UDC 004.9 **doi:** https://doi.org/10.20998/2522-9052.2024.3.11

Valentyn Sobchuk[1], Roman Pykhnivskyi[1], Oleg Barabash[2], Serhii Korotin[3], Shakhin Omarov[4]

[1] Taras Shevchenko Kyiv National University, Kyiv, Ukraine
[2] National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine
[3] National Defence University of Ukraine, Kyiv, Ukraine
[4] Kharkiv National University of Radio Electronics, Kharkiv, Ukraine

SEQUENTIAL INTRUSION DETECTION SYSTEM FOR ZERO-TRUST CYBER DEFENSE OF IOT/IIOT NETWORKS

Abstract. Relevance. The Internet of Things (IoT) and the Industrial Internet of Things (IIoT) and their widespread application make them attractive targets for cyber attacks. Traditional cybersecurity methods such as firewalls and antivirus software are not always effective in protecting IoT/IIoT networks due to their heterogeneity and large number of connected devices. The zero-trust principle can be more effective in protecting IoT/IIoT networks. This principle assumes on no inherent trustworthiness of any user, device, or traffic, requiring authorization and verification before accessing any network resource. **This article presents** a zero-trust-based intrusion detection system (IDS) that uses machine learning to secure IoT/IIoT networks. **The aim of this article** is to develop a two-component IDS for detecting and classifying cyber-attacks. **The study utilizes** machine learning techniques, such as Decision Tree, Random Forest, and XGBoost, on the Edge-IIoTset dataset. The following **results** were obtained. The IDS structure proposed here employs a sequential approach that consists of two AI modules. The first module detects attacks using a simpler model like Decision Tree. The second module uses more complex models like Random Forest or XGBoost to classify attack types. Experimental evaluation on the Edge-IIoTset dataset demonstrates the system's effectiveness, with an overall accuracy of 95% and significantly reduced response time compared to single complex model systems. **Conclusion**. The proposed design for an Intrusion Detection System (IDS) achieves high accuracy in detecting attacks while maintaining optimal performance and minimizing additional computational costs. This is especially crucial for real-time network monitoring in IoT/IIoT environments. **Further research** can focus on the practical implementation of the proposed IDS structure for physical realization in securing IoT/IIoT networks based on the zero-trust principle.

Keywords: cybersecurity; zero-trust security; IoT; IIoT; intrusion detection; machine learning.

Introduction

The Industrial Internet of Things (IIoT) refers to a complex network of interconnected devices, sensors, and machinery utilized in industrial environments to gather, share, and analyze data. Its objective is to augment operational efficiency, facilitate predictive maintenance, refine processes, and boost overall productivity across various sectors, including manufacturing, energy, transportation, and healthcare. IIoT is revolutionizing urban areas worldwide, turning them into smart cities. A study from 2021 [1] highlighted a notable growth in the number of IIoT-connected devices: from 8.6 billion in 2019 to 9.76 billion in 2020, reaching 11.28 billion in 2021. Furthermore, projections estimate an exponential increase to approximately 29.42 billion connected devices by 2030.

As the internet has become indispensable in our daily lives, the quantity of internet-connected systems continues to rise. The evolution of computer networks, servers, and mobile technology has significantly expanded internet access. However, the widespread use of the internet has also attracted cybercriminals, who are continuously developing more advanced and potent cyber-attack methods for their gain. According to IBM [2], the average data breach cost in 2022 was $4.35 million USD, a 2.6 percent increase from 2021's $4.24 million USD. This estimate is based on the expenses of 550 organizations experiencing data breaches across 17 countries and industries, such as healthcare, finance, and energy, indicating the significant financial impact of cybersecurity threats.

In response to these evolving challenges, the concept of Zero-Trust Architecture (ZTA) [3–5] is rapidly gaining traction and is increasingly regarded as the preferred security architecture for these environments. It marks a paradigm shift from the traditional “trust but verify” approach to a more robust “never trust, always verify” stance. ZTA is characterized by a fundamental stance where no user or device is inherently trusted, regardless of status or location. Instead, it requires continuous monitoring, robust authorization, authentication methods, and ongoing assessment of the trustworthiness of all users and devices in the network. However, Implementing Zero Trust (ZT) principles using static policies is an exceptionally complex task, becoming even more challenging in IoT/IIoT environments due to their dynamic nature.

To mitigate cyber threats, zero-trust networks must implement an Intrusion Detection System (IDS) to promptly detect potential cyberattacks and anomalies. IDS ensures network systems can effectively respond to evolving threats while maintaining integrity and security. As the number of users and devices grows, automated real-time monitoring and dynamic security assessments, essential aspects of Zero Trust Architecture (ZTA), require solutions and methods capable of handling large volumes of data. Artificial intelligence (AI) algorithms can play a pivotal role in overcoming these challenges through intelligent monitoring, evaluation, and decision-making processes.

Thus, Spadaccino and Cuomo [6] explored the potential and obstacles of implementing edge computing within an IDS-equipped IoT setting. They utilized machine learning within their IDS to facilitate the detection of anomalies. Their examination included the pros and cons of deploying IDS, focusing on the necessities for immediate responses, storage capabilities, and processing power.

DNNs and other complex ML algorithms are widely employed by researchers [7–11] to develop IDSs. However, these models are becoming increasingly intricate in architecture, requiring substantial computing resources and hardware. The complexity of ML-based IDS models makes it challenging to elucidate the reasoning behind their predictions and complicates the process for humans to understand the rationale behind these decisions. Additionally, such models are difficult to troubleshoot and maintain, further complicating their practical application.

