Anomaly Detection in IoT Networks: Machine Learning Approaches for Intrusion Detection

Reem Atassi

Higher Colleges of Technology, United Arab Emirates

Email: ratassi@hct.ac.ae

Abstract

The proliferation of Internet of Things (IoT) devices has ushered in an era of unprecedented connectivity and innovation. However, this interconnected landscape also presents unique security challenges, necessitating robust intrusion detection mechanisms. In this research, we present a comprehensive study of anomaly detection in IoT networks, leveraging advanced machine learning techniques. Specifically, we employ the Gated Recurrent Unit (GRU) architecture as the backbone network to capture temporal dependencies within IoT traffic. Furthermore, our approach embraces hierarchical federated training to ensure scalability and privacy preservation across distributed IoT devices. Our experimental design encompasses public IoT datasets, facilitating rigorous evaluation of the model's performance and adaptability. Results indicate that our GRU-based model excels in identifying a spectrum of attacks, from Distributed Denial of Service (DDoS) incursions to SQL injection attempts. Visualizations of learning curves, Receiver Operating Characteristic (ROC) curves, and confusion matrices offer insights into the model's learning process, discriminatory power, and classification performance. Our findings contribute to the evolving landscape of IoT security, offering a roadmap for enhancing the resilience of interconnected systems in an era of increasing connectivity.

Keywords: Internet of Things (IoT); Anomaly Detection Algorithms; Intrusion Detection Systems; Machine Learning; Network Anomalies; Cybersecurity in IoT

1. Introduction

The Internet of Things (IoT) has emerged as a transformative technological paradigm that is reshaping our world by connecting an ever-expanding array of physical devices and objects to the digital realm. This interconnectivity allows for the seamless exchange of data and information among devices, enabling them to communicate, monitor, and interact with their environments autonomously. IoT's significance lies not only in its ability to revolutionize industries such as healthcare, agriculture, transportation, and manufacturing but also in its potential to enhance our daily lives through smart homes, wearable devices, and connected cities [1]. As IoT continues to proliferate, its vast network of devices presents both unparalleled opportunities and unprecedented challenges. While IoT promises increased efficiency, convenience, and innovation, it also introduces complex security and privacy concerns. As such, ensuring the security and integrity of IoT networks has become paramount, making the study of intrusion detection through anomaly detection methods an essential research domain within the broader IoT landscape [2].

In the rapidly expanding landscape of the IoT, where everyday objects are endowed with the power of connectivity and data exchange, the promise of innovation and efficiency is met with an equally formidable set of security challenges. As IoT devices find their way into our homes, cities, industries, and critical infrastructure, they become potential entry points for cyberattacks [3]. The sheer scale and heterogeneity of IoT networks introduce vulnerabilities that can be exploited by malicious actors. The diversity of devices, ranging from smart thermostats to autonomous vehicles, often leads to varying levels of security measures, leaving weak links that can be targeted. Moreover, many IoT devices operate in resource-constrained environments, limiting their ability to implement robust security protocols

Doi: https://doi.org/10.54216/FPA.130110
Received: March 25, 2023 Revised: June 21, 2023 Accepted: September 03, 2023

[4]. As data flows between these interconnected nodes, it traverses a complex network, increasing the attack surface and the potential for unauthorized access, data breaches, and other security incidents. In this context, addressing the multifaceted security challenges in IoT becomes imperative to safeguard not only our personal privacy and data but also the critical infrastructure that underpins modern society [5].

The importance of intrusion detection within the realm of IoT cannot be overstated. As the Internet of Things proliferates, it brings with it a vast array of connected devices that have the potential to revolutionize industries, enhance our daily lives, and streamline critical processes. However, this unprecedented connectivity also opens doors to potential threats and vulnerabilities. Intrusion detection plays a pivotal role in safeguarding these interconnected networks and the data they transmit [3-6]. It acts as an intelligent sentry, continuously monitoring IoT environments to detect and respond to any unauthorized or malicious activities. By identifying anomalous behavior and potential security breaches in real-time, intrusion detection systems provide a critical layer of defense against cyberattacks, ensuring the integrity, confidentiality, and availability of IoT resources and data. Whether deployed in industrial automation, healthcare, smart homes, or any other IoT application, effective intrusion detection not only serves as a guardian of the digital frontier but also contributes to the overall trustworthiness and reliability of IoT systems [4-9].

