Journal of Engineering and Technology for Industrial Applications

ITEGAM-JETIA

Manaus, v.12 n.57, p. 1132-1147. January/February, 2026.
DOI: https://doi.org/10.5935/jetia. v12i57.3290

ISSN ONLINE: 2447-0228

RESEARCH ARTICLE OPEN ACCESS

SECURE AND INTELLIGENT SDN ROUTING AND ANOMALY DETECTION USING XG-BOOST FOR REAL-TIME IOT TRAFFIC OPTIMIZATION

Sohaib R. Awad[1], Qutaiba I. Ali[2] and Amar I. Daood*[3]

[1]Computer and Information Engineering Department, Ninevah University, Mosul, Iraq
[2]Mechatronics Engineering Department, College of Engineering, University of Mosul, Mosul, Iraq
[3]Computer Engineering Department, College of Engineering, University of Mosul, Mosul, Iraq

[1]https://orcid.org/0000-0002-8714-9574, [2]https://orcid.org/0000-0002-0640-0561, [3]https://orcid.org/0000-0002-6841-5259

Email: sohaib.awad@uoninevah.edu.iq, qutaibaali@uomosul.edu.iq, *amar.daood@uomosul.edu.iq

ARTICLE INFO

Article History
Received: January 12, 2025
Revised: January 20, 2026
Accepted: January 30, 2026
Published: February 28, 2026

Keywords:
Software-Defined Networking SDN,
Internet of Things IoT,
Machine Learning ML,
intelligent routing, anomaly detection,
XG-Boost,
Light-GBM,
real-time traffic optimization,
network security,
traffic engineering.

ABSTRACT

The fast growth of the Internet of Things IoT technology generates extraordinary stress on network systems because it requires improved traffic performance and strengthened security measures. The central control capabilities of Software-Defined Networking (SDN) receive limited intelligence from conventional controllers when dealing with evolving network conditions and security threats. This study designs a protected and knowledgeable SDN routing framework for IoT traffic real-time optimization by integrating machine learning algorithms for path optimization and anomaly detection. The proposed method embeds two predictive models within the SDN controller: Light Gradient Boosting Machine (Light-GBM) for performance-aware routing optimization, and XG-Boost for real-time detection of malicious or anomalous flows. The system uses a hybrid decision-making pipeline for Quality of Service QoS measurement elements, such as latency, congestion level, and bandwidth utilization, together with security feedback like threat scores, blacklist status, and intrusion detection alerts. The system was tested by the research team using a simulated network infrastructure that emulates the common pattern of IoT traffic. The designed competitive metrics were latency, throughput, packet loss rate, accuracy of anomaly detection, false positive rate, and controller decision latency. Experimental findings suggest that the suggested SDN controller solution has a higher throughput and faster operations, with a difference to a baseline controller system of 42.7 and 49.7, respectively, and a 75.9% lower packet loss. The XG-Boost model gave an accurate detection rate of 99.8 percent with a false positive rate of 0.2 percent, with a controller decision time of 23.7 ms, which is compatible with real-time operations. Experimental evidence shows that the introduction of machine learning into SDN controller systems increases security operations in IoT and network routing implementation. This system demonstrates scalability together with modularity for direct implementation in operational SDN platforms, including POX and Ryu. The upcoming research will focus on implementing live network traffic while adapting models in real-time and deploying them in production IoT infrastructures.

I. INTRODUCTION

As the Internet of Things grows exponentially, IoT device numbers force network managers to find more efficient methods that guarantee security [1-5]. Because traditional network architectures fail to handle IoT dynamic requirements, SDN has emerged to be the adopted solution [6-9]. SDN splits the control and data planes into separate entities through central control and programmatic capabilities needed for handling IoT networks' complex requirements and growth scale [10], [11]. Leadership processes within SDN require adjustment to incorporate machine learning ML techniques into SDN controllers [12], [13].