As evidenced by numerous surveys [12-17], many researchers have focused more on improving the accuracy of various classification models rather than developing realistic and trustworthy IDS systems. This trend highlights a potential gap in addressing the practical implementation challenges and the overall reliability of IDS solutions in real-world scenarios. Our study proposes a zero-trust IDS framework with two AI-based modules for anomaly detection and classification:

1. Attack Detection Module: This module is tasked with identifying attacks. It can be situated on edge servers in a 5G network to optimize learning traffic patterns from connected devices. Its design prioritizes low computational demands, rapid traffic analysis, and high detection accuracy.

2. Attack Classification Module: Utilizing more sophisticated and complex AI algorithms, this module specializes in categorizing the types of attacks. It can be deployed in the cloud or on-premise servers and integrate third-party applications. Its functionality hinges on analyzing attack traffic, making it versatile for deployment scenarios.

This study includes an experimental analysis of the proposed solution to test the effectiveness, efficiency, and practicality of the zero-trust IDS in real-world scenarios. The aim is to demonstrate its capabilities and identify areas for improvement.

By focusing on these critical areas, the study seeks to contribute valuable insights and advancements to the field of cybersecurity, particularly in developing and implementing more secure, reliable, and transparent IDS.

The rest of the paper is organized as follows. Section 2 briefly reviews zero trust architecture principles, network micro-segmentation for IoT security, types and classifications of IDS, and machine learning approaches for anomaly-based network IDS, and provides an overview of the Edge-IIoTset dataset as a testbed for IDS. Section 3 introduces the proposed IDS framework architecture and workflow, including details on the Attack Detection Module and the Attack Classification Module. Section 4 contains the experimentation process, the dataset used for evaluation, the preprocessing steps, the training process for the detection and classification models, the evaluation metrics employed, and the analysis of the results obtained. Finally, Section "Conclusions" summarizes the essential findings and contributions of the study in this section, along with potential future research directions.

1. Background and Related Work

The United States Department of Defense (DoD) has introduced a Zero-Trust Architecture (ZTA) framework [5] that integrates threat intelligence and remediation strategies. Central to this framework are machine learning analytics, real-time network traffic monitoring, and orchestration capabilities.

Network micro-segmentation is crucial for implementing Zero Trust (ZT) security within IoT networks. The key benefits of using micro-segmentation are:

- Micro-segmentation minimizes the attack surface by dividing the network into smaller, controlled segments. It confines potential breaches, significantly reducing the overall attack surface.
- Granular access control for precise access control policies, ensuring devices can only access necessary network resources, aligning with the Zero Trust principle of "never trust, always verify."
- Lateral movement prevention segmentation limits an attacker's ability to move laterally within the network, containing any damage to isolated segments.
- Improved compliance: helps meet regulatory standards by restricting access to sensitive data only to authorized devices and users.
- Scalability and flexibility: adapts to changes in the network, such as adding or removing devices, without compromising security.
- Enhanced incident response: Facilitates quicker identification and isolation of compromised devices, minimizing the impact of security incidents.

Micro-segmentation in the IoT context can be implemented through software-defined networking (SDN), supplemented by network function virtualization (NFV) and a software-defined perimeter (SDP). These components work together to form an overlay network, providing enhanced resource protection.

Syed et al. in [18], showed that IDS integrated within SDN environments significantly enhances network security through centralized monitoring, detection, and responsive measures against malicious activities and policy violations. This integration facilitates the dynamic deployment of security policies. SDN controllers can quickly adjust network configurations in response to detected threats, such as rerouting traffic or isolating compromised network segments. Additionally, the programmable nature of SDN enhances traffic analysis capabilities, allowing for selective traffic inspection and more efficient use of resources. Upon identifying potential threats, IDS can trigger automated responses to contain and mitigate these risks promptly.

Intrusion Detection Systems (IDS) are typically divided into two main types: Signature-based IDS (SIDS) and Anomaly-based IDS (AIDS) [16]. SIDS matches network traffic against a predefined database of known attack signatures, effectively identifying only previously recognized threats. This approach, however, cannot detect novel, zero-day attacks or sophisticated threats that still need to be cataloged, highlighting a significant vulnerability in the face of rapidly evolving cyber threats.

Additionally, IDS technologies can be categorized based on their data source into Host-based IDS (HIDS) and Network-based IDS (NIDS). HIDS monitors data from a specific device or host, examining system logs, firewall logs, and application audits, among other sources. This method is particularly adept at uncovering insider threats that may not generate observable network traffic. Conversely, NIDS scrutinizes data traversing the network to identify malicious activity through traffic analysis, offering a broader, albeit potentially less granular, view of network security.

The concept of anomaly-based NIDS has gained significant attention among scholars due to its potential to overcome the limitations of traditional signature-based IDS. Furthermore, the rapid development of machine learning and artificial intelligence algorithms has contributed to the growing popularity of anomaly-based NIDS. Surveys [19-21] in the IDS domain have shown that these algorithms have improved NIDS's accuracy and detection rates, making it a promising area of research for scholars in the field.

