Meta-Learning–Driven Intrusion Detection for Zero-Day Attack Adaptation in Cloud-Native Networks

Vimal Raja Gopinathan
Senior Principal Consultant, Oracle Financial Service Software Ltd, Washington, USA

Abstract

Zero-day attacks are a very critical factor to cloud-native networks because they are evolving in nature, dynamic load, and highly distributed networks. Conventional intrusion detection systems (IDS) whose models are built on a fixed set of rules or under the watch of a supervised learning model find it difficult to generalize new attack patterns and changing traffic patterns which happen very fast. The article presents a Meta-Learning-Based Intrusion Detection Framework that is intended to allow adapting to zero-day attacks in cloud-native applications quickly. The given method is based on Model-Agnostic Meta-Learning (MAML) combined with deep neural network classifiers to acquire transferable representations with respect to a wide range of attack conditions. The features are container-level, network-flow, and system-call-based features, which are extracted out of cloud-native workloads on Kubernetes-based infrastructure. In meta-training, the model is presented with several attack tasks so that it is exposed to new, unseen attacks with little labeled samples. Hybrid dataset that is comprised of CICIDS2017, UNSW-NB15, and artificially created traces of zero-day attacks is used to evaluate the experiment. The proposed model attains a mean detecting precision of 96.8, F1-score of 0.964 and 21 percent faster detection speed than the traditional deep learning-based IDS models. The performances have shown better conformability, lower false positives and better strength in the face of concept drift. The results uphold that meta-learning is one of the most effective strategies in strengthening the resistance of zero-day attacks, and thus the suggested framework is ideal in the intrusion detection process of elastic cloud-native networks in real-time.

Keywords: Artificial Intelligence, Cybersecurity, Intrusion Detection Systems, Machine Learning, Threat Detection, Anomaly Detection

DOI: 10.21590/ijhit.06.01.03

1. Introduction

Cloud-native networks have become the foundation of a new digital infrastructure and allow organizations to deploy, scale and manage large-scale applications faster than ever. Microservices, containerization, virtualization and orchestration platforms like

Kubernetes are technologies that have radically changed the manner in which applications are designed and run. Cloud-native architectures provide better scalability, fault tolerance, and resource efficiency in the form of de-monolithic systems by breaking down monolith systems into loosely coupled services. Nevertheless, the very same features also pose new and challenging security dilemmas and intrusion detection becomes a more challenging and a highly priority task [1].

Application components in cloud-native settings are very dynamic and short-lived. Containers can be deployed and removed in a matter of seconds, workloads can be automatically scaled depending on demand and services often interact by communicating east-west within the cluster. Such environments do not readily fit traditional perimeter-based security model that mainly monitors northsouth traffic. The speed of the deployment and continuous integration/continuous delivery (CI/CD) pipelines only exacerbate the security risks by making less time to conduct a manual security assessment. Therefore, cloud-native network presents a much larger and more dynamic attack surface as compared to traditional enterprise networks.

The Intrusion Detection Systems (IDS) remain critical in detecting malicious activities and ensuring the integrity of the network [2]. The simplicity and interpretability of signature-based IDS solutions have led to extensive usage based on the use of predetermined attack patterns of known attackers. These systems are however basically reactive and do not work with zero-day attacks that take advantage of vulnerabilities that have not been realized before. Even minor changes in the attack pattern can go unnoticed, making signature-based methods inadequate to deal with the current threat environment [3].

To circumvent such shortcomings, IDS models based on machine learning (ML) have been suggested to learn network traffic behavior patterns based on network traffic data. By using statistical and temporal features, supervised and semi-supervised learning algorithms have been shown to have better detection accuracy of known classes of attacks. However, the models of ML-based IDS have big problems with cloud-native environments. A significant one is the concept drift in which the statistical characteristics of network traffic vary over time because of workloads, user behavior, and the structure of the infrastructure. Historical data models can be quite inaccurate when subjected to novel network patterns or denial of service techniques [4].

These further problems are enhanced by zero-day attacks. These attacks take advantage of the vulnerabilities in a system that have never been discussed by the system designers and security analysts and therefore there is no previous signatures or any data labeled to be used as training. Attackers in cloud-native networks are able to leverage service-to-

service trust relationships and misconfigurations and spread zero-day exploits within microservices easily due to their lateral propagation. Timely detection is even harder given the large volume and heterogeneity of the telemetry data generated in the infrastructure, platform, and application levels. Due to this, IDS solutions cannot just be limited to static learning paradigms but rather show adaptability, scalability and tolerance to changing threats [5].