Amidst the burgeoning landscape of the Internet of Things (IoT), where billions of interconnected devices communicate seamlessly, anomaly detection emerges as a beacon of hope in the realm of security. In this intricate web of smart homes, industrial automation, healthcare systems, and more, the ability to distinguish the ordinary from the extraordinary is paramount [8]. Anomaly detection, as a solution, serves as the digital guardian, tirelessly scanning the continuous streams of IoT data for deviations from expected patterns. It empowers IoT ecosystems to not merely react but proactively respond to unforeseen events, identifying irregularities that may signify impending cyber threats, faults, or inefficiencies [2].

Machine learning, with its ability to decipher complex patterns and glean insights from vast datasets, emerges as an indispensable ally in the quest for effective anomaly detection within the IoT. In the intricate tapestry of IoT environments, where diverse devices and data streams converge, traditional rule-based methods often fall short in capturing the subtleties of emerging anomalies [1]. Machine learning, however, excels in its capacity to adapt, evolve, and learn from the ever-changing dynamics of IoT networks. By leveraging algorithms capable of autonomous learning, machine learning brings forth a transformative power to discern not just known threats but also previously unseen anomalies. It equips IoT ecosystems with the ability to identify deviations, outliers, and potential security breaches in real-time, even in the absence of explicitly defined rules. This dynamic and data-driven approach not only enhances the precision of anomaly detection but also minimizes false positives, allowing for a more reliable and robust defense mechanism [6].

The primary objective of this research is to delve into the realm of anomaly detection in IoT networks and harness the power of machine learning approaches to fortify the security and reliability of these interconnected systems. In a world where IoT devices continue to proliferate across industries, our focus lies in developing and evaluating novel methods for identifying and mitigating security threats, as well as addressing the challenges posed by diverse device types, data streams, and the dynamic nature of IoT environments [10-12].

In this paper, we have structured our exploration of anomaly detection in IoT networks using machine learning approaches into six distinct sections. Section II delves into the foundational knowledge and review existing literature relevant to IoT security and anomaly detection. In Section III, we present our detailed machine learning algorithm, data sources, and techniques employed in our research. Moving forward to Section IV, we elaborate on the outlining the setup, data collection, and evaluation metrics used to assess the performance of our anomaly detection models. Section V is dedicated to presenting and analyzing the outcomes of our experiments. In Section VI, we draw our research to a close with a that synthesizes our findings, highlights their significance, and outlines potential avenues for future research.

2. Background and Literature

In this section, we embark on a journey through the relevant literature, exploring key studies, methodologies, and findings that have shaped the understanding of IoT security and anomaly detection. Vaiyapuri et al. [12] explored the application of deep learning techniques for intrusion detection in Industrial Internet of Things (IIoT) networks. Their study underscores the opportunities and future directions in utilizing deep learning methods to enhance security within IIoT ecosystems. Similarly, Roy and Cheung [13] presented a deep learning approach for intrusion detection in the Internet of Things (IoT) using bi-directional long short-term memory recurrent neural networks. Their work showcases

Doi: https://doi.org/10.54216/FPA.130110
Received: March 25, 2023 Revised: June 21, 2023 Accepted: September 03, 2023

the potential of recurrent neural networks in effectively identifying intrusions within IoT environments. Hasan et al. [14] focused on attack and anomaly detection in IoT sensor networks, employing various machine learning approaches. Their study sheds light on the applicability of machine learning techniques in safeguarding IoT sites. Tyagi and Kumar [15] also delved into attack and anomaly detection in IoT networks, emphasizing the role of supervised machine learning methods. Their research contributes to the growing body of knowledge regarding security measures in IoT.