Our research study utilized a state-of-the-art cybersecurity dataset called the Edge-IIoTset, which was published in 2022 by Ferrag et al. in [22]. This cutting-edge dataset is widely used for evaluating AI-based NIDS (Network Intrusion Detection Systems). It is generated using more than ten types of IoT devices, including low-cost digital sensors for sensing temperature and humidity, ultrasonic sensors, water level detection sensors, pH sensor meters, soil moisture sensors, heart rate sensors, flame sensors, and many more. The dataset contains 14 different attack categories related to IoT/IIoT connectivity protocols, including DoS/DDoS attacks, information gathering, man-in-the-middle attacks, injection attacks, and malware attacks. So this comprehensive dataset is particularly useful for evaluating the performance of AI-based NIDS in detecting and mitigating various types of cyber attacks on IoT/IIoT devices.

The authors of Edge-IIoT-2022 conducted the most relevant study to our work. This study [22] achieved high accuracy results for binary-class classifiers, scoring between 99.98% and 99.99% classification accuracy using five algorithms. However, multiclass threat classification had much lower accuracy, ranging from 67.11% to 83.39% using Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (KNN). The highest accuracy achieved for multiclass threat classification was 96.01% using DNN.

Taraf et al. [23], evaluated six different classification algorithms: J48, PART, BayesNets, AdaBoost, LogitBoost, and an Attribute-Selected Classifier. The highest accuracy achieved for multiclass threat classification was 92.92% using DNN.

Nkoro et al. [24] introduced a novel NIDS model that employed a deep learning approach based on a combination of Convolutional Neural Network (CNN) and Bidirectional Long Short-Term Memory (BiLSTM) architectures. The proposed model was evaluated on the Edge-IIoT dataset and achieved an impressive accuracy of 92% for 4-class classification.

Latif et al. in [25], proposed tri-layer approach for attack detection combines Convolutional Neural Networks, Genetic Algorithms, and bootstrap aggregation ensemble techniques to achieve a 100% accuracy rate for binary and multi-class classification.

As we can observe, achieving high accuracy in threat classification through machine learning models comes at the cost of increased complexity. This increased complexity makes debugging, interpreting, and maintaining such models challenging. Additionally, high computational costs make applying Intrusion Detection Systems (IDSs) that use such models in IoT environments difficult.

2. The Proposed Framework

The architecture of SDN with an Intrusion IDS framework is illustrated in Fig. 1.

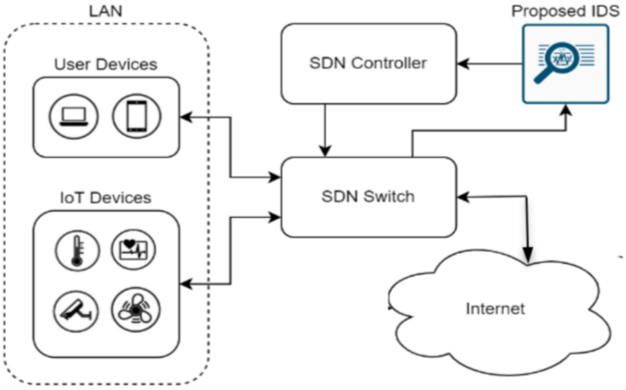

Fig. 1. Architecture of SDN with IDS

The proposed IDS framework comprises three major components: an SDN switch, an SDN controller, and the IDS. The SDN switch is responsible for forwarding network traffic based on the instructions received from the SDN controller. The SDN controller acts as a central point of control for the SDN network, enabling administrators to manage network traffic flows efficiently. Finally, the IDS monitors network traffic for signs of malicious activity and alerts administrators of potential security threats. Together, these components form a comprehensive IDS framework that helps network administrators proactively detect and mitigate security risks in the SDN environment.

Our Intrusion Detection System (IDS) comprises two modules: the Attack Detector and the Attack Classifier. The Attack Detector utilizes a relatively simple and easy-to-understand machine learning (ML) model for binary classification, such as Logistic Regression (LR) or Decision Tree (DT). This makes it effective in environments where resources are limited. On the other hand, the Attack Classifier is based on a more complex and powerful ML model for multiclass classification, such as Random Forest (RF) or XGBoost (XGB).

The workflow of our IDS is illustrated in Fig. 2. The IDS uses an attack detector to filter and identify malicious traffic efficiently. Once identified, the traffic is sent to the Attack Classifier for further analysis. This approach reduces the computational cost of IDS operations and enables distributed training of the detector and classifier.

The attack detector can be fine-tuned for specific network segments, allowing it to detect anomalies in the traffic more effectively. This is important because different network segments may have different characteristics that need to be considered when detecting attacks.

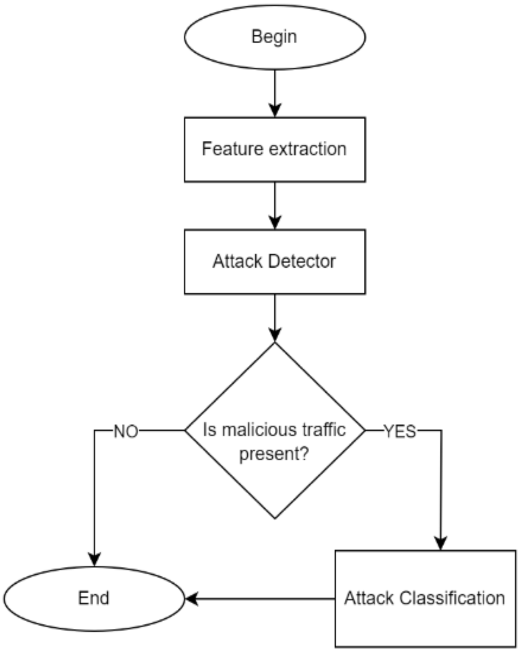

Fig. 2. The workflow of the proposed IDS

The Attack Classifier can be a third-party application based on a large amount of data used to classify attacks. That will make the classifier more accurate and effective at identifying attacks, as it has access to a broad range of data to draw upon.