Some of these problems have been promising to be resolved using deep learning methods to model non-linear relationships in high-dimensional data. Convolutional Neural Networks (CNNs), which are architectures, are able to learn spatial correlations among traffic characteristics, and Recurrent Neural Networks (RNNs) and Long Short-term memory (LSTM) networks can learn temporal correlations. Combination deep learning models have also enhanced the detected accuracy of known attacks on benchmark datasets. Although they exist, it is a fact that deep learning-based IDS systems continue to be heavily dependent on large, labeled datasets and periodic retraining, which is not practical in the face of zero-day attacks in fast-evolving cloud-native systems.

One of the main weaknesses of traditional deep learning models is the lack of ability to generalize to unknown attack classes. The models tend to label malicious traffic as normal when they are presented with a zero-day attack because they tend to be based on patterns that have been learned. The retraining models to ensure the inclusion of new attack data is slow and computationally intensive and hence, it is not suitable when one is dealing with operational cloud environments where quick response is needed. Thus, it is experiencing a severe shortage of solutions to IDS that can be adjusted to the new threats in a short period of time and with minimum labelled data.

A nice solution to this issue can be presented by metalearning, or sometimes it is called learning to learn. In contrast to traditional learning methods that help to optimize models with reference to a single task, meta-learning trains models on several related tasks to acquire transferable knowledge. This allows the quick acquisition of new tasks using very few training samples. In intrusion detection, meta learning enables IDS model to learn the experience of various kinds of attacks and apply it to identify an attack that has not been previously witnessed. This feature is especially useful in the zero-day attack detection, where there are limited or no labeled data.

Metalearning is naturally well-suited in the cloud-native environments that are multi-tasks in nature. Every microservice, workload, tenant, or deployment environment can be regarded as its own learning task having its own traffic patterns and security features. Meta-learning is capable of utilizing this diversity to learn generalized representations that are resistant to service and type of attack. By combining meta-learning and deep

neural networks, the IDS systems can be able to balance between expressive modeling capacity and quick adaptability.

In this paper, a Meta-Learning-Driven Intrusion Detection Framework is proposed, which is specifically used to adapt to the zero-day attacks in cloud-native networks. In the proposed structure, the Model-Agnostic Meta-Learning (MAML) is used to train a deep classifier, which can be fine-tuned quickly when presented with novel pattern of attacks. The structure is designed to work on Kubernetes-based systems, which can be easily integrated with cloud-native monitoring and telemetry systems. Multi-layered data collection on network, container and system level gives a holistic picture of runtime behaviour which increases the detection accuracy and resilience.

The main works of this work are four-fold. Originally, we offer a new meta-learning-based IDS architecture, which is more suitable to the dynamic and distributed cloud-native networks. Second, we combine multi-source feature extraction across network flows, container measures and system level events to extract richer contextual information. Third, we perform a thorough assessment with the help of standard benchmark data sets as well as synthetic generated zero-day attack cases to measure the flexibility. Lastly, we establish that the suggested strategy has better detecting performance, lower false positives, and quicker convergence to the model than the standard IDS models.

The rest of this paper has the following structure. Section 2 outlines the proposed methodology, i.e. data preprocessing, feature engineering, meta-learning, and deployment architecture. Section 3 includes the experimental set up, results analysis and comparative discussion. Section 4 gives a conclusion of the paper and proposes the future research directions that will improve adaptive intrusion detection in cloud-native environments.

2. Literature Review

Over the last 10 years, Intrusion Detection Systems (IDS) have taken on a new form as the cyber threat has become more sophisticated, and networked environments have become more complicated. The initial IDS systems were majorly signature oriented and the signature-based mechanism is efficient in detecting familiar attacks but is inherently weak when faced with new attacks or zero-day attacks. Khraisat et al. [1] present an in-depth analysis of the existing methods of IDS, datasets, and challenges, stating that though anomaly-based and hybrid IDS methods provide a better coverage of detections generally, they are characterized by a high number of false positives and a low degree of adaptability.