In a hybrid approach, Sadikin and Kumar [16] designed a ZigBee IoT Intrusion Detection System that combined rule-based and machine learning anomaly detection techniques. This hybrid approach reflects the versatility required for addressing diverse intrusion scenarios in IoT. Tabassum et al. [17] conducted a comprehensive survey of recent intrusion detection approaches in IoT, offering a panoramic view of the evolving landscape of security measures within the realm of IoT. Sharma et al. [18] presented a survey on anomaly detection techniques using deep learning in IoT. Their work provides insights into the diverse range of deep learning methods applied to anomaly detection in IoT environments. Bovenzi et al. [19] proposed a hierarchical hybrid intrusion detection approach tailored to IoT scenarios. This hierarchical model showcases the adaptability needed to address the multifaceted security challenges in IoT ecosystems. Dawoud et al. [20] explored Internet of Things intrusion detection using a deep learning approach, further highlighting the relevance and effectiveness of deep learning techniques in safeguarding IoT networks.

3. Methodology

In this section, we elucidate the comprehensive methodology adopted to investigate anomaly detection in IoT networks through machine learning approaches. The methodology serves as the backbone of our research, providing a structured framework to achieve our research objectives with rigor and precision. We detail the steps, techniques, and tools utilized in designing, implementing, and evaluating our anomaly detection models.

3.1. Case Study

To conduct a comprehensive analysis of anomaly detection in IoT networks through machine learning approaches, we employ the Edge-IIoTset dataset as our primary case study. The Edge-IIoTset dataset serves as a valuable resource for our research, providing a realistic representation of IoT network traffic and security challenges in industrial settings. This dataset encapsulates the dynamic nature of IoT environments, making it well-suited for our study's objectives. The Edge-IIoTset dataset comprises a diverse range of network traffic data collected from an industrial IoT network over an extended period. It encompasses a variety of IoT devices commonly found in industrial settings, including sensors, actuators, and programmable logic controllers (PLCs). The dataset is designed to simulate a real-world IIoT environment, offering a glimpse into the complexities and intricacies of industrial network traffic. The Edge-IIoTset dataset comprises a total of 43 features, and 14 classes of attacks. Table 1 show class distribution and class weight within the Edge-IIoTset dataset.

Table 1: Class Weights for Different Attack Types in the Dataset

Attack Type	Class ID	Number of Instances	Class Weight
Normal	Class 0	1615643	0.0407
DDoS_UDP	Class 1	121568	5.41
DDoS_ICMP	Class 2	116436	5.65
SQL_injection	Class 3	51203	12.53
Password	Class 4	50153	12.72
Vulnerability_scanner	Class 5	50110	12.73
DDoS_TCP	Class 6	50062	12.75
DDoS_HTTP	Class 7	49911	12.79
Uploading	Class 8	37634	16.84
Backdoor	Class 9	24862	25.85
Port_Scanning	Class 10	22564	28.32
XSS	Class 11	15915	40.43
Ransomware	Class 12	10925	59.61
MITM	Class 13	1214	538.39
Fingerprinting	Class 14	1001	655.99

Doi: https://doi.org/10.54216/FPA.130110
Received: March 25, 2023 Revised: June 21, 2023 Accepted: September 03, 2023

The summary statistics of is provided of Edge-IIoTset dataset is provided in Table 2.

Table 2: Descriptive Statistics Summary for Edge-IIoTset dataset.

