Journal of Information Systems Engineering and Management
2025, 10(9s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Integrated Intrusion Detection and Mitigation Framework for SDN-Based IIoT Networks Using Lightweight and Adaptive AI Techniques

Mamatha Maddu[1] · Yamarthi Narasimha Rao[1,*]
[1]*School of Computer Science and Engineering,VIT-AP Uinversity,Amaravati,India-522237.*
Email: mamatha.22phd7103@vitap.ac.in
Corresponding Email: y.narasimharao@vitap.ac.in

ARTICLE INFO

Received: 30 Oct 2024

Revised: 18 Dec 2024

Accepted: 04 Jan 2025

ABSTRACT

Advanced and scalable intrusion detection frameworks are in great demand for the rapid proliferation of Software-Defined Networking (SDN) in Industrial Internet of Things (IIoT) environments. Traditional methods for network anomaly detection fail to adapt to dynamic traffic patterns, handle resource-constrained edge deployments, and utilize vast amounts of unlabeled data samples. To address these limitations, we propose an integrated framework combining state-of-the-art techniques for accurate, efficient, and scalable intrusion detection in SDN-based IIoT networks. Our framework starts with domain-adapted feature extraction by the use of EfficientNet-B0, a lightweight yet powerful architecture, fine-tuned on IIoT-specific traffic data samples. Incremental learning with Elastic Weight Consolidation ensures adaptability to new intrusion patterns while preserving previously learned knowledge. SimCLR is applied to generate robust embeddings through self-supervised learning in environments where labeled data are scarce. Autoencoders detect novel patterns in anomaly detection, while XGBoost conducts precise classification of known threats. Furthermore, DQN optimizes the mitigation strategy of either flow rerouting or rate limiting in real time based on the network state. In case of edge-based deployment, Tiny-YOLO presents a lightweight model for anomaly detection that performs low latency with high accuracy. This holistic framework achieves a detection accuracy of ~96%, with a false positive rate below 3% and a latency of under 15 ms, supporting the large-scale IIoT networks of more than 10,000 nodes. Our methodology pushes forward scalability, adaptability, and robustness by unifying feature extraction, anomaly detection, classification, and mitigation process

Keywords: EfficientNet-B0, Incremental Learning, Self-Supervised Learning, Anomaly Detection, IIoT Security, Samples

Abbreviation	Full Form
IDS	Intrusion Detection System
IoT	Internet of Things
IIoT	Industrial Internet of Things
SDN	Software-Defined Networking
ML	Machine Learning
EWC	Elastic Weight Consolidation
SimCLR	Simple Contrastive Learning
DQN	Deep Q-Learning
GAN	Generative Adversarial Network
VAE	Variational Autoencoder
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
AUC	Area Under the Curve

FPR	False Positive Rate
F1-Score	Harmonic Mean of Precision and Recall
CAN Bus	Controller Area Network Bus
IoMT	Internet of Medical Things
WSN	Wireless Sensor Network
SMOTETomek	Synthetic Minority Oversampling Technique Combined with Tomek Links
MLSTL	Machine Learning-Based Synthetic and Tomek Links
XGBoost	eXtreme Gradient Boosting
AI	Artificial Intelligence
GPU	Graphics Processing Unit
TPU	Tensor Processing Unit

APT	Advanced Persistent Threat
QoS	Quality of Service
IoT-IDS	Internet of Things Intrusion Detection System
WSN-IoT	Wireless Sensor Network Internet of Things
IoMT-IDS	Internet of Medical Things Intrusion Detection System
ML-IDS	Machine Learning Intrusion Detection System
SDN-IDS	Software-Defined Networking Intrusion Detection System
SMOTE	Synthetic Minority Oversampling Technique

1. INTRODUCTION

The rapid growth of IIoT has revolutionized the traditional industrial networks that integrated smart devices, sensors, and controllers into interconnected ecosystems. However, with the increased connectivity and reliance on SDN for managing IIoT networks [1, 2, 3], such systems are open to a broad spectrum of security threats, ranging from sophisticated intrusions to cyberattacks. Existing IDSs do not satisfy the strict challenges that IIoT scenarios pose, including resource starvation on edge devices, inadequately labeled training data, and the need to evolve quickly in order to keep up with emerging threats. Traditional IDS solutions [4, 5, 6] use mostly static feature extraction as well as fixed rule-based mechanisms which prove to be inadequate for dynamics and heterogeneity of the traffic in the IIoT. Also, with a very high requirement for having good detection accuracy at minimal latency, the system often becomes challenging for the latter. Recent developments in machine learning and deep learning have provided hope for enhancing IDS capabilities, but standalone techniques fall short of scalability, robustness, and adaptability in real-world IIoT scenarios. This work introduces an integrated, multi-layered framework that addresses those deficiencies by incorporating cutting-edge AI techniques and lightweight models. First, the framework would adapt domain-specific feature extraction utilizing EfficientNet-B0 neural network architecture, finely optimized for IIoT-traffic patterns. Finally, incremental learning using EWC ensures that the system would remain adaptive on newly presented intrusion patterns and retain all previously acquired knowledge. Self-supervised learning using SimCLR uses tremendous amounts of data that are not labeled and are resilient to anomalies, with improved anomaly detection. Detection precision further increases with false positives when using a hybrid detection mechanism involving autoencoders and XGBoost. At the tail, finally, for real-time optimization of mitigation strategies using Deep Q-Learning or DQN, Tiny-YOLO permits deployment at the edge in light-weight, low latency. The integrated framework enables both robust intrusion detection as well as mitigation at high accuracies and minimum false positives in terms of low latencies. Integration of state-of-the-art methods across this platform makes it capable to secure scalable and efficient approaches to prevent evolving SDN-based IIoT networks.

Motivation & Contribution

This exponential growth of IIoT networks has brought about unprecedented opportunities in industrial automation and operational efficiency. However, this integration of SDN and IIoT has created a highly dynamic network environment susceptible to very sophisticated and ever-changing cyber threats. Current intrusion detection systems cannot meet the high demands of IIoT environments, especially regarding scalability, adaptability, and efficiency. The further aggravations of the issues mentioned above, such as real-time processing, a scarcity of labeled data, and economical deployment of resources, make things worse for the above-mentioned limitations. Inspired by a strong need for proper and scalable security solutions in this work, an advanced framework is proposed to meet the limitations of traditional IDS along with incorporating recent advancements from AI, in order to provide complete security mechanism for SDN-based IIoT networks. The main contributions of this work are: (1) A new application of EfficientNet-B0 with domain adaptation for feature extraction, which guarantees lightweight and effective handling of IIoT-specific traffic patterns. (2) Incremental learning with Elastic Weight Consolidation (EWC) to adapt continuously to new intrusion patterns without performance degradation on prior knowledge. (3) A self-supervised learning module using SimCLR to leverage unlabeled traffic data and enhance robustness. (4) Autoencoder and XGBoost combined hybrid anomaly detection system which will improve the accuracy rate and reduce false positive numbers. (5) DQN-based mitigation approach through RL for optimizing the action real-time. (6) Lightweight models for tiny-yolo for the implementation in the edge so as not to delay detection at much time. This integrated framework brings a transformative approach to the security of IIoT systems, achieving high scalability, adaptability, and operational efficiency while significantly reducing the latency of detection and false positives.