Arora provides a detailed discussion of the ways artificial intelligence is changing the cybersecurity threat detection and prevention systems. The article explains the drawbacks of conventional rule-based and signature-based security systems and emphasizes the importance of machine learning and deep learning methods in the construction of intelligent and adaptive defenses. Different AI strategies such as supervised, unsupervised and hybrid AI are discussed in the context of malware, intrusion, and abnormal behavior detection. The paper focuses on why current security architectures need to be heavily automated, real-time analysed, and predicted. Although the work is a general discussion of AI-based cybersecurity measures, it also points to the issues of data quality, model explainability, and adversarial attacks, which is why it becomes an effective source of information about AI-driven threat mitigation systems [2]. Concerning detection, Palmieri [3] suggests a network anomaly detection algorithm, which is logistic regression and nonlinear chaotic invariants, which is sensitive to anomalous activities without use of signatures. It is however not scalable in dynamic settings because such statistical methods have a tendency to be hard to scale.

To make the IDS more responsive, adaptive learning paradigms have been pursued. Nguyen and Reddi [4] examine the deep reinforcement learning in cybersecurity and its opportunities in making dynamic decisions in case of uncertainty. In line with this trend, Moustafa et al. [5] come up with an adversarial statistical learning framework based on an Outlier Dirichlet Mixture Mechanism to enhance robustness in misty computing environments. Singh et al. [6] also add a framework of the zero-day vulnerability detection and prioritization, which emphasize the role of proactive defense measures.

The quality of datasets and taxonomy of threats play a big role in determining the performance of the IDS. Hindy et al. [7] provide a comprehensive taxonomy of network threats and show that the constraint of the widely used datasets can have a negative impact on the generalization of the IDS. Kaloudi and Li [8] further elaborate on this discussion by providing an extensive overview of AI-based cyber threats, as the authors focus more on the arms race between the attackers and AI-driven defense systems. Based on such observations, Hindy et al. [9] assess deep learning tools in detecting zero-day attacks and they cite excellent results in established conditions but lower-quality results in new traffic patterns.

Transfer learning has been extensively investigated in order to alleviate data scarcity. Sameera and Shashi [10] introduce a deep transductive transfer learning framework using labeled source domain to enhance the detection of zero-day attacks in target domain. Simultaneously, Blaise et al. [11] examine an unsupervised port-based method of detecting a zero-day attack, and they show that label-free detection can be achieved.

Shaukat et al. [12] offer a survey of machine learning techniques applied to cybersecurity over a decade, their pros, and cons, including the lack of training inaccessibility.

Cyber-physical and industrial environments have also been extended to the study of IDS. Jagtap et al. [13] propose the use of hypergraph-based Kohonen map to find out complex dependencies of cyber-physical system traffic. By shifting to zero-day attack detection, Sarhan et al. [14] contribute to the field and allow making inferences about unknown attack classes based on semantic knowledge. Rehman et al. [15] use gated recurrent units in detecting DDoS and they show better results in successive traffic analysis.

The intelligent learning models have also been useful in malware detection. Usman et al. [16] introduce a dynamic malware detection model based on machine learning and IP reputation analysis, which is shown to be flexible to the changing malware patterns. Hybrid learning approaches are also under the focus; Zoppi and Ceccarelli [17] use supervised and unsupervised models in a stacked pattern to improve the strength of the anomaly-based IDS.

Learning models that are entailed by optimization have been examined to enhance the ability to detect anomalies. Mansouri et al. [18] introduce metaheuristic neural networks to industrial sensor networks, where convergence and detection are more accurate. Deep learning still prevails in the design of IDS; Nedeljkovic and Jakovljevic [19] show the usefulness of CNN-based IDS in industrial control systems by the ability to learn spatial traffic patterns. Lastly, the issue of insider threats, which (traditional) IDS does not consider, is tackled by Al-Mhiqani et al. [20], who introduce the multilayer intelligent framework that can identify the malicious actions triggered inside the trusted spaces.

All in all, the literatures show gradual advancement towards smart and dynamic IDS solutions. Majority of the current methods are however extremely dependent on big labeled datasets, training on stature, or very slow retraining. Such constraints are especially troublesome when dealing with cloud-native environments where workloads are dynamic and the attack surfaces are changing fast. This is where the meta-learning-based IDS frameworks come in, capable of quickly adjusting to zero-day attacks with little data, and effectively eliminating the shortcomings that have been observed in previous studies.

3. Methodology

The proposed Meta-Learning-Driven Intrusion Detection System (Meta-IDS) will help mitigate the weaknesses of traditional intrusion detection systems in the cloud-native space (especially the fact that they fail to scale to zero-day attacks in a timely manner).