3. Performance Evaluation

To determine the effectiveness of the proposed design, we constructed two IDS. The first IDS used a combination of DT and RF, which we called DT-RF. The second IDS combined DT and XGBoost, which we named DT-XGB. We compared the performance of our IDS systems with single-model-based IDS that used RF and XGBoost. We employed an ML pipeline, as illustrated in Fig. 3.

This consisted of dataset preprocessing, ML model training, and evaluation using standard metrics: Accuracy (1), Precision (2), Recall (3), and F1-score (4):

$$Accuracy = \frac{TN + TP}{TN + TP + FP + FN}; \qquad (1)$$

$$Precision = \frac{TP}{TP + FP}; \qquad (2)$$

$$Recall = \frac{TP}{TP + FN}; \qquad (3)$$

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}. \qquad (4)$$

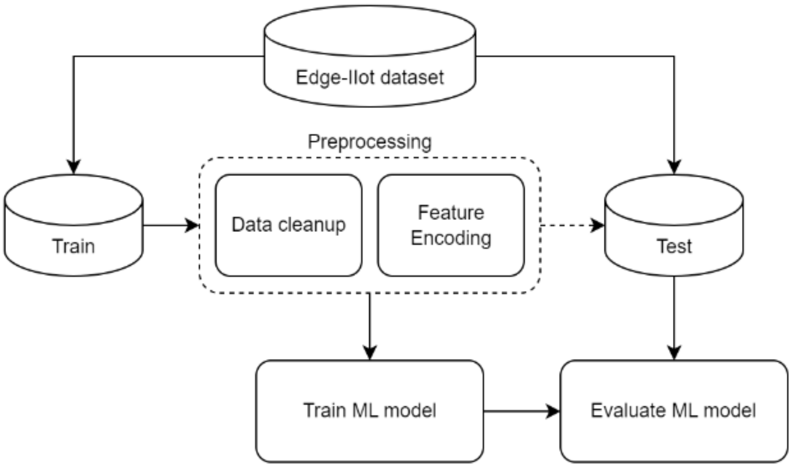

Fig. 3. Used ML classification pipeline

These metrics use different parameters to measure the performance of the model TP (True Positive) represents the number of correctly classified attacks, TN (True Negative) denotes the number of correctly classified non-attacks, FP (False Positive) is the number of wrongly classified attacks, and FN (False Negative) refers to the number of the misclassified non-attack records.

In our multi-class classification, we used macro-averaged Precision, Recall, and F1-score to provide an average performance measure across all classes. This gives us a comprehensive view of the IDS's overall effectiveness.

In addition to overall performance measures, we conducted two types of inference time performance evaluations. The first, batch classification, involved running an ML model on a set of records. The second, sequential packet-wise classification, evaluated the model's ability to process packets individually.

3.1. Dataset Description. The Edge-IIoTset dataset encompasses 61 features generated from a test bed that includes the cloud computing layer, network functions virtualization layer, blockchain network layer, fog computing layer, software-defined networking layer, edge computing layer, and IoT and IIoT perception layer. These features meet the critical requirements of IoT communications.

The dataset contains 20,939,646 records, with 11,209,923 representing regular traffic and 9,729,723 corresponding to 14 attack classes. Our study used a sample dataset with 244,460 records to evaluate machine learning-based intrusion detection systems. This sample is balanced concerning 'Attack_label,' which indicates the traffic type: 0 for regular traffic and 1 for attack. It is also balanced within 'Attack_type' for attack scenarios.

3.2. Dataset Preprocessing And Cleanup.

Step 1: Remove ‘NaN’ values, 29 rows.

Step 2: Remove duplicated rows, 6201 removed.

Step 3: Drop unnecessary features: “frame.time”, “ip.dst_host”, “arp.src.proto_ipv4”, “http.file_data”, “ip.src_host”, “tcp.srcport”, “arp.dst.proto_ipv4”, “http.request.uri.query”, “icmp.transmit_timestamp”, “http.request.full_uri”, “tcp.payload”, “tcp.options”, “udp.port”, “tcp.dstport” and “mqtt.msg” (15 columns removed).

Step 4: Fix the representation of zero as a string. We replaced all instances of “0” with “0.0” in rows containing categorical (non-numeric) data: “mqtt.topic”, “http.request.version”, “dns.qry.name.len”, “mqtt.protoname” and “http.request.method”.

It’s crucial to note that normal records have zeros as “0.0” and attack records have zeros as “0”. This inconsistency can cause inaccurate machine learning models with high binary classification accuracy. Correcting this discrepancy is necessary for accurate models.

Step 5: Perform encoding of categorical features using one-hot encoding, a technique to represent categorical variables as numerical values.

Fig. 4. and 5 illustrate the distribution of records in the dataset after preprocessing and cleanup concerning “Attack_label” and “Attack_type” respectively.