Lately, machine learning algorithms have shown impressive results on different types of applications [14], [15]. The integration of ML techniques must include three critical requirements: real-time processing ability, data management of large quantities, and model adaptability to changing network situations [16-18]. SDN security frameworks demonstrate weaknesses in their ability to provide thorough combined solutions for routing optimization as well as anomaly detection, since these capabilities exist in isolation, resulting in security risks [19], [20]. A new SDN framework merges ML models for both intelligent routing operations and a real-time anomaly detection system [21], [22]. XG-Boost is used in the system to identify abnormal traffic behavior, while Light-GBM assists with routing decision predictions. The integration results in a system that enhances network functionality in terms of both performance and security qualities of IoT infrastructure. Our key contributions are:

1. The development of an ML-Enhanced SDN Framework combines Light-GBM and XG-Boost models into the SDN control plane through a framework to execute optimized routing and anomaly detection functions.
2. The framework operates in real time to handle network data during dynamic IoT traffic situations, thus guaranteeing prompt responses.
3. Our assessment of the framework's performance utilizes extensive simulation results to evaluate it through latency measurements, throughput attainment, packet loss avoidance, detection precision measurements, and false positives rates evaluation.
4. The proposed solution has been purposefully designed to expand according to increasing network requirements and handle traffic pattern adjustments, which guarantees sustained efficiency.

The next sections of this paper are divided into the following: Section 2 analyzes the existing literature about integrating SDN and ML technologies. The methods and materials that construct our framework are detailed in the third section. The fourth section of this paper presents both experimental results and accompanying analysis. Section 5 analyzes the results against existing research. Finally, section 6 concludes the paper and outlines the future research directions.

II. LITERATURE REVIEW

SDN development has created powerful changes in network management by promoting scalability while improving security features for IoT environments [23], [24]. Research investigations now explore how ML methods function inside SDN controllers for boosted traffic optimization as well as threat protection methods [25], [26]. The researchers presented in [27] a fast threat recognition system for 5G SDN platforms that uses a PSO-GRUGAN hybrid model as its core methodology. The detection system improved performance but restricted its application to 5G networks exclusively, with minimal capability for IoT-based SDN framework analysis. The study by [28] performed an extensive review of SDN security tools, including traditional and ML as well as blockchain-based approaches, yet did not supply experimental evidence for their investigated techniques. In turn [29] analyzed the existing SDN controller landscape for enhancing IoT security and determined centralized SDN approaches to be the most vital architecture.

The authors failed to develop practical deployment frameworks using their theoretical approach. By [30] demonstrated how machine learning techniques enhance SDN traffic classification results, while this research did not integrate anomaly defense or routing performance improvements into the process. The work of [31] created efficient routing through the implementation of deep reinforcement learning for dynamic SDN traffic routing. The evaluated routing performance of the solution improved, but security measures related to anomaly detection and path trustworthiness evaluation remained a weakness. In the same approach, the research team at [32] created a deep learning hybrid system to find abnormal traffic patterns in SDN networks, which brought better detection capabilities yet added excessive complexity that exceeds IoT lightweight needs. The advanced IS2N, an intent-driven SDN security system, becomes the next SDN generation security system according to [33], who implemented blockchain capabilities into it.

The system strengthened trust mechanisms and enabled auditing functions, although it encountered difficulties that affected its scalability in IoT deployments at scale. A cross-domain intelligent routing method for SDN based on multi-agent reinforcement learning was developed by. [34] to improve network throughput at the same time it reduced latency. The deployment capabilities of their multiple agents in constrained IoT networks are restricted by excessive coordination complexity. Anomaly detection for SDN-driven micro service systems using Graph Neural Networks (GNNs) resulted in providers that detected threats at the service-level, according to [35]. The improved processing requirements of GNNs generate challenges regarding their practical use in real-time situations. By [36] researched DDoS threats in SDN networks by investigating attack patterns and defense methods. Yet, they presented minimal practical frameworks and materials for ML-based and deep learning opposition techniques.

All surveyed studies presented three main disadvantages: multiple optimization strategies and security approaches cannot operate concurrently, complex computations are inappropriate for real-time IoT networks, and the security systems are separate from the network management process. In light of these challenges, this research has advanced this field, but there is still a requirement for SDN frameworks that deliver real-time security intelligence alongside performance optimization capabilities. The proposed work develops a new SDN framework that implements Light-GBM routing optimization and XG-Boost anomaly detection through direct implementation in the controller decision pipeline. The proposed system seeks to manage IoT traffic intelligently throughout three essential aspects, including traffic management, security standards maintenance, and real-time operation. A detailed description of materials and methods relating to the proposed solution appears in the next section.

III.METHODS AND MATERIALS

The research establishes an intelligent methodology to improve SDN routing effectiveness and safety, specifically for IoT platforms. The proposed system implements two connected machine learning pipelines through which it optimizes routing performance and detects security threats in real-time. The methodology starts by developing synthetic data, which comprises 10,000 samples that model traffic sessions through SDN switches. The collected dataset includes quantitative network performance information (latency, throughput, packet loss, hop count etc.) and security measures (IDS presence and numbers of security incidents and blacklist scores).