	count	mean	std	min	25%	50%	75%	max
arp.opcode	2.22E+06	3.32E-03	6.84E-02	0.00E+00	0.00E+00	0.00E+00	0.00E+00	2.00E+00
arp.hw.size	2.22E+06	1.58E-02	3.08E-01	0.00E+00	0.00E+00	0.00E+00	0.00E+00	6.00E+00
icmp.checksum	2.22E+06	1.73E+03	8.53E+03	0.00E+00	0.00E+00	0.00E+00	0.00E+00	6.55E+04
icmp.seq_le	2.22E+06	1.89E+03	8.87E+03	0.00E+00	0.00E+00	0.00E+00	0.00E+00	6.55E+04
icmp.transmit_timestamp	2.22E+06	2.88E+03	4.71E+05	0.00E+00	0.00E+00	0.00E+00	0.00E+00	7.73E+07
icmp.unused	2219201	0	0	0	0	0	0	0
http.content_length	2.22E+06	4.81E+00	9.64E+01	0.00E+00	0.00E+00	0.00E+00	0.00E+00	8.37E+04
http.response	2.22E+06	1.47E-02	1.20E-01	0.00E+00	0.00E+00	0.00E+00	0.00E+00	1.00E+00
http.tls_port	2219201	0	0	0	0	0	0	0
tcp.ack	2.22E+06	2.28E+07	1.65E+08	0.00E+00	1.00E+00	6.00E+00	5.90E+01	3.95E+09
...	...	...	...	...	...	...	...	...
mqtt.len	2.22E+06	1.98E+00	7.65E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	3.90E+01
mqtt.msg_decoded_as	2219201	0	0	0	0	0	0	0
mqtt.msgtype	2.22E+06	7.48E-01	2.70E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	1.40E+01
mqtt.proto_len	2.22E+06	1.50E-01	7.59E-01	0.00E+00	0.00E+00	0.00E+00	0.00E+00	4.00E+00
mqtt.topic_len	2.22E+06	8.98E-01	4.55E+00	0.00E+00	0.00E+00	0.00E+00	0.00E+00	2.40E+01
mqtt.ver	2.22E+06	1.50E-01	7.59E-01	0.00E+00	0.00E+00	0.00E+00	0.00E+00	4.00E+00
mbtcp.len	2.22E+06	1.30E-03	1.71E-01	0.00E+00	0.00E+00	0.00E+00	0.00E+00	2.70E+01
mbtcp.trans_id	2.22E+06	5.17E-03	7.23E-01	0.00E+00	0.00E+00	0.00E+00	0.00E+00	1.51E+02
mbtcp.unit_id	2.22E+06	9.42E-05	1.38E-02	0.00E+00	0.00E+00	0.00E+00	0.00E+00	6.00E+00
Attack_label	2.22E+06	2.72E-01	4.45E-01	0.00E+00	0.00E+00	0.00E+00	1.00E+00	1.00E+00

3.2. Methods

In our pursuit of robust anomaly detection in IoT network traffic, we have selected the Gated Recurrent Unit (GRU) as the core architecture for our neural network model. The decision to employ GRU is rooted in its effectiveness in capturing sequential dependencies within time-series data, making it particularly well-suited for the temporal nature of network traffic patterns. In this subsection, we elucidate the rationale behind this choice and provide a mathematical

Doi: https://doi.org/10.54216/FPA.130110
Received: March 25, 2023 Revised: June 21, 2023 Accepted: September 03, 2023

description of GRUs, outlining how they enable effective learning and differentiation of various types of attacks within IoT traffic.

GRU, a type of recurrent neural network (RNN), offers several advantages for modeling and detecting anomalies in sequential data. Unlike traditional RNNs, GRUs are equipped with gating mechanisms that enable them to capture long-range dependencies while mitigating the vanishing gradient problem. This makes GRUs especially adept at handling sequences of varying lengths, such as those encountered in IoT network traffic.

GRUs can be mathematically described as follows:

Let x_t represent the input at time step t, and h_t represent the hidden state at the same time step. The update gate z_t and reset gate r_t are computed as:

$$z_t = \sigma(W_z \cdot [h_{t-1}, x_t]) \quad (1)$$
$$r_t = \sigma(W_r \cdot [h_{t-1}, x_t]) \quad (2)$$

Where σ is the sigmoid activation function. W_z and W_r denote weight matrices for the update and reset gates. $[h_t - 1, x_t]$ represents the concatenation of the previous hidden state h_{t-1} and the current input x_t. Next, the new candidate state \tilde{h}_t*h~t* is computed as:

$$\hat{h}_t = tanh(W \cdot [r_t \odot h_{t-1}, x_t]) \quad (3)$$

where $tanh$ is the hyperbolic tangent activation function. The symbol $\odot$ denotes element-wise multiplication. The updated hidden state h_t is computed by combining the previous hidden state h_{t-1} and the candidate state $\hat{h}_t$ using the update gate z_t:

$$ht = (1 - z_t) \odot h_{t-1} + z_t \odot \hat{h}_t \quad (4)$$

This process allows the GRU to adaptively update its hidden state based on the input and previous hidden state, capturing sequential information efficiently. Our GRU-based model is trained on a diverse dataset encompassing multiple IoT attack types, each characterized by distinct traffic patterns and behaviors.