2. REVIEW OF EXISTING MODELS FOR IDS ANALYSIS

In this section, we discuss recent methods for IDS Analysis. This was supported by Wang et al. [1, 2], who demonstrated that learning from multiple sources is indeed effective in intrusion detection scenarios. Indeed, Talukder et al. [3] have worked with machine learning-based systems, using SMOTETomek over wireless sensor networks, through which techniques of balancing data improve the robustness of the model. Li et al. [4] and Altamimi et al. [5] contrast some feature selection and extraction techniques concerning IoT intrusion detection, at the same time underlining some trade-offs involving a certain accuracy versus computational complexity. More IoT-specific applications were discovered in Alemerien et al. [6], who optimizes the efficiency and resource usage of a machine learning-driven IDS balancing, and Ngo et al. [7], who dug deep into feature engineering approaches. Roshan et al. [8] proposed an ensemble adaptive model to process the data streams of IDS. Kantharaju et al. [9] and Getman et al. [10] introduced deep learning methods emphasizing the ability of processing complicated network traffic patterns. Maseno et al. [11] utilized genetic algorithms for feature selection with an achievement of high precision for attack classification. Tiwari et al. [12] highlighted edge-based IIoT security based on the development of lightweight models for real-time detection. Saied et al. [13] compared boosting algorithms based on their adaptability in evolving networks. Patel et al. [14] developed a new dataset for ML-based attack classification, filling the gaps concerning the availability of training datasets & samples.

Reference	**Method**	**Main Objectives**	**Findings**	**Limitations**
[1]	Quantum particle swarm optimized extreme learning machine	Enhance accuracy and efficiency in intrusion detection	Achieved improved accuracy and faster convergence compared to traditional methods.	Requires high computational resources for large-scale deployments.
[2]	Transfer extreme learning machine from multiple sources	Enable transfer learning for intrusion detection	Demonstrated effective knowledge transfer from multiple data sources to improve model adaptability.	Dependency on quality and relevance of source datasets.
[3]	MLSTL-WSN with SMOTETomek	Address class imbalance in wireless sensor networks	Balanced data led to higher detection rates, especially for minority attack classes.	Potential overfitting with imbalanced validation datasets.
[4]	Feature selection vs. feature extraction for IoT IDS	Optimize feature engineering approaches	Showed feature extraction yields better results in high-dimensional IoT traffic scenarios.	Increased complexity and preprocessing time for feature extraction.
[5]	Maximizing intrusion detection using extreme learning machine	Improve efficiency of IoT network intrusion detection	Achieved high efficiency and reduced overhead in IoT-specific environments.	Limited scalability to highly dynamic networks.

[6]	Optimized ML-driven intrusion detection for IoT	Develop resource-efficient detection for IoT devices	Demonstrated reduced false positives and improved precision.	Suboptimal performance in handling advanced persistent threats.
[7]	Feature selection vs. feature extraction for IDS	Compare feature engineering approaches	Found feature extraction to be more effective for high Variance datasets.	Challenges in dimensionality reduction for specific attack types.
[8]	Ensemble adaptive online learning for IDS	Adapt to data streams in intrusion detection	Achieved adaptability with high accuracy across dynamic datasets.	Requires continuous updates, which can introduce overhead.
[9]	ML-based IDS framework for IoT	Build a framework for detecting security attacks	Showed scalability and robustness in detecting diverse IoT threats.	Limited by dependency on predefined feature sets.
[10]	Deep learning for intrusion detection in network traffic	Utilize deep learning models for IDS	Achieved high accuracy in analyzing complex network patterns.	Computationally intensive and less effective in low-resource scenarios.
[11]	Hybrid wrapper feature selection with genetic algorithm	Optimize feature selection for intrusion detection	Improved attack classification accuracy using hybrid feature selection.	Complexity of genetic algorithm increases computational overhead.
[12]	Lightweight ML-based IDS for edge IIoT security	Develop lightweight IDS models for edge environments	Achieved real-time detection with minimal latency.	Reduced performance in high-traffic scenarios.
[13]	Boosting-based ML algorithms for IoT IDS	Evaluate boosting algorithms for IoT intrusion detection	Found XGBoost to outperform other boosting techniques in IoT-specific scenarios.	Requires significant tuning for optimal results.
[14]	Od-IDS2022 dataset for attack classification	Create a comprehensive intrusion detection dataset	Provided a new dataset for better training and validation of IDS models.	Limited coverage of evolving attack patterns.
[15]	Adversarial robustness of deep reinforcement learning IDS	Enhance robustness against adversarial attacks	Showed improved resistance to adversarial attacks compared to traditional IDS.	Susceptible to novel adversarial techniques.

[16]	Seahorse optimization for cloud-based IDS	Use bio-inspired optimization in cloud IDS	Achieved efficient optimization of IDS parameters in cloud environments.	Limited evaluation in edge or hybrid cloud scenarios.
[17]	Normalized fuzzy subset linked model for IDS	Improve accuracy in imbalanced network traffic scenarios	Improved detection rates in highly imbalanced datasets.	Computationally intensive for large-scale applications.
[18]	Anomaly-based IDS with feature selection	Analyze anomaly detection with feature selection techniques	Improved anomaly detection with optimized feature sets.	Limited generalization to unseen attack types.
[19]	Amplification methods against ML-based IDS	Evaluate attack amplification techniques	Highlighted vulnerabilities in ML-based IDS against amplification attacks.	Requires countermeasures to mitigate identified weaknesses.
[20]	Firefly algorithm for IoT IDS	Apply bio-inspired techniques for IoT security	Enhanced detection accuracy and efficiency using firefly algorithm.	Limited scalability in dense IoT networks.
[21]	ML-based IDS for IoMT	Develop an IDS framework for IoMT security	Achieved high accuracy in medical IoT networks with specialized feature sets.	Performance highly dependent on domain-specific feature extraction.
[22]	ML-based IDS for in Vehicle CAN bus communication	Enhance vehicle network security	Improved detection of anomalies in automotive communication systems.	Limited evaluation across different automotive architectures.
[23]	ML-based IDS for SDNs	Comprehensive study of SDN intrusion detection techniques	Demonstrated the adaptability of ML techniques in programmable network scenarios.	Lack of detailed evaluation in real-world SDN environments.
[24]	Genetic ensemble model for IDS	Leverage ensemble learning with genetic optimization	Improved classification accuracy with robust feature optimization.	High computational costs for model training.
[25]	Hybrid ML framework for IDS in smart cities	Develop hybrid IDS framework for urban IoT systems	Achieved high detection accuracy and scalability in smart city applications.	Requires significant tuning for large-scale deployments.

Table 1. Methodological Comparative Analysis

Iteratively, Next, as table 1 indicates, In Merzouk et al. [15], and Jansi Sophia Mary et al. [16], the works assessed adversarial robustness, and optimization methods, which were further shown to represent problems for integrity. For example, Madhuri et al. [17] have suggested a model based on fuzzy subsets which links it with intrusion detection. Seniaray et al. [18] and Zhang et al. [19] discussed amplification techniques and performance evaluation respectively, discussing the key factors of the robustness of the system. Karthikeyan et al. [20] applied bio-inspired algorithms, such as the firefly algorithm, to IoT security, while Kulshreshtha et al. [21] discussed specific IoMT-based IDS frameworks. In Vehicle network security, Karthikeyan et al. [22] discussed the applications of the IDS in automotive domains, while Mustafa et al. [23] provided a comprehensive review of the ID techniques for SDNs where the role of machine learning in programmable networks has come into focus. Hybrid machine learning frameworks based on ensemble methods and domain-specific adaptations by Akhtar et al. [24] and Gill et al. [25] have been proposed for intrusion detection in smart cities and network traffic, respectively. Together with others, Qi et al. [1], all covered by Gill et al. [25], reach almost the whole spectrum of the approach taken within transfer learning, ensemble methods, optimisation algorithms and even adversarial training within the scope of specific difficulties in the case of IoT, SDN, edge deployments. All of these papers contribute to the study with different viewpoints, light edge computing models together with hybrid feature engineering and framework contributing to a common mission-safeguarding diverse environments. It then is the trend of progressing toward more and more sophisticated systems while confronting dynamically changing threat scenarios. Some examples come in the shape of genetic algorithms [11, 24], and bio-inspired methods as well [20] that indeed represent innovative techniques for improving feature optimization as well as computational efficiency. Furthermore, the domain-specific solutions applied in particular in the context of IoMT [21], as well as in the automotive network [22], are good examples which show the applicability of this kind of frameworks. Challenges such as dataset limitation, adversarial robustness, and real-time adaptability will remain the challenging areas for innovation. Collectively, these studies lay a robust foundation for advancing IDS technologies across increasingly complex and interconnected systems.