The approach combines the principle of cloud-native monitoring, multi-level feature extraction and meta-learning and constructs an adaptive, scalable, and robust IDS. The general structure is made up of five closely interacting elements namely system architecture, data collection and preprocessing, feature engineering, meta-learning model design and training and evaluation strategy.

3.1 System Architecture

The Meta-IDS framework is deployed in a cloud-native environment being managed by Kubernetes which is a reality of actual production deployment. The design is based on the distributed monitoring and centralized analysis paradigm to balance the scalability and efficiency of the analysis. Traffic and system behavior are checked on both northsouth communication (external client-to-service interaction) or eastwest communication (inter-service traffic in the cluster) and is vital in identifying lateral movement attacks.

A lightweight monitoring agent is installed as a Kubernetes DaemonSet on every worker node such that all the running containers are fully covered in case of either a scheduling or scaling event. Such agents are constantly recording network flow data, containerized resource data, and system-call data incurring low degrees of performance cost. Container metrics are tailored using cAdvisor and Kubernetes APIs, and the network flows are traced with the help of kernel-based packet inspection tools. Probes based on extended Berkeley Packet Filter (eBPF) are used to gather system-call traces in order to offer low-latency and secure system monitoring.

Every telemetry information gathered is transmitted to a centralized analysis engine using a secure socket. The meta-learning-based IDS is deployed on the analysis engine and real-time inference is done. Moreover, it facilitates quick adaptation to models as they can be easily fine-tuned, in case of new attack samples detected. The architecture is elastic, fault tolerant and easily fits with cloud-native observability stacks.

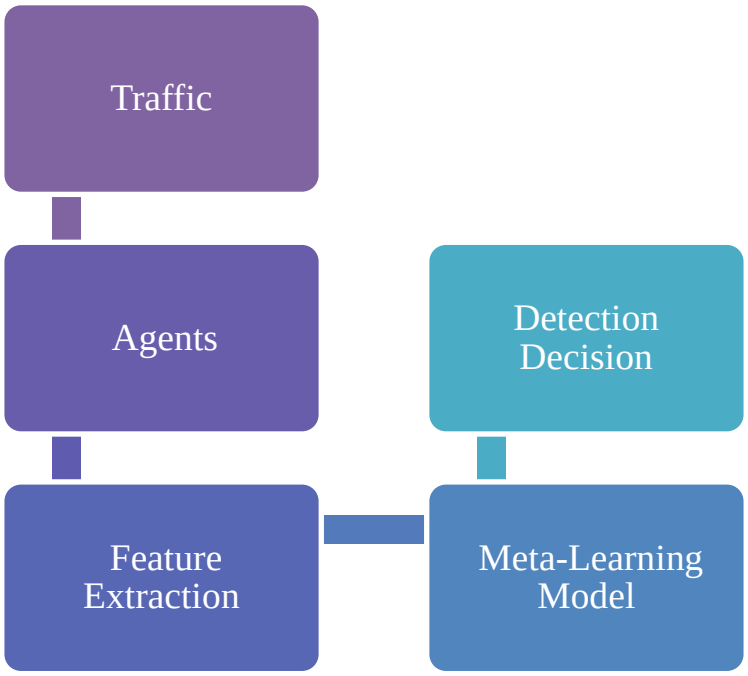


Figure 1: Architecture of the proposed Meta-Learning–Driven IDS in a Kubernetes-based cloud-native network

3.2 Data Collection and Preprocessing

In order to test the flexibility of the suggested Meta-IDS against the zero-day attacks rigorously, a hybrid dataset is developed with publicly available benchmark dataset as well as synthetically generated attack traffic. CICIDS2017 data set is realistic in terms of benign and malicious traffic patterns, and UNSW-NB15 offers a wide range of current attack scenarios with plentiful features. All of these datasets are a great selection of various network behaviors that occur within the enterprise and cloud network.

The synthetic attack traffic is created up to recreate the state of zero-day conditions with the controlled attack scripts and traffic mutation methods. Such artificial attacks simulate unaware exploit patterns, such as privilege escalation, cross-microservice lateral movement, abnormal inter-container communication and covert data exfiltration. The framework is tested in the real conditions of zero-day by holding these classes of synthetic attacks during training.