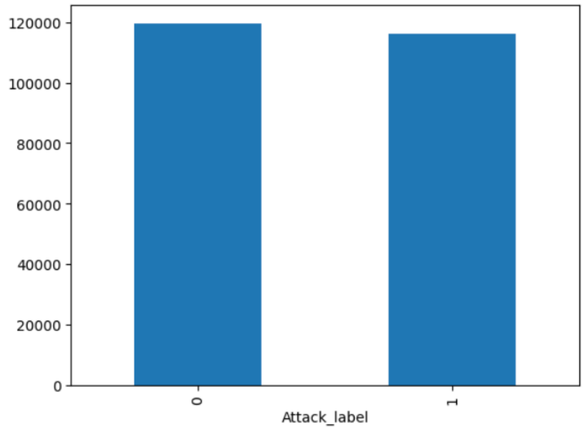

Fig. 4. Class distribution concerning “Attack_label”

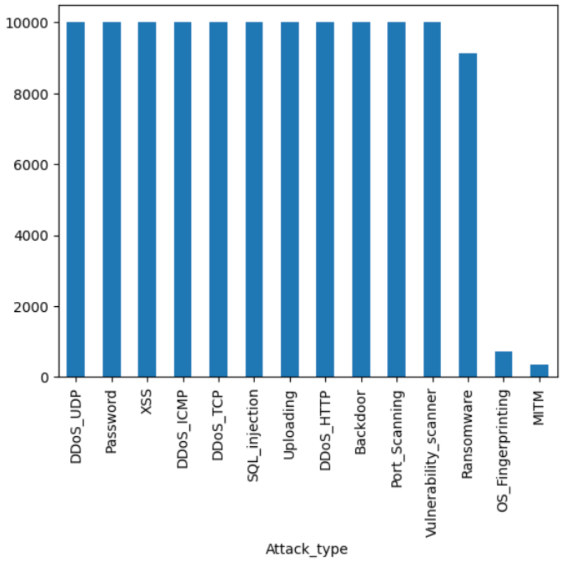

Fig. 5. Class distribution concerning “Attack_type”

4. Training of Detection Models

We considered two lightweight classification algorithms, DT and LR, for the detection phase of the proposed IDS system. From an ML perspective, the detection phase is a binary classification problem where “Attack_label” is the value to predict. We split the data set into training and evaluation sets, with 70% for training and 30% for testing. We performed hyperparameter tuning using Grid Search with stratified cross-validation to obtain a more efficient and generalized model.

As shown in Fig. 6, DT performs much better as the detector, showing 96% accuracy compared to LR algorithm, which has 60% accuracy. This suggests a non-linear dependency between features and the target. DT showed good results in terms of detecting anomalous network traffic while minimizing the number of false-positive predictions.

We will use DT as the detector for further implementation of our IDS.

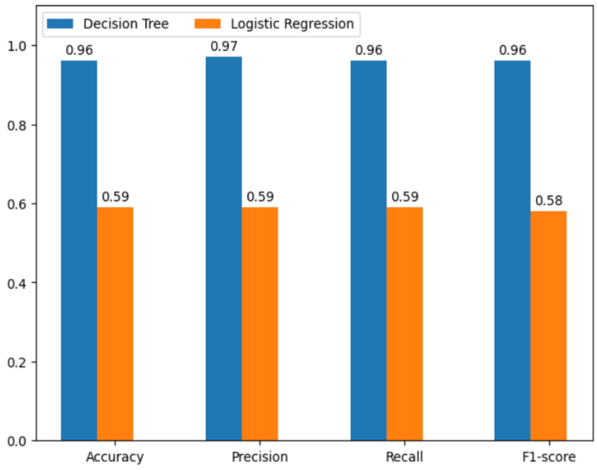

Fig. 6. Detection performance results

4.1. Training Of Classification Models. We used two advanced ML models for classifying attack types: the Random Forest (RF) classifier and XGBoost. Both methods demonstrated promising results in classifying 14 attack types, with average accuracies of 91% and 92%, respectively. Fig. 7 illustrates the performance comparison between the Random Forest and XGBoost methods.

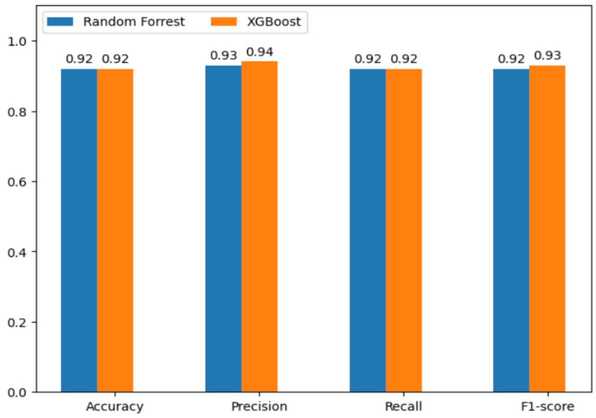

Fig. 7. Random Forrest and XGBoost performance comparison

4.2. Training Of Classification Models. We also measured the inference time of the considered models using a set of 10,000 network packets with 10% malicious traffic.

The results and the models' performance metrics are presented in Table 1. It is evident that our sequential IDS, utilizing two ML models, demonstrates comparable performance to single-model IDS but also shows significantly better runtime performance with lower inference time.

Fig. 8 Illustrates the average inference time after 10 trials for a single packet classification.

We used a set of 10,000 network packets, with 50% consisting of malicious traffic. It is evident that for normal traffic, the inference time using DT as the detector is significantly lower than the inference time when using more complex models like RF or XGB. Low computational overhead is crucial for IDS, especially in IoT environments. Even for malicious traffic, our IDS performs better than single-model IDS.