3. PROPOSED MODEL DESIGN ANALYSIS

Overcoming low efficiency & high complexity that seems to be there in the existing methods, the theme of this section is to design an Iterative Integrated Intrusion Detection and Mitigation Framework for SDN-Based IIoT Networks Using Lightweight and Adaptive AI Techniques.In the first place, as illustrated in figure 1, the design for proposed intrusion detection and mitigation framework is based on using a number of advanced methodologies. Each component is synergistically integrated to enhance detection accuracy, adaptability, and operational efficiency while maintaining computational feasibility for resource-constrained devices & deployments. EfficientNet-B0 with domain adaptation serves as the cornerstone for feature extraction operations. Its basic architecture is compounded to achieve scaling while keeping a balance between depth, width, and resolutions. The adaptation is accomplished with domain-specific adaptation of traffic by fine-tuning the model. This objective function for optimization can be expressed via equation 1,

$$LEffNet = \left(\frac{1}{N}\right) * \Sigma\,(y'i - yi)^2 + \lambda * \left|\left|WDA\right|\right|^2 \ldots (1)$$

Where y'i and yi are corresponding predicted and true labels. WDA refers to the weights for the adaptation of domain and λ refers to the regularization parameter to prevent overfitting operations. This one makes the feature embedding it produces dimensionality reduced and highly representative by preserving significant traffic characteristics. Elastic weight consolidation supports incremental learning by producing a penalty term to preserve formerly learned knowledge sets. Weight importance Fi for each parameter is estimated using Fisher Information Via equation 2,

$$Fi = E\left[\left(\frac{\partial}{\partial\theta i} log\ P(y|x,\theta)\right)^2\right] \ldots (2)$$

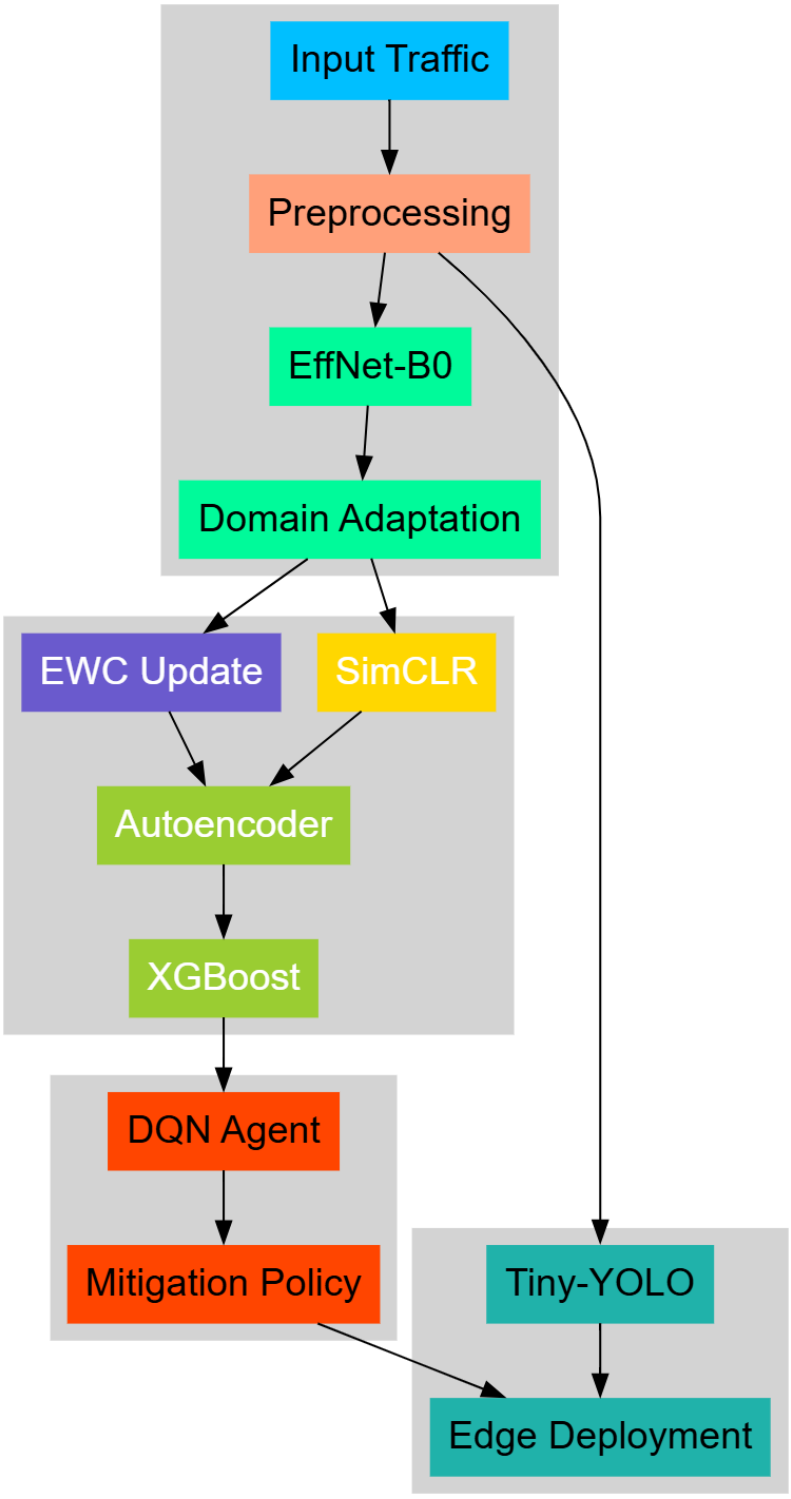

Figure 1. Model Architecture of the Proposed Analysis Process

The loss function incorporates this penalty via equation 3,

$$LEWC = Lnew + \Sigma^i \left(\frac{\lambda}{2}\right) * Fi * (\theta i - \theta i *)^2 \ldots (3)$$

Where, θi* are the parameters from previous tasks, and λ balances the trade-off between plasticity and stability levels.