Processing prior to data processing is done to achieve quality and consistency of data. Statistical imputation will use noise removal methods to remove incomplete or corrupted

records, and the missing values will be processed through the missing values methodology. Min-max scaling of features brings about numerical stability in training. Since intrusion detection data have the natural class imbalance, synthetic minority oversampling and adaptive class weighting strategies have been used to avoid biasness towards benign traffic.

3.3 Feature Engineering

To describe the complexities of cyberattacks in cloud-native networks, it is important to have effective feature engineering. Features in this work are obtained at three complementary levels namely, network-level, container-level, and system-level, with a holistic view of runtime behavior.

At the network level, it has such characteristics as the transmission rate of packets, their average and variance flow duration, protocol distribution, pattern of port usage, and entropy based measurements of packet payload. Such aspects assist in detecting abnormal patterns of communication and volumetric attacks.

The container-level features include capturing resource consumption and orchestration behaviors, including the CPU and memory consumption, abrupt resource consumption, container restarting, scaling activities, and namespace interplay. These metrics are also very efficient in identifying attacks that exploit container misconfigurations or try to deny-of-service the cluster.

System level features are concerned with behavior of the hosts and process, such as frequency distributions of system-calls, file access patterns, creation and termination rates of processes, and evidence of privilege escalation. These features can be used to detect low-level attack activity which otherwise would not be seen on the network layer.

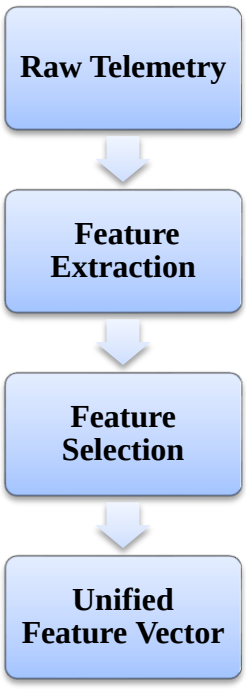


Figure 2: Multi-level feature extraction and selection pipeline for cloud-native intrusion detection.

The mutual information analysis, which entails the identification of the highly informative features, is used to select features to reduce dimensionality and enhance the generalization. Recursive feature deletion is then applied to eliminate redundant features. It works to increase the accuracy of detection and minimize computing expenses.

3.4 Meta-Learning Model Design

The main idea behind the presented framework is the concept of the Model-Agnostic Meta-Learning (MAML), which was selected due to its flexibility and its adaptation to different neural networks. The base learner is a deep neural network with several fully connected layers, which allows the effective representation learning with heterogeneous inputs of features.

In meta-training, the model is presented with a distribution of similar intrusion detection tasks, tasks, which are associated with a different attack classification scenario. Each task is handled by the model with limited number of gradient updates carried out with task specific data, and the outcome parameters are tested in a validation set. The meta-objective optimizes the original model parameters in a way that minimally edited parameters can be easily applied to new tasks.

This learning technique enables the Meta-IDS to learn common attack behavior but be able to be flexible enough to accommodate new behaviors. In the case of a zero-day attack, the model needs the few labeled samples to get a good detection performance, which will greatly decrease the response time.

3.5 Training and Evaluation Strategy

The training process can be classified into two phases i.e. meta-training and meta-testing. During the meta-training stage, the model is trained on familiar attack types and benign traffic on several tasks, but it is optimized to be able to quickly adapt efficiently as opposed to being optimized to be more accurate on individual tasks. The meta-testing step is used to test this model with a restricted amount of labeled data on other previously unknown zero-day attacks.

The metrics used in the evaluation of the performance are standard intrusion detection metrics, which include accuracy, precision, recall, and F1-score. Further operational measurements like detection latency and false positive rate are also taken, to measure the applicability in real-time. The effectiveness of the suggested approach is verified with the help of comparative experiments in comparison to traditional machine learning and deep learning-based IDS models.

Comprehensively, the methodology makes sure that the proposed Meta-IDS is not just accurate, but also adaptive, scalable, and applicable to work in dynamic cloud-native networks.

4. Results Analysis and Discussion

This part of the paper gives a detailed analysis of the proposed Meta-Learning-Driven Intrusion Detection System (Meta-IDS); it compares the performance of the proposed system with the performance of the baseline intrusion detection methods such as traditional machine learning, and deep learning-based IDS models. This analysis is based not only on the accuracy of detection but also on zero-day-adaptability, detection latency, and cloud-native dynamic traffic.