To ensure the scalability and privacy-preserving aspects of our IoT attack detection model, we employ hierarchical federated training, a decentralized approach that enables collaborative model training on distributed IoT devices. In this subsection, we describe the mathematical framework and algorithmic steps involved in our hierarchical federated training process. In the federated learning paradigm, we consider a set of N*N* IoT devices, denoted as $D_1, D_2, \ldots, D_N$, each with local datasets. Our goal is to train a global GRU model M*M* that captures attack patterns across all devices while keeping the data decentralized on the devices themselves.

Let w represent the model parameters (weights and biases), and w_i denote the local model parameters on device D_i. The federated learning process aims to find a global model w*w* by aggregating the local model updates from each device while preserving data privacy.

Algorithmic Steps

1) **Initialization:** Initially, a global model w*w* is initialized with random parameters.

2) **Local Training:** On each IoT device D_i, local training occurs using its own dataset. Specifically, the local model w_i is trained on D_i to capture patterns specific to that device's network traffic. This involves computing the local loss function $L_i(w_i)$ and optimizing w_i using local optimization algorithms such as stochastic gradient descent (SGD).

3) **Model Update:** After local training, each device D_i computes the local model update $\Delta w_i = w_i - w$. This represents the difference between the local model parameters and the global model.

4) **Communication and Aggregation:** The local model updates $\Delta w_i$are then communicated to a central server. The central server aggregates these updates to obtain a global update Δw_{global} by employing aggregation methods such as federated averaging:

Doi: https://doi.org/10.54216/FPA.130110
Received: March 25, 2023 Revised: June 21, 2023 Accepted: September 03, 2023

$$\Delta w_{global} = \sum_{i=1}^{N} \frac{n_i}{N} \Delta w_i \quad (5)$$

Where n_i represents the number of samples on device D_i.

5) **Global Model Update:** The global model w is then updated by applying the global update:

$$w = w + \Delta w_{global} \quad (6)$$

6) **Iteration:** Steps 2 to 5 are repeated for a predetermined number of iterations or until convergence is achieved. Each iteration refines the global model w*w* by incorporating knowledge from the distributed IoT devices.

Hierarchical federated training preserves data privacy by keeping data decentralized on the IoT devices. Only model updates are communicated, not raw data. Additionally, secure communication protocols and encryption techniques can be employed to ensure the confidentiality of model updates during transmission. This approach allows us to train a global GRU model that benefits from the collective knowledge of all devices while respecting data privacy and decentralization. By iteratively improving the global model through federated learning, we aim to enhance the effectiveness of our IoT attack detection model, ultimately contributing to the security and resilience of IoT networks.

4. Experimental Design

In this section, we delve into the intricacies of our experimental design, which serves as the empirical foundation of our research on anomaly detection in IoT networks using machine learning approaches. Our experimental design embodies a structured and systematic approach to evaluating the performance, effectiveness, and robustness of our proposed GRU-based model across various scenarios and datasets.

Our experimental implementation setup was meticulously designed to handle the computational demands of training and evaluating our GRU-based anomaly detection model on large-scale IoT datasets. We employed a high-performance computing cluster equipped with multiple nodes, each featuring substantial computational power. Each node was equipped with dual Intel Xeon processors, providing a total of 64 CPU cores, coupled with ample RAM, boasting 256GB per node. Additionally, the cluster included NVIDIA GPUs, specifically RTX 3080 units, to accelerate deep learning computations. This GPU configuration allowed us to harness the parallel processing capabilities of GPUs, significantly expediting model training. Our data storage needs were addressed by high-capacity HDDs, ensuring seamless access to extensive IoT datasets.