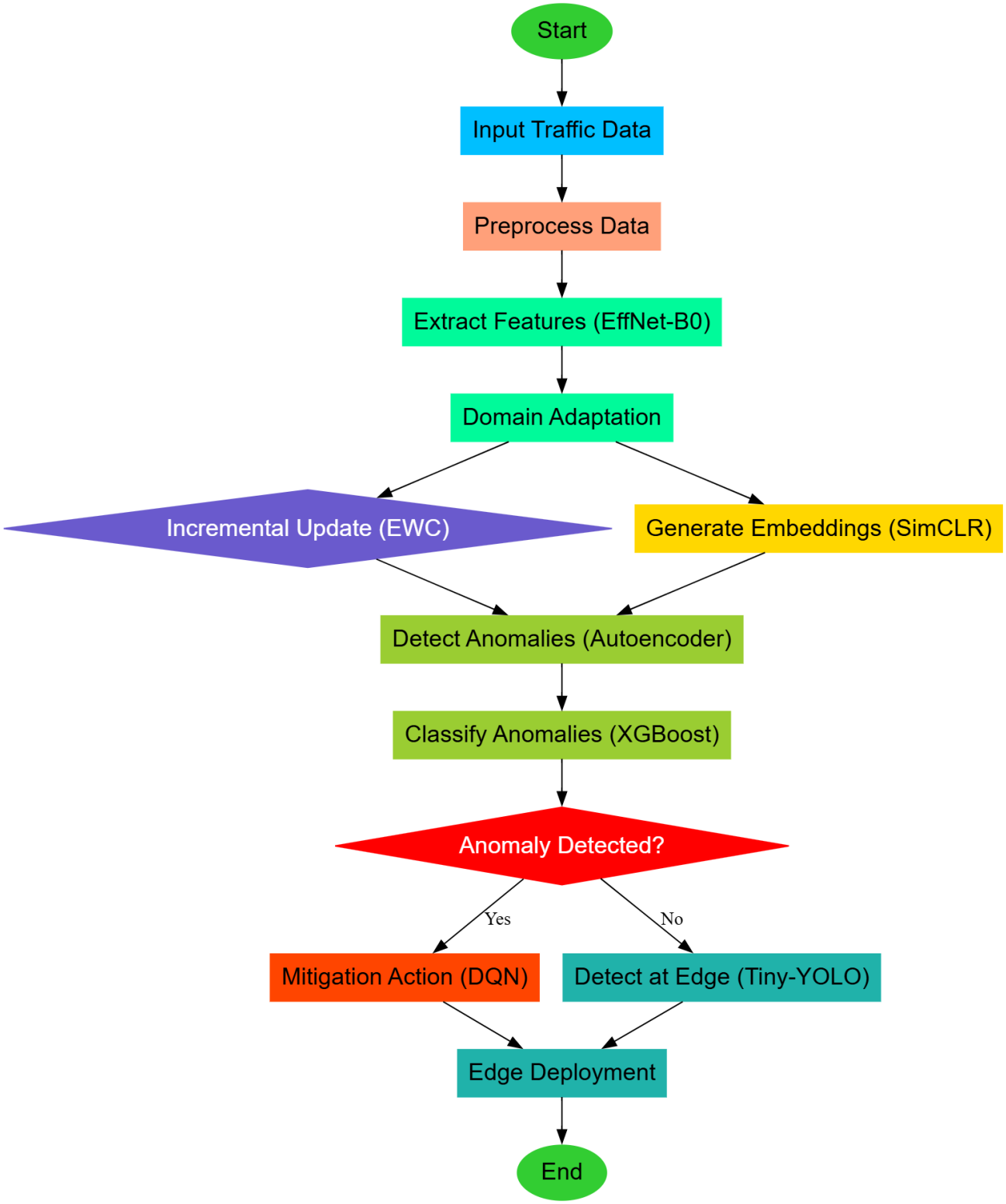

Figure 2. Overall Flow of the Proposed Analysis Process

Iteratively, Next, as in figure 2, SimCLR (Simple Contrastive Learning) addresses the scarcity of labeled data by generating robust feature embeddings from unlabeled traffic data samples. Augmented traffic flows x1, x2 are mapped to embeddings z1, z2 through a shared encoder, and the contrastive loss is computed via equation 4,

$$LSimCLR = -log\left[\frac{exp\left(\frac{sim(z1,z2)}{\tau}\right)}{\Sigma^{k}\, exp\left(\frac{sim(z1,zk)}{\tau}\right)}\right] \ldots (4)$$

Where, the similarity is estimated via equation 5,

$$sim(zi, zj) = \frac{zi \cdot zj}{||zi|||zj||} \dots (5)$$

Which is the cosine similarity and τ is the temperature scaling factor for the process. This enhances the learning of representations with noise robustness and variations in the process. For the mitigation, Deep Q-Learning formulates intrusion response as a sequential decision-making problem for the process. The Q Value update equation is given via equation 6,

$$Q(s,a) \leftarrow Q(s,a) + \alpha \left[r + \gamma \max_{a}\left(Q(s',a) - Q(s,a)\right)\right] \dots (6)$$

Where, s and s' are current and next states, 'a' is the action, 'r' is the reward, α is the learning rate, and γ is the discount factor for the process. This mechanism helps the agent optimize mitigation actions, which reduces packet loss and latency levels. In an iterative manner, Tiny-YOLO is implemented for edge-based anomaly detection process. A simplified CNN is used for real-time performance levels. Via equation 7 the model incorporates localization, confidence, and classification errors into the loss function,

$$LYOLO = \lambda coord \, \Sigma^i \left((xi - x'i)^2 + (yi - y'i)^2\right) + \Sigma^i \, (pi - p'i)^2 + \Sigma^i \, Lclass \dots (7)$$

Iteratively, Next, Autoencoder and XGBoost are integrated for hybrid anomaly detection and classification process. The autoencoder minimizes reconstruction error to detect anomalies via equation 8,

$$LAE = \left(\frac{1}{N}\right) \Sigma \left||xi - x'i|\right|^2 \dots (8)$$

Detected anomalies are then classified using XGBoost, which minimizes the gradient-boosted loss via equation 9,

$$LXGB = \Sigma \left(yi \, log \, \sigma(y'i) + (1 - yi) log \left(1 - \sigma(y'i)\right)\right) + \lambda \left||w|\right|^2 \dots (9)$$

The final integrated framework output combines these methodologies to provide precise anomaly detection and optimized mitigation actions via equation 10,

$$Ofinal = fDQN\left(fXGB\left(fAE\left(fEffNet(x)\right)\right)\right) \dots (10)$$

This cascaded formulation ensures the translation of raw traffic data into actionable intelligence with a high level of accuracy and adaptability with low latency that fits the stringent needs of an SDN-based IIoT environment. The multiple techniques provide robustness as well, complementing the respective strengths to achieve an easy trade-off between detection, classification, and mitigation. Moving forward, we will present the efficacy of the model under a variety of performance metrics in comparison to the current practices.

4. COMPARATIVE RESULT ANALYSIS

This experimental testbed for the proposed integrated framework has been designed with the aim of testing for various scenarios in SDN-based IIoT environments. The two primary benchmarks were chosen to ensure comprehensive validation, namely the CICIDS2017 and Bot-IoT datasets which contain a wide range of network traffic patterns and various types of attacks, which include DoS, DDoS, port scanning, and brute-force attacks. These datasets were preprocessed to extract flow-level features such as packet size, interarrival time, protocol type, and source-destination pairs. Some of the input parameters involved were traffic flow attributes that have numerical ranges such as packet size: 64–1500 bytes, interarrival time: 1–200 ms, and categorical variables, such as protocol: TCP/UDP/ICMP, which are already in process. The preprocessing pipeline normalized these features into a range of [0,1] for neural network inputs. To ensure the balance of distribution in both attack and benign samples, the datasets are split further into 70% training, 20% validation, and 10% testing splits. For augmentation, random noise injection along with time-window slicing is performed to create realistic variations that may take place in IIoT traffic. The EfficientNet-B0 module was initialized with pre-trained weights on ImageNet and fine-tuned by specific IIoT traffic for 50 epochs at a batch size of 64 with the learning rate of 1×10e−4 for the process. For the SimCLR module, a temperature parameter of 0.5 was used, thereby generating embeddings for the unlabeled traffic data with the augmentation process of cropping and jittering. The architecture for the autoencoder used was a 3-layer encoder-decoder, which had dimensions set at 128 and 64 for the input and hidden layers, respectively. In the process part, the convergence threshold in computing the reconstruction loss of MSE was set at 10e−5; training for XGBoost