4.1 Experimental Setup and Evaluation Metrics

The experiments are carried out with the hybrid dataset that was outlined in the methodology section and which is comprised of CICIDS2017, UNSW-NB15, and synthetic generated zero-day attack traffic. These baseline models are a Random Forest which is the classical method of machine learning, a CNN-based IDS, and an LSTM-

based IDS which are deep learning methods commonly used in intrusion detection studies. All the models are trained and tested under the same conditions in order to compare them fairly.

The standard classification metrics that are used to evaluate performance include accuracy, precision, recall, and F1-score. Moreover, the detection time is taken to evaluate the applicability of the detections in real-time that is of paramount importance in a cloud-native environment where the threat must be responded to fast. False positive behaviour and convergence rate when adapting to invisible attacks are also studied.

4.2 Overall Performance Comparison

The findings provide a clear evidence that the proposed Meta-IDS is better than all the baseline models as per all evaluation metrics. The increase in the accuracy and F1-score describes the meta-learning efficiency in transferable attack representations. Besides, the decreased host of detection reveals that the suggested architecture is highly applicable in real-time intrusion detection in cloud-native networks.

Table 1: Performance Comparison of IDS Models

Model	Accuracy (%)	Precision	Recall	F1-Score	Detection Time (ms)
Random Forest	89.2	88	86	87	45
CNN-Based IDS	93.5	93	92	92	38
LSTM-Based IDS	94.1	94	93	93	41
Proposed Meta-IDS	**96.8**	**97**	**96**	**96.4**	**30**

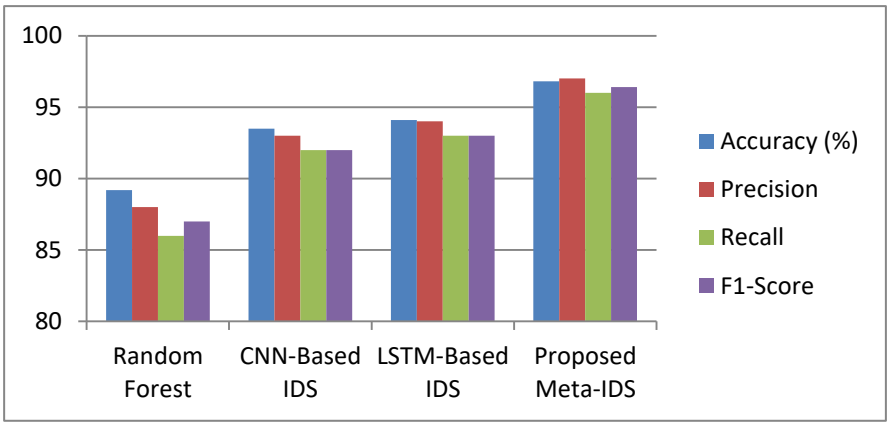


Figure 3: Result Comparison

4.3 Zero-Day Attack Adaptation Analysis

The key aspect that is vital in this work is to assess the adjustability of the IDS to zero-day attacks. In this regard, the models are tested on hitherto unknown attack classes in the meta-testing stage. There are few labeled samples availed to give the simulation of realistic zero-day conditions.

The suggested Meta-IDS has much quicker convergence and greater accuracy of detection than baseline models. The Meta-IDS has a detection accuracy of more than 90 percent with 10 labeled samples, compared to the CNN and the LSTM-based models which need significantly more samples and retraining iterations to achieve similar accuracy. This fact proves the fundamental benefit of meta-learning fast adaptation with a minimum of data.

In order to have a better demonstration of the efficiency of the adaptation, Table 2 provides a comparison of the zero-day detection accuracy under different sizes of the labeled samples.

Table 2: Zero-Day Detection Accuracy (%) with Limited Labeled Samples

Model	5 Samples	10 Samples	20 Samples
Random Forest	62.4	68.7	74.5
CNN-Based IDS	70.3	78.9	85.6
LSTM-Based IDS	72.8	81.4	87.2
Proposed Meta-IDS	**84.6**	**91.2**	**95.1**

