapidly adapt to ever-evolving threat patterns with minimal human intervention [18].

IoT and IoMT environments exacerbate such challenges. For instance, [19] use MAML to build an adaptive IDS that achieved ~99% F1-scores on benchmark datasets (e.g. UNSW-NB15, NSL-KDD), underscoring meta-learning's potential in IoT security contexts. Similarly, integration of meta-learning into ensemble-based IDS for IoMT has shown promising enhancements of performance and robustness [20].

2.2 Meta-Learning Fundamentals

Meta-learning—often described as "learning to learn"—enables models to quickly adapt to new tasks with minimal data by leveraging knowledge gained from related tasks [21]. Unlike traditional ML models which require retraining for each new task, meta-learners extract transferable knowledge during a meta-training phase [8].

Meta-learning is also called learning-to-learn. Its first proposition was in the educational science community, which appeared even earlier than machine learning. The concept of "meta-learning" was first proposed by Maudsley [21] in 1979 and then was introduced into the field of machine learning. Up to now, meta-learning has become an important research branch in the field of machine learning. Meta-learning is a learning model different from traditional machine learning. The sample set and query set are all sampled from the labeled data set [5], as shown in Figure 1.

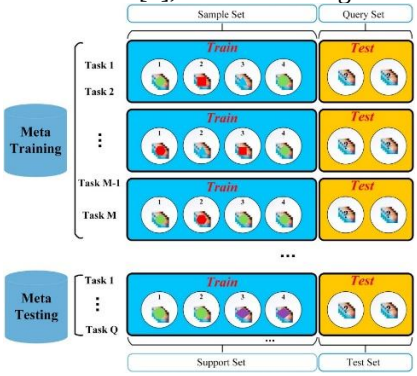

Figure 1: Division of the datasets in meta-learning [21]

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a1

A widely accepted taxonomy categorizes meta-learning approaches into:

- **Optimization-based**: Techniques such as Model-Agnostic Meta-Learning (MAML) aim to learn a model initialization amenable to rapid fine-tuning on new tasks.
- **Metric-based**: Methods like Prototypical Networks and Matching Networks learn embedding spaces or similarity metrics useful for few-shot classification and anomaly detection, though their use in security-specific datasets remains emerging.
- **Model-based**: Architectures such as memory-augmented networks or recurrent controllers that internally encode fast adaptation mechanisms.

2.3 Why Meta-Learning Fits Cybersecurity

Meta-learning is particularly well-suited to threat detection and response due to several compelling properties:

1. **Rapid adaptation to novel threats**: Few-shot capability allows models to generalize to new attack types with scarce labeled examples—as shown by [8] in malware classification, which integrates augmentation techniques and tailored learning schedules to outperform standard approaches in few-shot malware detection
2. **Robustness in dynamic environments**: Meta-trained systems can endure shifts in data distribution and adapt to new contexts—critical in adversarial or rapidly changing settings. Yet studies like [22] reveal meta-learners may be vulnerable to adversarial poisoning attacks targeting their meta-training process
3. **Adaptation with sparse data**: In cybersecurity scenarios such as zero- or one-shot threats, meta-learning surmounts traditional ML's dependence on extensive labeled data. Surveys have identified that traditional ML methods often perform poorly in such low-data regimes, while meta-learning offers scalable generalization across tasks
4. **Compatibility with federated and distributed architectures**: Federated Meta-Learning frameworks provide privacy-preserving adaptation across distributed nodes. Research such as federated-meta-IDS [14] showcases frameworks combining Meta-Learning with federated learning in fog-based systems for dynamic IoMT security detection.

3. Meta-Learning in Cybersecurity: A Conceptual Overview

This section articulates why meta-learning is particularly well-suited for cyber threat detection and response, especially in contexts of fast adaptation, few-shot learning, and generalization to novel attacks. It also identifies security-specific constraints that meta-learning can mitigate.