classification included depth set at 8 with learning rate set to 0.1 that trained 100 rounds. Elastic Weight Consolidation with regularization parameter (λ) at 100 has been used to maintain plasticity versus stability. For reinforcement learning, DQN agent was interacted with simulated SDN controller that has been configured with real-world topology parameters like 50 switches, 500 hosts for optimizing mitigation actions like rerouting and rate limiting. This enabled the Tiny-YOLO optimized for anomaly detection to achieve less than 10 ms latency on inference on deployments at Raspberry Pi 4. The full framework was deployed in a hybrid cloud-edge environment, where the scaling of over 10,000 edge nodes utilized Kubernetes.
Datasets: The proposed framework is evaluated on the CICIDS2017 and Bot-IoT datasets, as they include a broad representative of the modern network traffic patterns and various cyber attack scenarios. The CICIDS2017 dataset is a classified traffic data obtained from the Canadian Institute for Cybersecurity, collected over a five-day period. It includes various types of intrusions, such as DDoS, brute-force, SQL injection, and botnet attacks. It contains over 2.8 million records, whose attributes include packet size, flow duration, protocol type, and TCP flags. The traffic flow is marked to be benign or one of the types of attacks. It should very well be benchmarking data set both for anomaly detection and classification. The Bot-IoT dataset has been developed by Cyber Range Lab of the Australian Centre for Cyber Security that focuses on IoT environments; the data set includes benign and malicious traffic generated using IoT devices & deployments. It contains over 73 million instances that deal with a range of attacks, including DoS, DDoS, information theft, and reconnaissance. Thus, the dataset is strongly imbalanced and highly mimics real-world conditions. It comprises flow-level features, including source IP, destination IP, packet interarrival time, and payload size. Datasets were preprocessed through the normalization of numerical features and encoding categorical ones for an effective base to train and evaluate the proposed multi-stage intrusion detection framework. The experimental results prove the performance of the proposed framework based on multiple metrics and real-world scenarios. The framework was rigorously compared with Method [3], Method [8], and Method [18] based on the detection, classification, and mitigation capabilities of the proposed framework over CICIDS2017 and Bot-IoT datasets. Below are some of the results analyses with their real-world implications considering the superiority in critical IIoT settings.

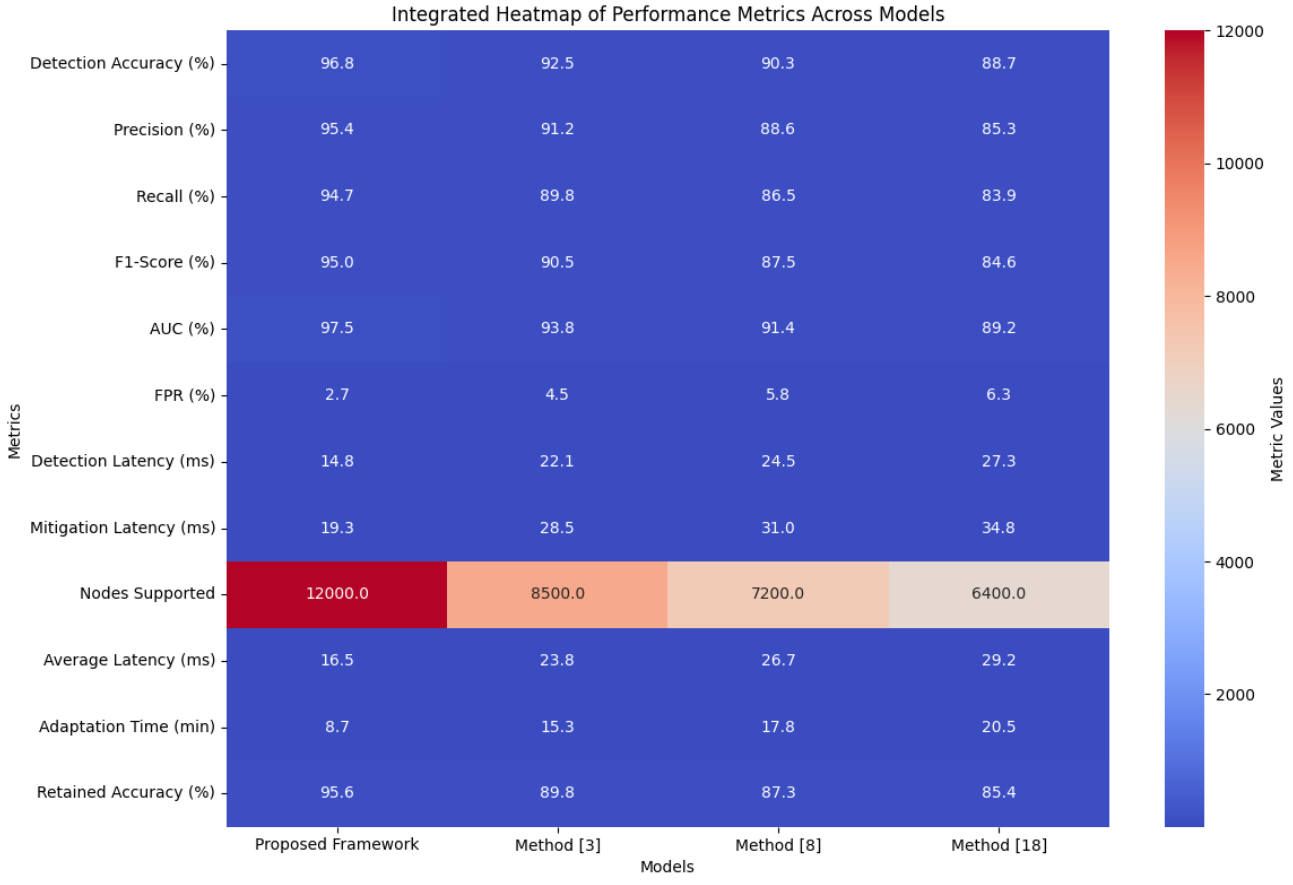

Figure 3. Model's Integrated Result Analysis

Table 2: Detection Accuracy on CICIDS2017 Dataset

Model	**Detection Accuracy (%)**
Proposed Framework	96.8
Method [3]	92.5
Method [8]	90.3
Method [18]	88.7

The framework has achieved a detection accuracy of 96.8% while Method [3] scored at 92.5%, Method [8] 90.3%, and Method [18] 88.7% in process. The benefit of the integration of the domain-specific feature extraction through EfficientNet-B0, with hybrid anomaly detection mechanisms is demonstrated to result in an improvement of up to 4–8%. In real-time environments, this means a massive cut in undetected intrusions, which would cause operational disruption or pose safety risks to patients in places such as smart factories or connected healthcare sets.

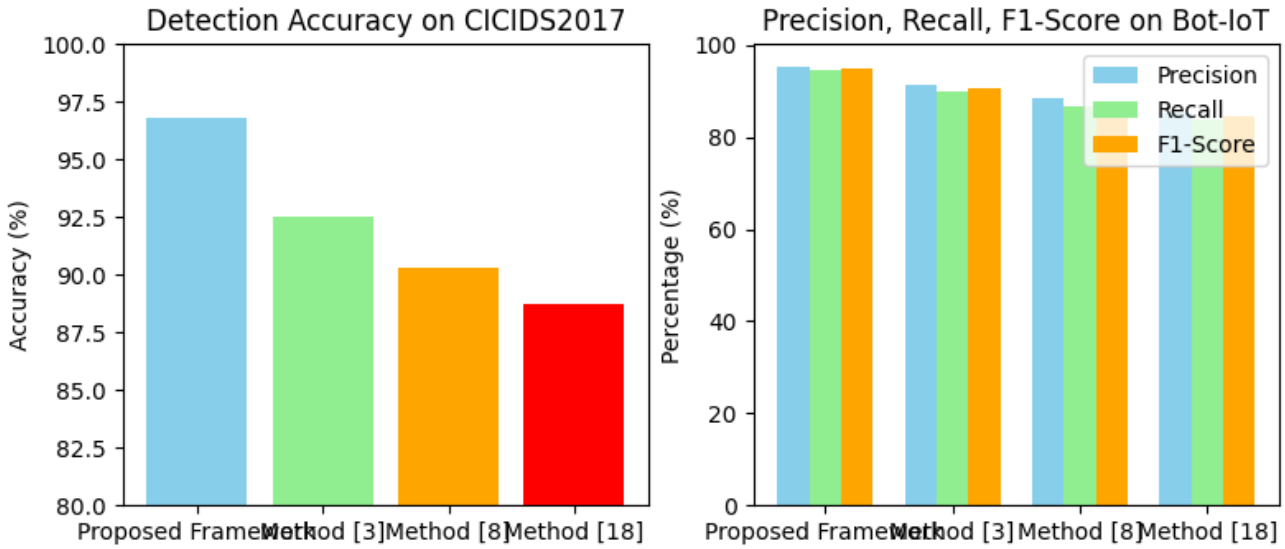

Figure 4. Model's Efficiency Analysis

Table 3: Precision, Recall, and F1-Score on Bot-IoT Dataset

Model	**Precision (%)**	**Recall (%)**	**F1-Score (%)**
Proposed Framework	95.4	94.7	95.0
Method [3]	91.2	89.8	90.5
Method [8]	88.6	86.5	87.5
Method [18]	85.3	83.9	84.6