Table 1 – **Comparison in model performances and inference time**

Model	Accuracy	Precision	Recall	F1-score	Batch classification inference time (ms)	Sequential inference time (ms)
RF	0.99	0.94	0.95	0.95	144	31,394
XGB	0.99	0.98	0.92	0.95	35	4,256
DT-RF	**0.99**	**0.99**	**0.93**	**0.96**	**24**	**3,373**
DT-XGB	**0.99**	**0.98**	**0.92**	**0.94**	**7**	**821**

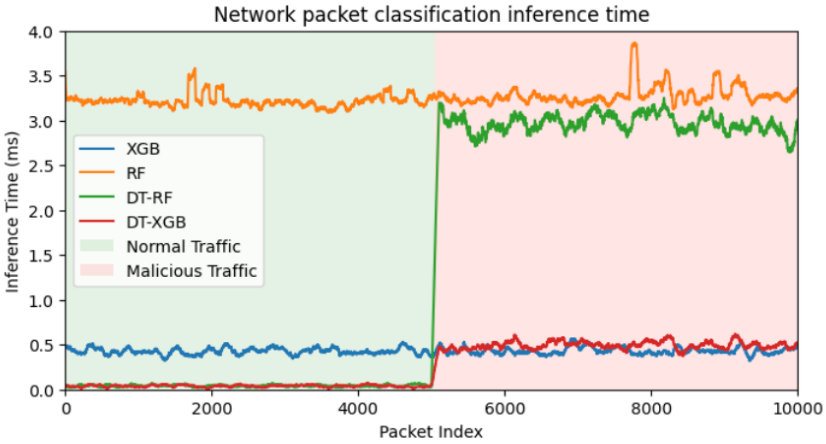

Fig. 8. Network packet classification inference time

We used a set of 10,000 network packets, with 50% consisting of malicious traffic. It is evident that for normal traffic, the inference time using DT as the detector is significantly lower than the inference time when using more complex models like RF or XGB. Low computational overhead is crucial for IDS, especially in IoT environments. Even for malicious traffic, our IDS performs better than single-model IDS.

Conclusions

This paper presents a design for a machine learning-based Intrusion Detection System (IDS) that adopts a zero-trust security paradigm for IoT/IIoT systems. We tested our design using Edge-IIoTset, one of the most recent cybersecurity datasets. We created a two-stage anomaly detection and classification system capable of identifying diverse cyber threat patterns with a high accuracy of 95% and high run-time efficiency. Our simulation results showed a speedup of 5 times for batch classification compared to single-model-based IDS using complex models like Random Forest (RF) or eXtreme Gradient Boosting (XGB) and 5 (RF vs. DT-RF) to 8 times (XGB vs. DT-XGB) for sequential packet-wise classification, where packets were inputted to the model one by one.

Our results showed that the presented design of IDS with Decision Tree (DT) as a relatively simple ML model for malicious traffic detection, accompanied by more complex and powerful models like RF or XGB, has significantly lower overhead than IDSs based on only complex models. This indicates that our two-stage model has significant potential for real-time Network-based IDS (NIDS) usage. Additionally, using a simple ML model as the attack detector is much easier to debug, maintain, and interpret. For example, a Decision Tree (DT) delivers the classification decision and elucidates its rationale.

In future work, we will assess our design on other popular cybersecurity datasets and a real Software-Defined Networking (SDN) system and evaluate its throughput and latency performance.

Data availability

The dataset used in this research is available online: https://ieee-dataport.org/documents/edge-iiotset-new-comprehensive-realistic-cyber-security-dataset-iot-and-iiot-applications

Acknowledgments, funding sources

The research was partially supported by the research project No 24БФ038-01 within the framework of the comprehensive scientific program "Modern Mathematical Problems of Natural Science, Economics and Finance".