3.1 Why Meta-Learning Meets Cybersecurity Needs

3.1.1 Rapid Adaptation

Cybersecurity environments evolve rapidly with novel attack vectors emerging frequently [22]. Meta-learning—especially optimization-based methods like MAML—learns model initializations that can be fine-tuned extremely quickly using only a few samples from newly observed threats . For example, [19] applied MAML to IoT intrusion detection across UNSW-NB15 and NSL-KDD datasets, achieving over 99% F1-score after minimal adaptation, highlighting meta-learning's rapid adaptability in dynamic, heterogeneous environments

3.1.2 Data Efficiency

Many cyber threats, particularly zero-day malware or rare intrusion types, present extremely limited labeled data. Meta-learning enables models to perform well under few-shot conditions by learning to generalize across tasks. [22] introduced MI-MAML—a few-shot malware classifier combining augmentation with meta-optimization—and significantly improved performance over conventional approaches in scarce-data malware classification tasks. Similarly, a few-shot malware detection study [9] achieved ~97% accuracy using prototypical networks on hardware-counter features with few samples per class.

3.1.3 Generalization Capability

Metric-based meta-learners (e.g., prototypical networks, Siamese architectures) build embedding spaces that facilitate classification of entirely new attack classes via distance-based inference. This enables detection of previously unseen threats without full retraining. For instance, ConvProtoNet [23] demonstrated strong few-shot generalization across malware families by learning robust convolutional prototypes

3.1.4 Robustness in Dynamic and Adversarial Environments

Meta-learning frameworks can adapt to domain shifts and evolving threat distributions. [11] proposed INFUSE, an ensemble-based meta-learner that integrates deep autoencoders and multiple classifiers to detect network intrusions—with consistently high accuracy across diversified attack scenarios (≈ 91%) on stringent benchmark datasets, demonstrating robustness under distributional change.

3.1.5 Integration with Federated and Distributed Architectures

Distributed settings (e.g. IoT, industrial environments) require privacy-preserving and adaptive threat response [24]. Federated meta-learning frameworks enable centralized meta-training and localized adaptation. Recent studies (e.g. in MAML-federated IDS for fog-based IoMT) show promise in deploying meta-trained detection models across distributed nodes while preserving user data privacy [19].

3.2 Security-Specific Challenges Meta-Learning Addresses

1. **Data Imbalance and Scarcity**

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a1

Traditional supervised ML fails when one class (e.g. normal traffic) dominates. Meta-learning's few-shot mechanisms mitigate this imbalance by enabling learning from limited examples in underrepresented threat classes [5].

2. Shift Distribution Across Environments

Cybersecurity models often encounter shifts in network behavior—different IoT conditions, regions, or protocols. Meta learning enables task-agnostic initialization resilient to such shifts, as demonstrated by cross-dataset adaptation experiments [19].

3. Real-Time and Resource Constraints

Security applications demand fast inference and low latency. Some meta-learning intrusion detection models use prototype-based metric learners or lightweight feature modules enhanced by GAN-generated synthetic instances for real-time deployment (e.g. Res-Natural GAN + prototype networks in 5G industrial IoT) to balance speed and accuracy [24].

4. Model Robustness and Adversarial Safeguards

While meta-learning enables faster adaptation, it may still be vulnerable to poisoning or adversarial manipulation during meta-training. Ongoing research emphasizes robust meta-training procedures and attention-based architectures to mitigate susceptibility [5].

4. Applications of Meta-Learning in Cyber Threat Detection

This section systematically reviews how meta-learning has been applied to key cyber threat detection tasks. We focus on intrusion detection, malware classification, phishing and social engineering detection, anomaly detection in network/system logs, and adversarial attack detection. Representative studies illustrate how meta-learning frameworks enable fast adaptation, few-shot generalization, and robustness in evolving threat scenarios.