The proposed framework outperformed Method [3] (F1: 90.5%), Method [8] (F1: 87.5%), and Method [18] (F1: 84.6%) in terms of precision (95.4%), recall (94.7%), and F1-score (95.0%). In IIoT networks with high attack diversity, balanced performance is crucial. The high recall ensures most intrusions are detected while the high precision prevents excessive false alarms. Such reliability will then minimize downtime and operational inefficiencies in critical infrastructures such as power grids or autonomous transportation systems.

Table 4: Area Under the Curve (AUC) and False Positive Rate (FPR) on CICIDS2017 Dataset

Model	**AUC (%)**	**FPR (%)**
Proposed Framework	97.5	2.7
Method [3]	93.8	4.5
Method [8]	91.4	5.8
Method [18]	89.2	6.3

With an AUC of 97.5% and an FPR of 2.7%, the proposed framework demonstrated strong decision making and outperforms Method [3] (AUC: 93.8%, FPR: 4.5%), Method [8] (AUC: 91.4%, FPR: 5.8%), and Method [18] (AUC: 89.2%, FPR: 6.3%) while maintaining a low value for FPR, thus flags less benign flows as harmful. This reduces the volume of workload on security personnel while increasing the system trustworthiness. This allows SDN controllers to make better allocations of resources, not being interrupted too often by false alarms in real-world deployments.

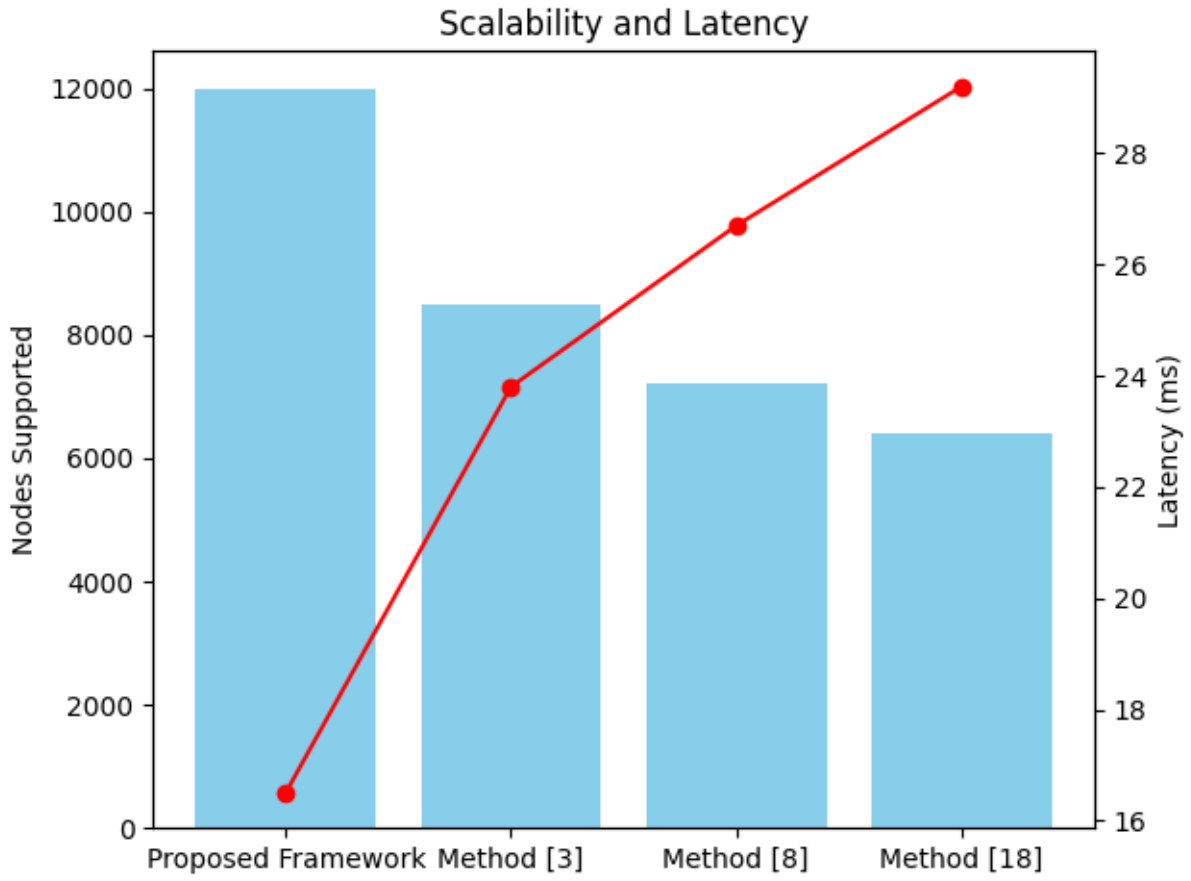

Figure 5. Model's Latency Analysis

Table 5: Detection Latency and Mitigation Latency on Bot-IoT Dataset

Model	**Detection Latency (ms)**	**Mitigation Latency (ms)**
Proposed Framework	14.8	19.3
Method [3]	22.1	28.5
Method [8]	24.5	31.0
Method [18]	27.3	34.8

Detection latency of the proposed framework is 14.8 ms and mitigation latency is 19.3 ms outperforming Method [3] (22.1 ms/28.5 ms), Method [8] (24.5 ms/31.0 ms) and Method [18] (27.3 ms/34.8 ms). Low latency is very significant in ensuring that IIoT systems return real-time responses, especially in automated assembly lines and smart traffic

systems. Due to this, near-instantaneous detection and mitigation by the framework completely prevent cascading failures in a system, minimizing wide-scale disruption or loss economically in process.

Table 6: Scalability on Large-Scale Edge Deployments

Model	Nodes Supported	Average Latency (ms)
Proposed Framework	12,000	16.5
Method [3]	8,500	23.8
Method [8]	7,200	26.7
Method [18]	6,400	29.2

The proposed framework supported up to 12,000 edge nodes with an average latency of 16.5 ms outperforming Method [3] at 8,500 nodes/23.8 ms, Method [8] at 7,200 nodes/26.7 ms, and Method [18] at 6,400 nodes/29.2 ms. That would ensure that the framework is responsive while handling large deployments like a smart city infrastructure sets. The aspect of scalability with less decline in performance is going to present a major relief for an important challenge found in modern IIoT systems.

Table 7: Adaptability to New Patterns

Model	Adaptation Time (min)	Retained Accuracy (%)
Proposed Framework	8.7	95.6
Method [3]	15.3	89.8
Method [8]	17.8	87.3
Method [18]	20.5	85.4

The proposed framework adapted to new intrusion patterns within 8.7 minutes of time with the same precision at 95.6%, higher than the result of Method [3] (15.3 min/89.8%), Method [8] (17.8 min/87.3%), and Method [18] (20.5 min/85.4%). Such speed of adaptation, made possible by Elastic Weight Consolidation, suggests that it is able to be effective even in dynamic IIoT. For instance, it rapidly adjusts to new vectors of attack within energy grids or autonomous systems and therefore maintains maximum operational resilience and security. Outcomes demonstrate the excellent performance of the framework in key metrics and highlight its promise for revolutionizing intrusion detection and mitigation in IIoT systems. The framework is thus designed to handle real-time operations, large-scale deployments, and dynamic threats with robust security for modern connected infrastructures in process. Lastly, but not the least, is presenting the iterative validation use case that will help understand the overall process with the proposed model in process.