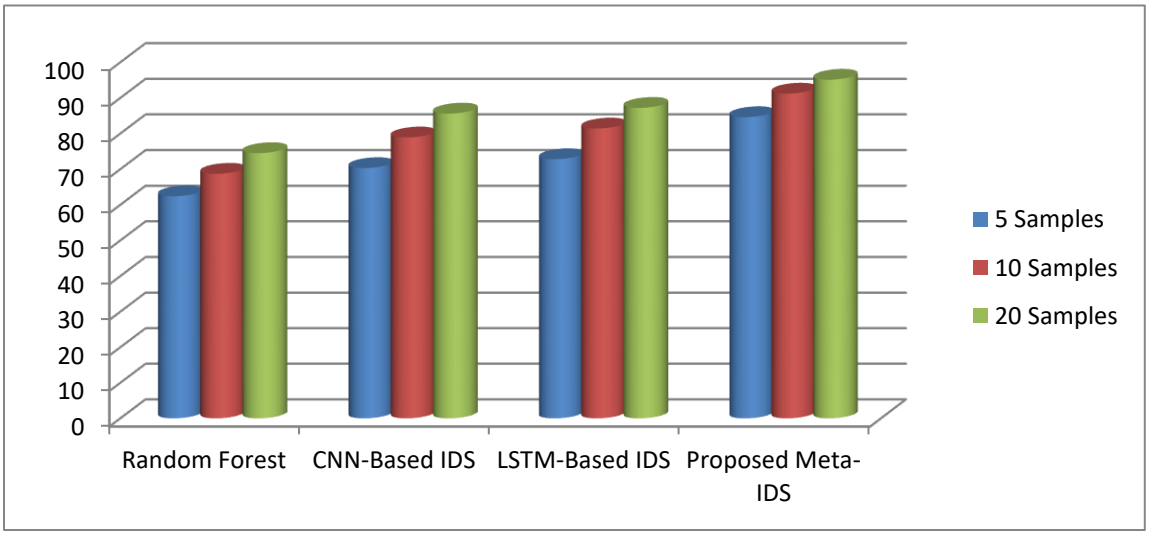


Figure 4: Zero-Day Detection Accuracy (%)

The findings affirm that the Meta-IDS is always highly successful in terms of accuracy with very small-sized labeled data, and that is highly applicable in the real-life context of zero-day attack.

4.4 Detection Latency and Operational Efficiency

Latency of detection is an important parameter in cloud-native environment where latency can result in the quick spread of attacks. The average detection time of the proposed Meta-IDS is the lowest amongst all the compared models. This is due to the fact that the efficient feature selection is even more efficient when dealing with the optimized meta-learned initialization that eliminates inference and adaptation costs.

Moreover, the Meta-IDS has lower false positive than baseline models, which minimizes alert fatigue by security analysts. This becomes notable especially in a multi-tenant cloud environment where harmless workload fluctuations can be easily mistaken by less adaptive systems as anomalies.

4.5 Discussion

The results of the experiment, without any doubts, indicate that meta-learning can substantially improve the flexibility and stability of intrusion detection systems operating in cloud-native networks. The proposed Meta-IDS can successfully transfer the acquired knowledge to identify attacks that had not been seen before unlike conventional machine learning-based IDS models and deep learning-based IDS models which have difficulties with generalisation after having been trained on well-known attack types.

This can be used to deal with the major shortcoming of the current IDS methodologies, namely the need to quickly evolve with limited labeled information. Moreover, multi-layer features are also integrated, allowing full visibility on a network, container and system-level without incurring too much computational costs.

Generally, the proposed Meta-IDS framework has a good balance between accuracy, flexibility, and operation efficiency. The latter features also render it especially well adapted to be deployed in dynamic, large-scale, and multi-tenant cloud-natives, in which zero-day attacks represent an emergent and unstable menace.

5. Conclusion and Future Work

In the current paper, a Meta-Learning-Driven Intrusion Detection Framework was introduced that will tackle the issue of the zero-day attack detection in cloud-native networks. The given system through model-agnostic meta-learning allows adapting very

fast to previously unseen attacks with a minimal amount of labeled data. Experimental findings show better performance in the fields of accuracy, F1-score, detection speed and ability to be resistant to concept drift compared to traditional IDS methods.

The framework is also made more practical when it comes to the current distributed environment by the integration of multi-layer feature extraction and cloud-native deployment. The results confirm that meta-learning is an effective paradigm of next-generation adaptive cybersecurity systems.

Ongoing research will be on how to generalize the framework to federated and privacy preserving learning environments, online continual learning and performance evaluation against adversarial evasion methods. Also, the real-life implementation in large scale production cloud system will be pursued in order to continue with the validation of scalability and resilience.