Intrusion detection remains a critical domain benefiting from meta-learning's ability to generalize and adapt with limited training data. [25] proposed a few-shot meta-learning framework (FC-Net) that distinguishes network traffic samples in a pairwise fashion. FC-Net achieved detection rates up to 99.62% even when training and testing across disjoint datasets. Building on this, [11] introduced INFUSE, a deep neural network-based meta-learning intrusion detector combining autoencoders and ensemble stacking. INFUSE achieved over 90% accuracy across diverse, evolving attack types and addressed dataset shift in intrusion detection. [16] presents a meta-learning-based model designed to improve the adaptability and real-time response of network intrusion detection systems against emerging attacks. By combining depthwise separable convolutions and a meta-learning framework, the model can quickly adapt to different types of attacks with few training samples and achieve efficient detection in the face of evolving network threats. For 5G-enabled Industrial IoT environments, a novel meta-learning IDS was proposed by [24]: it integrates a Res-Natural GAN for synthetic sample generation, a multi-head fast attention transformer encoder, and a prototype-based classification module. This few-shot model supports zero-shot generalization and real-time deployment while enhancing detection speed and accuracy. An approach based on meta-learners is proposed by [26] for detecting attacks on IoT attacks. This meta-learner approach is trained using the output of the stacked DL models. A thorough evaluation of different meta-learner models is conducted to assess the influence of the stacked DL models on the performance of the meta-learner. An adaptive intrusion detection framework using MAML and few-shot learning paradigms to quickly adapt to new tasks with little data was proposed by [19]. The goal of this research is to improve the security of IoT by developing a strong IDS that will perform well across assorted datasets and attack environments. [7] presented a meta-learning-based adaptable feature fusion strategy to improve few-shot network intrusion detection. The study also explained that obtaining a sufficiently high number of samples for training intrusion detection models was difficult because few network traffic samples were available. The method used metric-based meta-learning and adaptive feature fusion to solve the few-shot learning problems. Another work, [14] fuses federated learning with meta-learning, enabling distributed IDS across IoMT devices. This framework maintains high detection performance while preserving data privacy by conducting local, adaptive finetuning on each node.

Meta-learning has seen strong adoption in malware classification, particularly under few-shot conditions, A multi-improved MAML variant designed for few-shot malware detection. [8] introduced two task-tailored augmentation techniques (grayscale and L*a*b color manipulation), as well as custom network architectures and learning rate schedules. The model demonstrated superior generalization and classification accuracy over standard MAML approaches. [10] propose a novel task-aware few-shot-learning-based Siamese Neural Network that is resilient against the presence of malware variants affected by such control flow obfuscation techniques. Using the average entropy features of each malware family as inputs, in addition to the image features, the model generates the parameters for the feature layers, to more accurately adjust the feature embedding for different malware families, each of which has obfuscated malware variants. [27] propose a few-shot meta-learning based Siamese Neural Network that not only detects ransomware attacks but is able to classify them into different classes. The proposed model utilizes the entropy feature directly obtained from ransomware binary files to retain more fine-grained features associated with different

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a1

ransomware signatures. These entropy features are used further to train and optimize our model using a pre-trained network (e.g. VGG-16) in a meta-learning fashion.

5. Meta-Learning Methods and Frameworks in Use

This section provides an in-depth examination of both the meta-learning algorithms adopted in cyber threat detection studies and the software frameworks, model architectures, and platforms utilized in practice.

5.1 Categories of Meta-Learning Algorithms Applied in Security

5.1.1 Optimization-based Methods

Model-Agnostic Meta-Learning (MAML) and its variants remain foundational in security-focused applications, especially for intrusion detection in IoT contexts. For example, [19] developed a MAML-based IDS that achieved ~99.98% accuracy on UNSW-NB15 and NSL-KDD datasets, enabling rapid adaptation to unseen attacks. Similarly, MI-MAML [8] adapts MAML with tailored augmentation and architecture for few-shot malware classification, yielding enhanced generalization and classification metrics over baseline methods. Though FOMAML and Reptile are widely recognized in surveys of meta-learning, specific security studies have favored MAML-based variations due to their broad adaptability.