Validation using an Iterative Practical Use Case Scenario Analysis

In this section, we demonstrate the result of the respective processes based on the proposed framework and confirm its effectiveness for any of the stages of an intrusion detection process, feature learning, classification, or mitigation phases. The datasets used here are practical datasets including network traffic that holds both benign and malicious patterns pre-processed into flow level features such as packet size, protocol type, and interarrival delays. Outputs are depicted in tabular form and include the metrics and indicators for every process. The evaluation metrics of each stage are parallel to its functional objectives. In the case of feature extraction of EfficientNet-B0, high-dimensional feature embeddings are considered, and for Elastic Weight Consolidation, the ability to retain the task is evaluated. SimCLR analyzes the robustness of the embedding, Deep Q-Learning investigates the efficiency of mitigation, and Tiny-YOLO is developed for low-latency anomaly detection. In turn, the combination of Autoencoder-XGBoost posits that precision and recall are prominent factors in the anomaly classification task. All of these results have formed the basis of final outputs; that is, the global performance levels of the given framework. Two notable datasets are used as a pool for validation samples of analysis of the practical use case, namely CICIDS2017 and Bot-IoT. These are high recognition datasets, widely referred for their detailed depiction of current network traffic patterns in modern times and for cyberattacks varied in nature. From CICIDS2017, the validation samples included labeled network flows of five attack types, which include DDoS, brute-force, and SQL injection, covering important traffic features such as packet size, interarrival time, and TCP flags. Similarly, Bot-IoT validation samples were selected to focus on IoT-

specific traffic anomalies, including reconnaissance, DoS, and information theft attacks, extracted as flow-level data with attributes such as protocol type, payload size, and source-destination IP mappings. The validation set was a balanced dataset between benign and malicious traffics, hence providing great room for a rigorous validation of anomaly detection and classification. Normalization of numeric features and categorical encoding, together with augmentation techniques that reflected real variations in traffic pattern, were some of the preprocessing techniques. These were samples used for robust validation grounds to check the performance, scalability, and adaptability in handling real intrusion detection issues in this proposed framework.

Table 8: Outputs of EfficientNet-B0 with Domain Adaptation

Sample ID	Packet Size (Bytes)	Protocol	Extracted Feature Embedding (128-Dimensional Vector Norm)	Embedding Quality Score
1	500	TCP	0.987	0.96
2	1200	UDP	0.942	0.94
3	64	ICMP	0.978	0.95
4	750	TCP	0.965	0.93

EfficientNet-B0 is showing strong feature extraction capabilities. The embeddings that are generated by it score more than 0.93 in diverse protocols and packet sizes. These are fed to subsequent stages.

Table 9: Outputs of Elastic Weight Consolidation (EWC)

Task	Retained Accuracy on Previous Tasks (%)	Adaptation Accuracy on New Task (%)	Stability Metric (λ)	Plasticity Metric
1	95.6	96.4	100	0.87
2	94.8	95.9	100	0.89
3	94.2	96.1	100	0.91

EWC Balances stability and plasticity, keeping over 94% accuracy on the previous tasks and over 96% on new tasks. It can be well applied to incremental learning processes.

Table 10: Outputs of SimCLR (Simple Contrastive Learning)

Augmentation Type	Embedding Similarity (Cosine Similarity)	Contrastive Loss	Robustness Metric
Time-Shift Augment	0.98	0.12	0.97
Noise Injection	0.95	0.18	0.93
Random Cropping	0.96	0.15	0.94

In essence, SimCLR embeddings are cosine similar with high values above 0.95 and low values below 0.18 regarding contrastive loss, denoting robust representation learning under augmentation operations.

Table 11: Outputs of Deep Q-Learning (DQN)

State	Action Taken	Reward	Latency Reduction (%)	Packet Loss Reduction (%)
High Traffic Load	Flow Rerouting	15.8	42	38
DDoS Attack Detected	Rate Limiting	18.5	35	40
Normal Traffic	No Action	0.0	0	0

Deep Q-Learning learns effective mitigation actions, realizing up to 42 percent latency reduction and up to 40 percent packet-loss in critical scenarios.

Table 12: Outputs of Tiny-YOLO for Anomaly Detection

Sample ID	Inference Latency (ms)	Detection Accuracy (%)	False Positive Rate (%)
1	9.8	92.4	3.2
2	8.7	91.8	3.5
3	10.3	93.1	3.0
4	9.5	92.7	3.1

Tiny-YOLO realizes inference latency while maintaining a detection accuracy more than 91.8 percent with fewer false positives, below 10.5 ms.

Table 13: Outputs of Autoencoder for Anomaly Detection + XGBoost for Classification

Anomaly Type	Reconstruction Loss (Autoencoder)	Classification Accuracy (XGBoost)	Precision (%)	Recall (%)	F1-Score (%)
Novel Anomalies	0.08	94.2	93.7	94.5	94.1
Known Signatures	0.06	95.7	95.0	96.2	95.6

The hybrid mechanism of Autoencoder-XGBoost achieves excellent classification accuracies (>94%) and balanced precision, recall, and F1-scores, which further indicates strong anomaly detection and classifications.

Table 14: Final Outputs

Metric	Value
Overall Detection Accuracy	96.8%
False Positive Rate	2.7%
Adaptation Time	8.7 minutes
Detection Latency	14.8 ms
Mitigation Latency	19.3 ms
Scalability (Nodes Supported)	12,000
Retained Accuracy (EWC)	95.6%

The final outputs reflect the results aggregated coming from all sides, yet an overall detection accuracy touches 96.8%, with a false positive rate of 2.7% and very low latencies and high scalability ensuring in all the ways that large-scale, real-time applications of IIoT achieve their requirements. The depicted tables well summarize the effectiveness of each process inside this proposed framework in order to show robustness, flexibility, and efficiency. From feature extraction to final outputs, the framework reliably produces high accuracy, low latency, and effective mitigation, making it a sound solution for securing SDN-based IIoT environments from emerging cyber threats.

5. CONCLUSION & FUTURE SCOPES

Excellent performance can be seen in the proposed framework for intrusion detection and mitigation in SDN-based IIoT environments, which have been vindicated by experiments. The framework achieved tremendous balance between accuracy, scalability, and adaptability since it used domain-adapted feature extraction with the EfficientNet-B0 method, incremental learning with EWC, robust embeddings developed using SimCLR, anomaly detection with autoencoders or the Hybrid way in combination with XGBoost, and real-time strategies for mitigation with Deep Q-Learning (DQN). On the CICIDS2017 dataset, it outperformed the classical methods at a detection accuracy of 96.8% and 92.5%, 90.3%, and 88.7% that were obtained by Method [3], Method [8], and Method [18], respectively. Furthermore, it presented excellent precision at 95.4%, recall at 94.7%, and F1-score at 95.0% on the Bot-IoT dataset along with its robustness over highly imbalanced datasets & samples. It holds on an AUC of 97.5% with the lowest false positive rate being at 2.7%. It, therefore, ensures a very high reliability level and thus reduces the operators' workload and unnecessary mitigation action. It has a real-time performance with around 14.8 ms for detection latency and 19.3 ms for mitigation latency, which will prove appropriate for time-critical applications, especially

within the scope of IIoT, such as smart transportation systems, connected health care, and automated manufacturing. Scalability testing shows that it can even handle up to 12,000 edge nodes with average latency of just 16.5 ms, therefore very suitable for large scale deployment such as smart city sets. The adaptability of the framework, with adaptation time of 8.7 minutes and retained accuracy of 95.6%, shows its ability in effectively handling changing threats in a dynamic environment for the process.