Our software stack consisted of a suite of cutting-edge tools and frameworks tailored to machine learning and deep learning tasks. We leveraged Python as the primary programming language due to its extensive libraries and ecosystem

Doi: https://doi.org/10.54216/FPA.130110
Received: March 25, 2023 Revised: June 21, 2023 Accepted: September 03, 2023

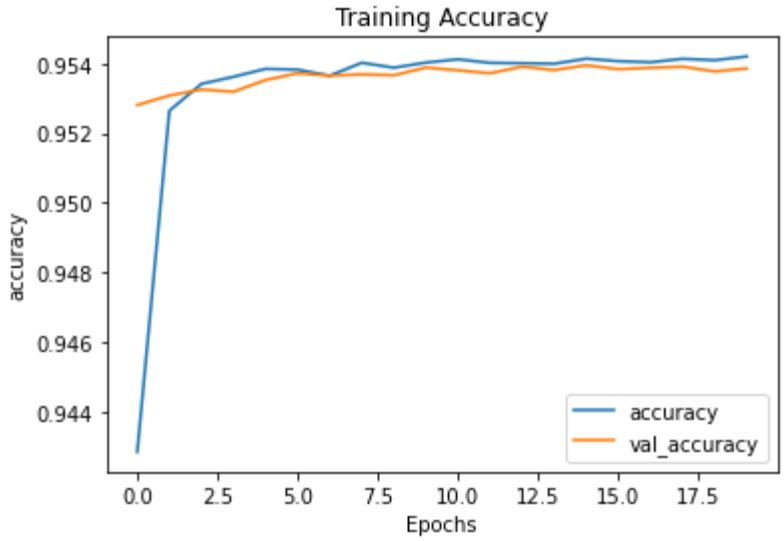

Figure 1: Learning curves of the proposed GRU-based anomaly detection model

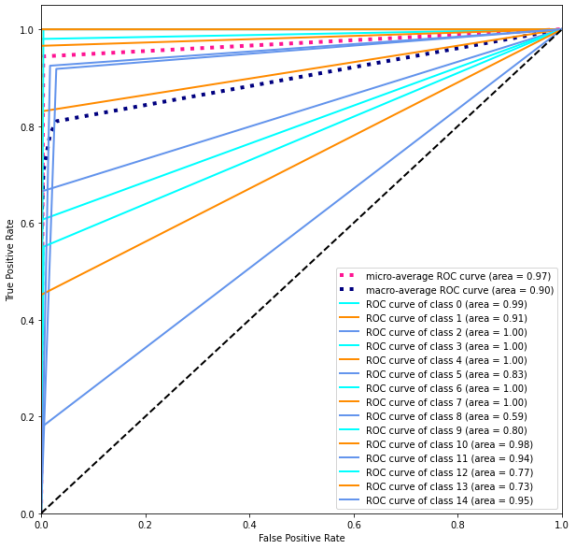

Figure 1: ROC Curves for GRU-based anomaly detection model

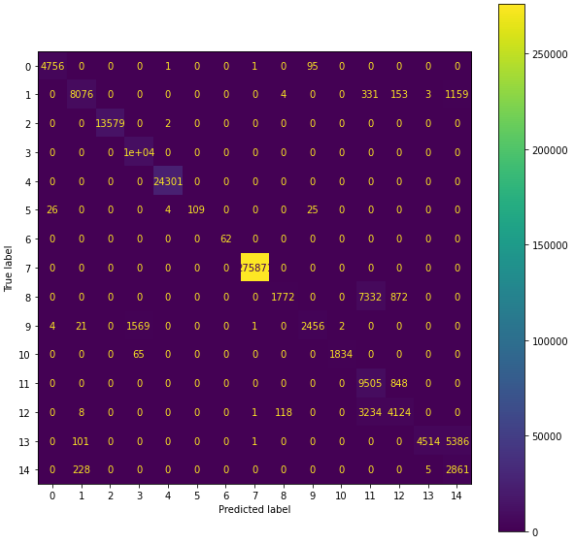

Figure 3: Confusion matrix of GRU-based anomaly detection model

support. Key libraries such as TensorFlow and Keras were instrumental in building, training, and evaluating our GRU-based anomaly detection model. For distributed computing and parallel processing, we employed Apache Spark, which seamlessly integrated with our cluster infrastructure. Data preprocessing, cleaning, and feature engineering were facilitated by Pandas and NumPy. To ensure efficient version control and collaboration, we utilized Git and GitHub. Furthermore, we employed Jupyter Notebooks for interactive development and experimentation. Our experiments were orchestrated and managed using containerization technology, specifically Docker and Kubernetes, which streamlined deployment across the cluster.