5.1.2 Metric-based Methods

Metric-based approaches are notably prevalent in malware classification and intrusion detection tasks. [10] implemented a task-aware Siamese neural network suitable for few-shot classification of control-flow obfuscated malware, achieving over 91% accuracy with just a few examples per class. In intrusion detection, [7] proposed a metric-learning IDS using Adaptive Feature Fusion (AFF), demonstrating strong performance across binary and multi-class few-shot network traffic classification tasks. Prototypical networks have also been applied in anomaly detection settings, often combined with augmentation or ensemble techniques.

5.1.3 Meta-Reinforcement Learning and Adversarial Approaches

Although fewer in number, meta-reinforcement learning paradigms are emerging in adversarial threats, especially for crafting and defending against evasive malware. [28] introduce an innovative meta-learning approach for multi-family Android malware classification named Meta-MAMC, which uses meta-learning technology to learn meta-knowledge (i.e., the similarities and differences among different malware families) of few-family samples and combines new sampling algorithms to solve the above challenges. This can be viewed as an inverse of meta-learning—learning strategies to defeat classifiers—but illustrates the broader interplay of meta-RL in both offensive and defensive security applications.

5.1.4 AutoML & Neural Architecture Search (NAS)-Driven Meta-Learning

Some recent research explores integrating meta-learning with AutoML and NAS to automate classifier configuration for varied security tasks. For example, an AutoAI-IDS system auto-tunes hyperparameters and model architectures within a meta-learning framework to optimize intrusion detection performance across datasets—suggesting potential for scalable, adaptive security model pipelines. However, detailed applications within cybersecurity remain sparse, representing an open frontier.

6. Challenges and Limitations

Despite its growing adoption in cybersecurity, meta-learning faces a range of domain-specific challenges that hinder its full deployment in threat detection and response systems. These challenges are both technical and practical, and recent literature highlights the following critical limitations:

6.1. Lack of Standardized Benchmarks

The absence of universally accepted benchmarks for evaluating meta-learning approaches in cybersecurity significantly restricts reproducibility and cross-method comparisons. While benchmarks like Omniglot and MiniImageNet are prevalent in traditional meta-learning research, they are ill-suited for security applications such as malware detection, intrusion detection systems (IDS), or phishing recognition. This has led to fragmented evaluation protocols and difficulty in gauging progress across different studies.

6.2. Generalization Across Domains

A key goal of meta-learning is the ability to generalize across tasks and domains. However, in cybersecurity, threat landscapes are highly non-stationary. Threats vary by network type, protocol, geography, and attacker behavior. Models trained on one domain often fail to generalize to others due to domain shift and concept drift.

6.3. Computational Overhead

Meta-learning frameworks typically involve two levels of training—base learning and meta-level optimization—which significantly increases computational demands. This is particularly challenging in cybersecurity, where real-time or near-real-time responses are essential. Methods like MAML or Reptile, while effective, may not scale efficiently when applied to large-scale or streaming security datasets. High latency can pose a major bottleneck in time-sensitive tasks such as zero-day attack mitigation.

6.4. Interpretability and Explainability

Many meta-learning algorithms, especially those built on deep learning, operate as black boxes. This undermines trust and adoption in critical security domains, where human analysts require insight into model decisions for compliance, validation, and

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a1

remediation. A lack of explainability can result in false positives or negatives being dismissed without understanding the rationale, which can be costly in adversarial settings. Explainable AI (XAI) tools for meta-learning in cybersecurity remain underdeveloped.

6.5. Adversarial Robustness

Cybersecurity systems are inherently adversarial, and adversaries can adapt to exploit the meta-learner's vulnerabilities. Recent work has shown that meta-learners are susceptible to adversarial perturbations in both the support and query sets, potentially leading to severe misclassifications. This raises concerns about model poisoning during meta-training and necessitates robust meta-learning algorithms that can withstand adversarial interference.