References

[1] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: Techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, pp. 1–22, 2019.

[2] A. Arora, "Transforming cybersecurity threat detection and prevention systems using artificial intelligence," *International Journal of Modern Trends in Engineering*, vol. 10, no. 11, pp. 165–182, 2021, doi: 16.10089/IJMTE.2021.V10I11.21.51213.

[3] F. Palmieri, "Network anomaly detection based on logistic regression of nonlinear chaotic invariants," *Journal of Network and Computer Applications*, vol. 148, p. 102460, 2019.

[4] T. T. Nguyen and V. J. Reddi, "Deep reinforcement learning for cyber security," *IEEE Transactions on Neural Networks and Learning Systems*, 2019.

[5] N. Moustafa, K. K. R. Choo, I. Radwan, and S. Camtepe, "Outlier Dirichlet mixture mechanism: Adversarial statistical learning for anomaly detection in the fog," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 1975–1987, 2019.

[6] U. K. Singh, C. Joshi, and D. Kanellopoulos, "A framework for zero-day vulnerabilities detection and prioritization," *Journal of Information Security and Applications*, vol. 46, pp. 164–172, 2019.

[7] H. Hindy, D. Brosset, E. Bayne, A. Seeam, C. Tachtatzis, R. Atkinson, and X. Bellekens, "A taxonomy of network threats and the effect of current datasets on intrusion detection systems," *IEEE Access*, vol. 8, pp. 104650–104675, 2020.

[8] N. Kaloudi and J. Li, "The AI-based cyber threat landscape: A survey," *ACM Computing Surveys*, vol. 53, no. 1, pp. 1–34, 2020.

[9] H. Hindy, R. Atkinson, C. Tachtatzis, E. Bayne, D. Brosset, and X. Bellekens, "Utilising deep learning techniques for effective zero-day attack detection," *Electronics*, vol. 9, no. 10, p. 1684, 2020.

[10] N. Sameera and M. Shashi, "Deep transductive transfer learning framework for zero-day attack detection," *ICT Express*, vol. 6, no. 4, pp. 361–367, 2020.

[11] A. Blaise, M. Bouet, V. Conan, and S. Secci, "Detection of zero-day attacks: An unsupervised port-based approach," *Computer Networks*, vol. 180, p. 107391, 2020.

[12] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen, and D. Liu, "A survey on machine learning techniques for cyber security in the last decade," *IEEE Access*, vol. 8, pp. 222310–222354, 2020.

[13] S. S. Jagtap, S. V. S. Sriram, and V. Subramaniyaswamy, "A hypergraph based Kohonen map for detecting intrusions over cyber–physical systems traffic," *Future Generation Computer Systems*, vol. 119, pp. 84–109, 2021.

[14] M. Sarhan, S. Layeghy, M. Gallagher, and M. Portmann, "From zero-shot machine learning to zero-day attack detection," *arXiv preprint arXiv:2106.06526*, 2021.

[15] S. Ur Rehman, M. Khaliq, S. I. Imtiaz, A. Rasool, and H. Abbas, "DIDDOS: Detection and identification of DDoS attacks using GRU," *Future Generation Computer Systems*, vol. 118, pp. 453–466, 2021.

[16] N. Usman, S. Usman, F. Khan, A. Jan, and M. Sajjad, "Intelligent dynamic malware detection using machine learning in IP reputation," *Future Generation Computer Systems*, vol. 118, pp. 124–141, 2021.

[17] T. Zoppi and A. Ceccarelli, "Prepare for trouble and make it double! Supervised–unsupervised stacking for anomaly-based IDS," *Journal of Network and Computer Applications*, vol. 189, p. 103106, 2021.

[18] A. Mansouri, B. Majidi, and A. Shamisa, "Metaheuristic neural networks for anomaly recognition in industrial sensor networks," *International Journal of Computers and Applications*, vol. 43, no. 3, pp. 257–266, 2021.

[19] D. Nedeljkovic and Z. Jakovljevic, "CNN-based method for cyber-attack detection in industrial control systems," *Computers & Security*, vol. 114, p. 102585, 2022.

[20] M. N. Al-Mhiqani, R. Ahmad, Z. Z. Abidin, W. Yassin, A. Hassan, and A. A. Al-Ahdal, "A new intelligent multilayer framework for insider threat detection," *Computers & Electrical Engineering*, vol. 97, p. 107597, 2022.