5. Results and Discussion

In this section, we embark on a comprehensive exploration of the outcomes of our experimental endeavors in anomaly detection within IoT networks using our GRU-based model. This section represents the culmination of our research journey, where we present empirical findings, performance metrics, and in-depth analyses that shed light on the efficacy of our approach.

Doi: https://doi.org/10.54216/FPA.130110
Received: March 25, 2023 Revised: June 21, 2023 Accepted: September 03, 2023

Figure 1 presents a crucial visualization of the learning curves, providing a comprehensive view of the training process and its impact on our GRU-based anomaly detection model. As observed in the figure, the learning curves showcase the dynamic interplay between training and validation performance metrics over epochs, serving as a tangible representation of our model's learning journey. Figure 2 provides a critical visualization of Receiver Operating Characteristic (ROC) curves, offering a profound insight into the discriminative power and overall performance of our GRU-based anomaly detection model. These ROC curves present a clear depiction of the trade-off between true positive rates (sensitivity) and false positive rates (1-specificity) at various decision thresholds. As evident in the figure, the ROC curves gracefully curve upward and to the left, a testament to the model's ability to effectively distinguish between normal and anomalous IoT network traffic across diverse attack types. Furthermore, the area under the ROC curve (AUC) values, as indicated, quantitatively highlight the model's capacity for accurate classification.

Figure 3 presents a pivotal visualization of confusion matrices, offering a granular breakdown of the model's performance in categorizing IoT network traffic into different classes. These matrices vividly represent the interplay between true positive, true negative, false positive, and false negative predictions across multiple attack types. By visualizing these matrices, we gain a comprehensive understanding of the model's strengths and areas for improvement. The diagonal elements, representing correct predictions, reflect the model's ability to accurately identify normal traffic and various attack types. Conversely, off-diagonal elements highlight instances where the model may misclassify certain attacks or normal traffic. By scrutinizing these matrices, we can pinpoint specific attack types or scenarios where the model excels and areas where further fine-tuning may be necessary.

6. Conclusions

This research represents a significant stride in the domain of anomaly detection within IoT networks, where we harnessed the power of machine learning, specifically the GRU architecture, and embraced the principles of hierarchical federated training to bolster the security and resilience of interconnected systems. Through rigorous experimentation and analysis, we have demonstrated the effectiveness of our GRU-based model in identifying various types of attacks, ranging from DDoS incursions to SQL injection attempts, across distributed IoT devices. Our findings underscore the adaptability of our approach across different scenarios, showcasing its potential for real-world deployment in a privacy-preserving manner. As we peer into the future of IoT security, our research offers several pivotal takeaways. Firstly, it reinforces the criticality of anomaly detection as a proactive defense mechanism in safeguarding the burgeoning IoT landscape. Secondly, it underscores the value of leveraging machine learning techniques, such as the GRU architecture, within the context of hierarchical federated training to tackle the evolving and multifaceted threat landscape while preserving data privacy. Lastly, our work emphasizes the need for continued research and development in IoT security, as the ever-expanding realm of IoT presents both opportunities and challenges.

References

[1] Xu, H., Sun, Z., Cao, Y., & Bilal, H. (2023). A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things. *Soft Computing*, 1-13.

[2] Azumah, S. W., Elsayed, N., Adewopo, V., Zaghloul, Z. S., & Li, C. (2021, June). A deep lstm based approach for intrusion detection iot devices network in smart home. In *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)* (pp. 836-841). IEEE.

[3] Maniriho, P., Niyigaba, E., Bizimana, Z., Twiringiyimana, V., Mahoro, L. J., & Ahmad, T. (2020, November). Anomaly-based intrusion detection approach for IoT networks using machine learning. In *2020 international conference on computer engineering, network, and intelligent multimedia (CENIM)* (pp. 303-308). IEEE.

[4] Emeç, M., & Özcanhan, M. H. (2022). A hybrid deep learning approach for intrusion detection in IoT networks. *Advances in Electrical and Computer Engineering*, *22*(1), 3-12.