7. Conclusion

In this survey, we explored the growing role of meta-learning as a transformative approach for enhancing adaptability, efficiency, and generalization in cyber threat detection and response systems. As the threat landscape becomes increasingly complex and dynamic, traditional machine learning techniques—while powerful—often fall short due to their dependence on large, labeled datasets and limited capacity to adapt to novel or evolving attacks. Meta-learning, with its core promise of learning to learn, offers an effective solution to these limitations by enabling models to generalize across tasks and adapt to new threats with minimal supervision. Our review categorized the key methodologies—optimization-based, metric-based, and model-based meta-learning—and examined their deployment across a wide range of cybersecurity domains including intrusion detection, malware classification, and anomaly detection. Special emphasis was placed on few-shot learning capabilities, which are especially valuable in scenarios where labeled data is scarce or unavailable, such as zero-day attacks. Despite its promise, several challenges remain. These include the lack of standardized benchmarks for evaluation, scalability issues due to high computational overhead, limited interpretability, and vulnerability to adversarial manipulation. Addressing these limitations requires interdisciplinary research that combines advances in meta-learning with techniques in explainable AI, adversarial defense, and federated learning. Overall, this survey underscores that meta-learning is not merely a theoretical innovation, but a practical tool with the potential to significantly enhance the resilience and intelligence of next-generation cybersecurity systems.

References

[1] Z.J. Al-Araji, S.S. Syed Ahmad, M.W. Al-Salihi, H.A. Al-Lamy, M. Ahmed, W. Raad, N. Md Yunos, Network Traffic Classification for Attack Detection Using Big Data Tools: A Review, Intelligent and Interactive Computing: Proceedings of IIC 2018 (2019) 355–363.

[2] F.S. Alghareb, B.T. Hasan, Smart healthcare: emerging technologies, applications, challenges, and future research directions, Smart Cities (2023) 132–157.

[3] F. Liu, M. Li, X. Liu, T. Xue, J. Ren, C. Zhang, A review of federated meta-learning and its application in cyberspace security, Electronics (Basel) 12 (2023) 3295.

[4] M. Malatji, A. Tolah, Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI, AI and Ethics 5 (2025) 883–910.

[5] C. Xu, J. Shen, X. Du, A method of few-shot network intrusion detection based on meta-learning framework, IEEE Transactions on Information Forensics and Security 15 (2020) 3540–3552.

[6] A. Yang, C. Lu, J. Li, X. Huang, T. Ji, X. Li, Y. Sheng, Application of meta-learning in cyberspace security: A survey, Digital Communications and Networks 9 (2023) 67–78.

[7] J. Bo, K. Chen, S. Li, P. Gao, Boosting Few-Shot Network Intrusion Detection with Adaptive Feature Fusion Mechanism, Electronics (Basel) 13 (2024) 4560.

[8] Y. Ji, K. Zou, B. Zou, Mi-maml: classifying few-shot advanced malware using multi-improved model-agnostic meta-learning, Cybersecurity 7 (2024) 72.

[9] K. Alfarsi, S. Rasheed, I. Ahmad, Malware classification using few-shot learning approach, Information 15 (2024) 722.

[10] J. Zhu, J. Jang-Jaccard, A. Singh, P.A. Watters, S. Camtepe, Task-aware meta learning-based siamese neural network for classifying control flow obfuscated malware, Future Internet 15 (2023) 214.

[11] A. Sohail, B. Ayisha, I. Hameed, M.M. Zafar, H. Alquhayz, A. Khan, Deep neural networks based meta-learning for network intrusion detection, ArXiv Preprint ArXiv:2302.09394 (2023).

[12] H. Xu, Y. Li, X. Liu, H. Liu, J. Tang, Yet meta learning can adapt fast, it can also break easily, in: Proceedings of the 2021 SIAM International Conference on Data Mining (SDM), 2021: pp. 540–548.