References

1. Vailshery. L. S. (2023), *Number of Internet of Things (IoT) Connected Devices Worldwide From 2019 to 2021, with Forecasts From 2022 to 2030*, available at: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/
2. (2024), Cost of a Data Breach Report 2023", IBM, available at: https://www.ibm.com/reports/data-breach
3. Rose, S., Borchert, O., Mitchell, S. and Connelly S. (2019), *Zero trust architecture*, NIST, Gaithersburg, MD, USA, Tech. Rep. NIST 800-207, available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
4. (2022), *DoD Zero Trust Strategy*, Department of Defense, USA, initial published version. 29 p., available at: https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
5. Freter, R. (2022), *Department of Defense (DoD) Zero Trust Reference Architecture*, Version 2.0, In Proceedings of the Defense Information Systems Agency (DISA) and National Security Agency (NSA), USA, July 2022, 104 p., available at: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf
6. Spadaccino, P. and Cuomo, F. (2022), "Intrusion Detection Systems for IoT: Opportunities and Challenges offered by Edge Computing", *arXiv 2022*, doi: https://doi.org/10.48550/arXiv.2012.01174
7. Gavrylenko, S., Poltoratskyi, V. and Nechyporenko, A. (2024), "Intrusion detection model based on improved transformer", *Advanced Information Systems*, vol.8, no.1, pp. 94 – 99, doi: https://doi.org/10.20998/2522-9052.2024.1.12
8. Ullah, S., Boulila, W., Koubâa, A. and J. Ahmad, (2023), "MAGRU-IDS: A Multi-Head Attention-Based Gated Recurrent Unit for Intrusion Detection in IIoT Networks," *IEEE Access*, vol. 11, pp. 114590–114601, doi: https://doi.org/10.1109/ACCESS.2023.3324657
9. Shmatko, O., Kolomiitsev, O., Rekova, N., Kuchuk, N. and Matvieiev, O. (2023), "Designing and evaluating DL-model for vulnerability detection in smart contracts", *Advanced Information Systems*, vol. 7, no. 4, pp. 41–51. doi: https://doi.org/10.20998/2522-9052.2023.4.05
10. Park, C., Lee, J., Kim, Y., Park, J.-G., Kim, H. and Hong, D. (2023), "An Enhanced AI-Based Network Intrusion Detection System Using Generative Adversarial Networks", *IEEE Internet of Things Journal*, vol. 10, no. 3, pp. 2330–2345, doi: https://doi.org/10.1109/JIOT.2022.3211346
11. Said R.B., Sabir, Z. and Askerzade, I. (2023), "CNN-BiLSTM: A Hybrid Deep Learning Approach for Network Intrusion Detection System in Software-Defined Networking With Hybrid Feature Selection", *IEEE Access*, vol. 11, pp. 138732–138747, doi: https://doi.org/10.1109/ACCESS.2023.3340142
12. Sultana, N., Chilamkurti, N., Peng, W. and Alhad, R. (2019), "Survey on SDN based network intrusion detection system using machine learning approaches", *Peer-to-Peer Networking and Applications*, vol. 12, pp. 493–501, doi: https://doi.org/10.1007/s12083-017-0630-0
13. Zaman, S., Alhazmi, Kh., Aseeri, M.A., Ahmed, M.R., Khan, R.T., Kaiser, M.S. and Mahmud, M. (2021), "Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey," *IEEE Access*, vol. 9, pp. 94668–94690, doi: https://doi.org/10.1109/ACCESS.2021.3089681
14. Buczak, A. L. and Guven, E. (2016), "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection", *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, second quarter, doi: https://doi.org/10.1109/COMST.2015.2494502
15. Moustafa, N., Hu, J. and Slay, J. (2019), "A holistic review of Network Anomaly Detection Systems: A comprehensive survey", *Journal of Network and Computer Applications*, vol. 128, pp. 33–55, doi: https://doi.org/10.1016/j.jnca.2018.12.006
16. Khraisat, A., Gondal, I., Vamplew, P. and Kamruzzaman J. (2019), "Survey of intrusion detection systems: techniques, datasets and challenges", *Cybersecurity*, vol. 2, article number 20, doi: https://doi.org/10.1186/s42400-019-0038-7
17. Lee, S.-W., Mohammed sidqi, H., Mokhtar, M., Rashidi, S., Rahmani, A.M., Masdari, M. and Hosseinzadeh, M. (2021), "Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review", J. *Netw. Comput. Appl.*, vol. 187, number 103111, doi: https://doi.org/10.1016/j.jnca.2021.103111
18. Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z. and Doss, R. (2022), "Zero Trust Architecture (ZTA): A Comprehensive Survey," IEEE Access, vol. 10, 12 May 2022, pp. 57143–57179, doi: https://doi.org/10.1109/ACCESS.2022.3174679
19. Yang, Z., Liu, X., Li, T., Wu, D., Wang, J., Zhao, Y. and Han, H. (2022), "A systematic literature review of methods and datasets for anomaly-based network intrusion detection", *Comput. Secur.*, vol. 116, 102675, doi: https://doi.org/10.1016/j.cose.2022.102675
20. Alsoufi, M.A., Razak, S., Siraj, M.M., Nafea, I., Ghaleb, F.A., Saeed, F. and Nasser, M. (2021), "Anomaly-Based Intrusion Detection Systems in IoT Using Deep Learning: A Systematic Literature Review", *Appl. Sci.*, 2021, vol. 11, 8383, doi: https://doi.org/10.3390/app11188383
21. Mishra, A. and Yadav, P. (2020), "Anomaly-based IDS to Detect Attack Using Various Artificial Intelligence & Machine Learning Algorithms: A Review", *2nd International Conference on Data, Engineering and Applications* (IDEA), Bhopal, India, pp. 1–7, doi: https://doi.org/10.1109/IDEA49133.2020.9170674
22. Ferrag, M.A., Friha, O., Hamouda, D., Maglaras, L. and Janicke, H. (2022), "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning," in IEEE Access, vol. 10, pp. 40281-40306. doi: https://doi.org/10.1109/ACCESS.2022.3165809
23. Nuaimi, T.A., Zaabi, S.A., Alyilieli, M., AlMaskari, M., Alblooshi, S., Alhabsi, F., Yusof, M.F.B. and Badawi, A.A. (2023), "A comparative evaluation of intrusion detection systems on the edge-IIoT-2022 dataset, Intelligent Systems with Applications", vol. 20, 200298, ISSN 2667-3053, doi: https://doi.org/10.1016/j.iswa.2023.200298

24. Nkoro, E.C., Njoku, J.N., Nwakanma, C.I., Lee, J.-M. and Kim, D.-S. (2024), “Zero-Trust Marine Cyberdefense for IoT-Based Communications: An Explainable Approach”, *Electronics*, vol. 13, is. 276, doi: https://doi.org/10.3390/electronics13020276
25. Latif, Sh., Boulila, W., Koubaa, A., Zou, Z. and Ahmad, J. (2024), “DTL-IDS: An optimized Intrusion Detection Framework using Deep Transfer Learning and Genetic Algorithm*”, Journal of Network and Computer Applications*, vol. 221, 103784, ISSN 1084-8045, doi: https://doi.org/10.1016/j.jnca.2023.103784

Received (Надійшла) 30.04.2024
Accepted for publication (Прийнята до друку) 10.07.2024

ВІДОМОСТІ ПРО АВТОРІВ/ ABOUT THE AUTHORS

Собчук Валентин Володимирович – доктор технічних наук, професор, професор кафедри інтегральних та диференціальних рівнянь, Київський національний університет імені Тараса Шевченка, Київ, Україна;
Valentyn Sobchuk – Doctor of Technical Sciences, Professor, Professor of the Department of Integral and Differential Equations, Taras Shevchenko Kyiv National University, Kyiv, Ukraine;
email: sobchuk@knu.ua; ORCID Author ID: https://orcid.org/0000-0002-4002-8206;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=25123261200.