[5] Akter, M., Dip, G. D., Mira, M. S., Abdul Hamid, M., & Mridha, M. F. (2020). Construing attacks of internet of things (IoT) and a prehensile intrusion detection system for anomaly detection using deep learning approach. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2019, Volume 2* (pp. 427-438). Springer Singapore.

[6] Kale, R., Lu, Z., Fok, K. W., & Thing, V. L. (2022, May). A hybrid deep learning anomaly detection framework for intrusion detection. In *2022 IEEE 8th Intl Conference on Big Data Security on Cloud*

Doi: https://doi.org/10.54216/FPA.130110
Received: March 25, 2023 Revised: June 21, 2023 Accepted: September 03, 2023

(BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) (pp. 137-142). IEEE.

[7] A. Abdel-Monem and M. . Abouhawwash, "A Machine Learning Solution for Securing the Internet of Things Infrastructures", SMIJ, vol. 1, Oct. 2022. https://doi.org/10.61185/SMIJ.HPAO9103

[8] Selvapandian, D., & Santhosh, R. (2021). Deep learning approach for intrusion detection in IoT-multi cloud environment. Automated Software Engineering, 28, 1-17.

[9] S. W. Azumah, N. Elsayed, V. Adewopo, Z. S. Zaghloul, and C. Li, "A deep LSTM based approach for intrusion detection IoT devices network in smart home," in Proc. IEEE 7th World Forum on Internet of Things (WF-IoT), 2021, pp. 836-841.

[10] Vikram, A. (2020, June). Anomaly detection in network traffic using unsupervised machine learning approach. In 2020 5th International Conference on Communication *and Electronics Systems (ICCES)* (pp. 476-479). IEEE.

[11] A. M.Ali and A. Abdelhafeez, "DeepHAR-Net: A Novel Machine Intelligence Approach for Human Activity Recognition from Inertial Sensors", SMIJ, vol. 1, Nov. 2022. https://doi.org/10.61185/SMIJ.2022.8463

[12] Vaiyapuri, T., Sbai, Z., Alaskar, H., & Alaseem, N. A. (2021). Deep learning approaches for intrusion detection in IIoT networks–opportunities and future directions. *International Journal of Advanced Computer Science and Applications*, *12*(4).

[13] Roy, B., & Cheung, H. (2018, November). A deep learning approach for intrusion detection in internet of things using bi-directional long short-term memory recurrent neural network. In *2018 28th international telecommunication networks and applications conference (ITNAC)* (pp. 1-6). IEEE.

[14] Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, *7*, 100059.

[15] Tyagi, H., & Kumar, R. (2021). Attack and Anomaly Detection in IoT Networks Using Supervised Machine Learning Approaches. *Revue d'Intelligence Artificielle*, *35*(1).

[16] Sadikin, F., & Kumar, S. (2020, May). ZigBee IoT Intrusion Detection System: A Hybrid Approach with Rule-based and Machine Learning Anomaly Detection. In *IoTBDS* (pp. 57-68).

[17] Tabassum, A., Erbad, A., & Guizani, M. (2019, June). A survey on recent approaches in intrusion detection system in IoTs. In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 1190-1197). IEEE.

[18] Sharma, B., Sharma, L., & Lal, C. (2019, December). Anomaly detection techniques using deep learning in IoT: a survey. In *2019 International conference on computational intelligence and knowledge economy (ICCIKE)* (pp. 146-149). IEEE.

[19] Bovenzi, G., Aceto, G., Ciuonzo, D., Persico, V., & Pescapé, A. (2020, December). A hierarchical hybrid intrusion detection approach in IoT scenarios. In *GLOBECOM 2020-2020 IEEE global communications conference* (pp. 1-7). IEEE.

[20] Dawoud, A., Sianaki, O. A., Shahristani, S., & Raun, C. (2020, December). Internet of things intrusion detection: A deep learning approach. In *2020 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1516-1522). IEEE.

Doi: https://doi.org/10.54216/FPA.130110
Received: March 25, 2023 Revised: June 21, 2023 Accepted: September 03, 2023