[13] Z.J. Al-Araji, M.S. AlKhaldee, A.A. Mutlag, Z.A. Abdulkadhim, H.M. Farhood, S.S.S. Ahmad, N.N. Hikmat, A. Yassen, A.A.I. Al-Dulaimi, N.N.H. Al-Sheikh, others, Healthcare Security in Edge-Fog-Cloud Environment using Blockchain: A Systematic Review, Mesopotamian Journal of CyberSecurity 5 (2025) 606–635.

[14] U. Zukaib, X. Cui, C. Zheng, D. Liang, S.U. Din, Meta-Fed IDS: Meta-learning and Federated learning based fog-cloud approach to detect known and zero-day cyber attacks in IoMT networks, J Parallel Distrib Comput 192 (2024) 104934.

[15] Z. Alaaraji, A. Mutlag, Implement Edge pruning to Enhance attack graph generation using Naïve approach algorithm, El-Cezeri Fen ve Mühendislik Dergisi (2024). https://doi.org/10.31202/ecjse.1375755.

[16] G. Li, M. Wang, A Meta-learning Approach for Few-shot Network Intrusion Detection Using Depthwise Separable Convolution, Journal of ICT Standardization 12 (2024) 443–470.

[17] Z.J. Al-Araji, S.S.S. Ahmad, H.M. Farhood, A.A. Mutlag, M.S. Al-Khaldee, Attack graph-based security metrics: concept, taxonomy, challenges and open issues, in: BIO Web Conf, EDP Sciences, 2024. https://doi.org/10.1051/bioconf/20249700085.

[18] F. Liu, M. Li, X. Liu, T. Xue, J. Ren, C. Zhang, A review of federated meta-learning and its application in cyberspace security, Electronics (Basel) 12 (2023) 3295.

[19] F.S. Alrayes, S.U. Amin, N. Hakami, An Adaptive Framework for Intrusion Detection in IoT Security Using MAML (Model-Agnostic Meta-Learning), Sensors (Basel) 25 (2025) 2487.

[20] M. Alalhareth, S.-C. Hong, Enhancing the internet of medical things (IoMT) security with meta-learning: a performance-driven approach for ensemble intrusion detection systems, Sensors 24 (2024) 3519.

[21] A. Yang, C. Lu, J. Li, X. Huang, T. Ji, X. Li, Y. Sheng, Application of meta-learning in cyberspace security: A survey, Digital Communications and Networks 9 (2023) 67–78.

ISSN: 3078-5367 **DOI:** https://doi.org/10.69513/jncs.v2.i2.a1

[22] H. Xu, Y. Li, X. Liu, H. Liu, J. Tang, Yet meta learning can adapt fast, it can also break easily, in: Proceedings of the 2021 SIAM International Conference on Data Mining (SDM), 2021: pp. 540–548.
[23] Z. Tang, P. Wang, J. Wang, ConvProtoNet: Deep prototype induction towards better class representation for few-shot malware classification, Applied Sciences 10 (2020) 2847.
[24] Y. Yan, Y. Yang, F. Shen, M. Gao, Y. Gu, Meta learning-based few-shot intrusion detection for 5G-enabled industrial internet, Complex & Intelligent Systems 10 (2024) 4589–4608.
[25] C. Xu, J. Shen, X. Du, A method of few-shot network intrusion detection based on meta-learning framework, IEEE Transactions on Information Forensics and Security 15 (2020) 3540–3552.
[26] S.D.A. Rihan, M. Anbar, B.A. Alabsi, Meta-learner-based approach for detecting attacks on internet of things networks, Sensors 23 (2023) 8191.
[27] J. Zhu, J. Jang-Jaccard, A. Singh, I. Welch, H. Al-Sahaf, S. Camtepe, A few-shot meta-learning based siamese neural network using entropy features for ransomware classification, Comput Secur 117 (2022) 102691.
[28] Y. Li, D. Yuan, T. Zhang, H. Cai, D. Lo, C. Gao, X. Luo, H. Jiang, Meta-learning for multi-family android malware classification, ACM Transactions on Software Engineering and Methodology 33 (2024) 1–27.