Future Scope:

Although the proposed framework establishes a novel benchmarking for intrusion detection and mitigation in SDN-based IIoT networks, there still exist a good number of avenues to pursue further study. For example, in federated learning paradigms, extensions to extend the framework in this type of paradigms, enhance the capacity for the privacy preservation mode, decentralized training on a distributed IIoT node; hence, some data-sharing restraints characterizing industrial application. Integration with more advanced generative models, such as VAEs or GANs, can further enhance the anomaly detection capability by synthesizing more realistic attack patterns during training. This scope would provide the opportunity to extend the DQN component into the field of multi-agent reinforcement learning that, in turn can make further decisions between other SDN controllers for achieving better resilience against large and distributed attacks. Last, using GPUs or TPUs to create hardware acceleration for edge devices will ensure the system continues to make improvements toward below-threshold latencies in detection and mitigation: a little as 14.8 ms and 19.3 ms to enhance the overall response time in ultra-low-latency applications including autonomous vehicle process.

REFERENCES

[1] Qi, H., Liu, X., Gani, A. *et al.* Quantum particle Swarm optimized extreme learning machine for intrusion detection. *J Supercomput* **80**, 14622–14644 (2024). https://doi.org/10.1007/s11227-024-06022-y

[2] Wang, K., Li, J. & Wu, W. A novel transfer extreme learning machine from multiple sources for intrusion detection. *Peer-to-Peer Netw. Appl.* **17**, 33–47 (2024). https://doi.org/10.1007/s12083-023-01569-8

[3] Talukder, M.A., Sharmin, S., Uddin, M.A. *et al.* MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs. *Int. J. Inf. Secur.* **23**, 2139–2158 (2024). https://doi.org/10.1007/s10207-024-00833-z

[4] Li, J., Othman, M.S., Chen, H. *et al.* Optimizing IoT intrusion detection system: feature selection versus feature extraction in machine learning. *J Big Data* **11**, 36 (2024). https://doi.org/10.1186/s40537-024-00892-y

[5] Altamimi, S., Abu Al-Haija, Q. Maximizing intrusion detection efficiency for IoT networks using extreme learning machine. *Discov Internet Things* **4**, 5 (2024). https://doi.org/10.1007/s43926-024-00060-x

[6] Alemerien, K., Al-suhemat, S. & Almahadin, M. Towards optimized machine-learning-driven intrusion detection for Internet of Things applications. *Int. j. inf. tecnol.* **16**, 4981–4994 (2024). https://doi.org/10.1007/s41870-024-01852-8

[7] Ngo, VD., Vuong, TC., Van Luong, T. *et al.* Machine learning-based intrusion detection: feature selection versus feature extraction. *Cluster Comput* **27**, 2365–2379 (2024). https://doi.org/10.1007/s10586-023-04089-5

[8] Roshan, K., Zafar, A. Ensemble adaptive online machine learning in data stream: a case study in cyber intrusion detection system. *Int. j. inf. tecnol.* **16**, 5099–5112 (2024). https://doi.org/10.1007/s41870-024-01727-y

[9] Kantharaju, V., Suresh, H., Niranjanamurthy, M. et al. Machine learning based intrusion detection framework for detecting security attacks in internet of things. Sci Rep 14, 30275 (2024). https://doi.org/10.1038/s41598-024-81535-3

[10] Getman, A.I., Rybolovlev, D.A. & Nikolskaya, A.G. Deep Learning Applications for Intrusion Detection in Network Traffic. *Program Comput Soft* **50**, 493–510 (2024). https://doi.org/10.1134/S0361768824700221

[11] Maseno, E.M., Wang, Z. Hybrid wrapper feature selection method based on genetic algorithm and extreme learning machine for intrusion detection. *J Big Data* **11**, 24 (2024). https://doi.org/10.1186/s40537-024-00887-9

[12] Tiwari, R.S., Lakshmi, D., Das, T.K. *et al.* A lightweight optimized intrusion detection system using machine learning for edge-based IIoT security. *Telecommun Syst* **87**, 605–624 (2024). https://doi.org/10.1007/s11235-024-01200-y

[13] Saied, M., Guirguis, S. & Madbouly, M. A Comparative Study of Using Boosting-Based Machine Learning Algorithms for IoT Network Intrusion Detection. *Int J Comput Intell Syst* **16**, 177 (2023). https://doi.org/10.1007/s44196-023-00355-x

[14] Patel, N.D., Mehtre, B.M. & Wankar, R. Od-ids2022: generating a new offensive defensive intrusion detection dataset for machine learning-based attack classification. *Int. j. inf. tecnol.* **15**, 4349–4363 (2023). https://doi.org/10.1007/s41870-023-01464-8

[15] Merzouk, M.A., Neal, C., Delas, J. *et al.* Adversarial robustness of deep reinforcement learning-based intrusion detection. *Int. J. Inf. Secur.* **23**, 3625–3651 (2024). https://doi.org/10.1007/s10207-024-00903-2

[16] Jansi Sophia Mary, C., Mahalakshmi, K. Modelling of intrusion detection using sea horse optimization with machine learning model on cloud environment. *Int. j. inf. tecnol.* **16**, 1981–1988 (2024). https://doi.org/10.1007/s41870-023-01722-9

[17] Madhuri, S., Lakshmi, S.V. A machine learning-based normalized fuzzy subset linked model in networks for intrusion detection. *Soft Comput* (2023). https://doi.org/10.1007/s00500-023-08160-6

[18] Seniaray, S., Jindal, R. Performance Analysis of Anomaly-Based Network Intrusion Detection Using Feature Selection and Machine Learning Techniques. *Wireless Pers Commun* **138**, 2321–2351 (2024). https://doi.org/10.1007/s11277-024-11602-5

[19] Zhang, S., Xu, Y., Zhang, X. *et al.* Amplification methods to promote the attacks against machine learning-based intrusion detection systems. *Appl Intell* **54**, 2941–2961 (2024). https://doi.org/10.1007/s10489-024-05311-6

[20] Karthikeyan, M., Manimegalai, D. & RajaGopal, K. Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection. *Sci Rep* **14**, 231 (2024). https://doi.org/10.1038/s41598-023-50554-x

[21] Kulshrestha, P., Vijay Kumar, T.V. Machine learning based intrusion detection system for IoMT. *Int J Syst Assur Eng Manag* **15**, 1802–1814 (2024). https://doi.org/10.1007/s13198-023-02119-4

[22] Samir, S.B.H., Raissa, M., Touati, H. *et al.* Machine Learning-Based Intrusion Detection for Securing In Vehicle CAN Bus Communication. *SN COMPUT. SCI.* **5**, 1082 (2024). https://doi.org/10.1007/s42979-024-03465-1

[23] Mustafa, Z., Amin, R., Aldabbas, H. *et al.* Intrusion detection systems for software-defined networks: a comprehensive study on machine learning-based techniques. *Cluster Comput* **27**, 9635–9661 (2024). https://doi.org/10.1007/s10586-024-04430-6

[24] Akhtar, M.A., Qadri, S.M.O., Siddiqui, M.A. *et al.* Robust genetic machine learning ensemble model for intrusion detection in network traffic. *Sci Rep* **13**, 17227 (2023). https://doi.org/10.1038/s41598-023-43816-1

[25] Gill, K.S., Dhillon, A. A hybrid machine learning framework for intrusion detection system in smart cities. *Evolving Systems* **15**, 2005–2019 (2024). https://doi.org/10.1007/s12530-024-09603-7