Пихнівський Роман Олегович – аспірант кафедри інтегральних та диференціальних рівнянь, Київський національний університет імені Тараса Шевченка, Київ, Україна;
Roman Pykhnivskyi – Postgraduate Student of the Department of Integral and Differential Equations, Taras Shevchenko Kyiv National University, Kyiv, Ukraine;
email: pro1710@gmail.com; ORCID Author ID: https://orcid.org/0009-0000-2514-8210.

Барабаш Олег Володимирович – доктор технічних наук, професор, професор кафедри інженерії програмного забезпечення в енергетиці, Національний технічний університет України “КПІ імені Ігоря Сікорського”, Київ, Україна;
Oleg Barabash – Doctor of Technical Sciences, Professor, Professor of the Department of Software Engineering for Power Industry, National Technical University of Ukraine “Igor Sikorsky Kyiv Polytechnic Institute”, Kyiv, Ukraine;
email: bar64@ukr.net; ORCID Author ID: https://orcid.org/0000-0003-1715-0761;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=36724076700.

Коротін Сергій Михайлович – кандидат технічних наук, доцент, заступник начальника інституту авіації та протиповітряної оборони, Національний університет оборони України, Київ, Україна;
Serhii Korotin – Candidate of Technical Sciences, Assistant Professor, Deputy Chief of Aviation and Air Defense Institute, National Defence University of Ukraine, Kyiv, Ukraine;
email: korotin2008@gmail.com; ORCID Author ID: https://orcid.org/0000-0003-2123-6103;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57207757916.

Омаров Шахін Анвер огли – доктор економічних наук, доцент, професор кафедри комп’ютерно-інтегрованих технологій, автоматизації та робототехніки, Харківський національний університет радіоелектроніки, Харків, Україна;
Shakhin Omarov – Doctor of Economic Sciences, associate Professor, Professor of Computer-Integrated Technologies, Automation and Robotics Department, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: shakhin.omarov@nure.ua; ORCID ID: https://orcid.org/0000-0002-2887-9083;
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=59178850600&origin=recordpage.

Послідовна система виявлення вторгнень для забезпечення кіберзахисту мереж IoT/IIoT на основі принципу нульової довіри

В. В. Собчук, Р. О. Пихнівський, О. В. Барабаш, С. М. Коротін, Ш. А. Омаров

Анотація. Актуальність. Мережі Інтернету Речей (IoT) і Промислового Інтернету Речей (IIoT) та їх широке застосування, роблять їх привабливою мішенню для кібератак. Традиційні методи кібербезпеки, такі як брандмауери та антивірусне програмне забезпечення, не завжди ефективні для захисту мереж IoT/IIoT через неоднорідність та велику кількість підключених приладів. Принцип нульової довіри (zero-trust) може бути більш ефективним методом забезпечення кібербезпеки мереж IoT/IIoT. Це принцип ґрунтується на припущенні, що жоден користувач, пристрій або трафік не є надійним за замовчуванням, і що всі вони повинні бути авторизовані та перевірені перед доступом до будь-якого мережевого ресурсу. **Предметом вивчення** цієї статті є система виявлення вторгнень (IDS) на основі моделей машинного навчання, розроблена для захисту мереж IoT/IIoT побудованих за принципом нульової довіри. **Метою статті** є розробка двокомпонентної IDS для виявлення та класифікації кібератак. В **дослідженні використані** методи машинного навчання, такі як Decision Tree, Random Forest та XGBoost, з використанням сучасного набору даних Edge-IIoTset. Отримано **наступні результати**. Запропонована структура IDS з використанням послідовного підходу, що включає два модулі штучного інтелекту: модуль виявлення зловмисного трафіку за допомогою простої моделі, як-от Decision Tree, і модуль класифікації атак, що використовує більш складні моделі, такі як Random Forest або XGBoost, для класифікації типів атак. Експериментальна оцінка на наборі даних Edge-IIoTset демонструє ефективність системи із загальною точністю 95% та значно меншим часом відповіді порівняно з системами на основі однієї складної моделі. **Висновок.** Запропонований дизайн IDS дозволяє досягти високої точності виявлення атак зі збереженням продуктивності і мінімізацією додаткових обчислювальних витрат, що є критичним для моніторингу мережі у реальному часі в середовищах IoT/IIoT. Також інтеграція IDS із програмно-конфігурованою мережею (SDN) сприяє централізованому контролю, динамічним оновленням політики безпеки та автоматизованим реакціям на загрози. Перспективним **напрямком подальших досліджень** є практична імплементація запропонованої структури IDS для фізичної реалізації в забезпеченні кібербезпеки мереж IoT/IIoT на основі принципу нульової довіри.

Ключові слова: кібербезпека; модель нульової довіри; IoT; IIoT; виявлення вторгнень; машинне навчання.