Feature engineering techniques generate three new metrics, namely, efficiency score, loss rate, and threat score, to improve the predictions by quantifying traffic flow risks. The dataset includes two labels per data point: congestion label and anomaly label, which are derived from heuristic evaluation criteria. The rare yet critical conditions within class imbalance are treated using the Synthetic Minority Over-Sampling Technique (SMOTE). The application trains two classifiers using Light-GBM for routing decisions involving threat risk assessment and XG-Boost for detecting network anomalies. All generated outputs are exported after analysis ends for use in ongoing studies and reproducibility needs. Figure 1 illustrates the methodology overview step by step.

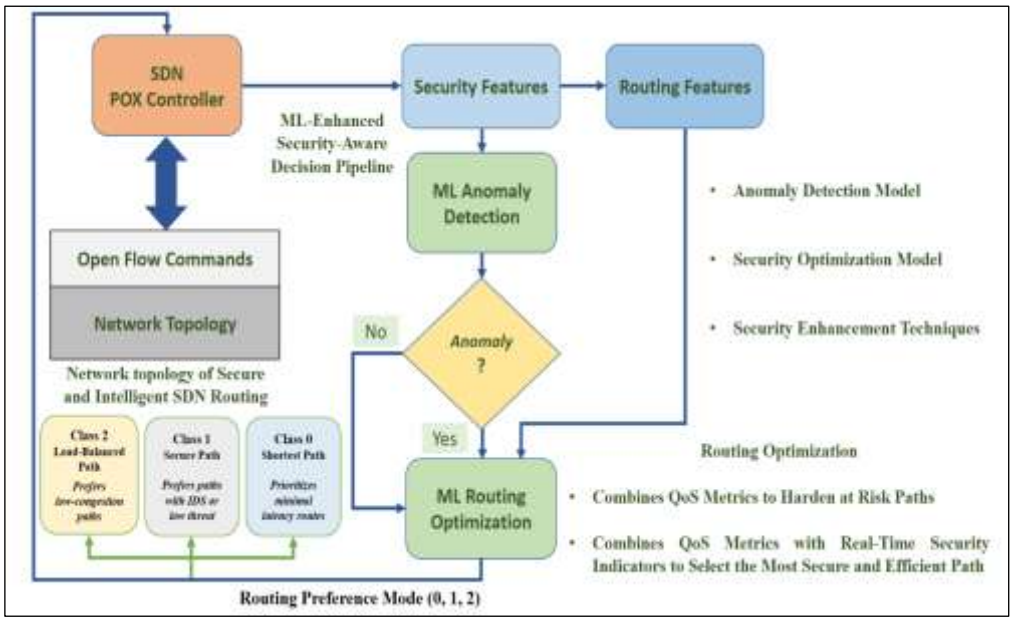


Figure 1: Methodology Diagram.
Source: Authors, (2026).

III.1 NETWORK TOPOLOGY DESCRIPTION

The hierarchy of the designed Software-Defined Networking (SDN) architecture features a single centralized control element connected to 5 network switches and 20 end-host devices. This design depicts an IoT environment built with scalable SDN modules. The SDN controller positioned at the top layer of the network functions as the intelligence hub by viewing all network infrastructure elements while performing dynamic management of real-time forwarding actions, security rules, and routing adjustment. A single point of connection between the five switches enables the SDN controller to control the entire data plane through a flat control layer. The SDN controller, as shown in Figure 2, operates each one of the five switches (S1 to S5) through direct connection. The switches are simply forwarding points that transmit data packets through the controller to the end devices connected to it.

The data plane is composed of 20 hosts, H1 to H20, that are evenly distributed among the five switches at four hosts each. The centralized location of the switches allows for an equal flow of data to be relayed between connected devices and also to distribute the various IoT devices within the network to simulate real-world scenarios. It involves having independent layers in its network design, which helps in the enhancement of routing performance, monitoring, and detecting anomalous events. The layout structure enables the SDN controller to run the XG-Boost and Light-GBM machine learning model that can be used to optimize traffic in real time and fine-grained control. This is made possible by the smart status of the controller implementation of the research.

III.2 DATASET GENERATION

The design and testing of the smart SDN controller needed to use synthetic data to model a variety of network traffic and security events common to software-defined IoT networks. The simulated data is filled with network traffic of normal and malicious nature, so it can offer both appropriate training data to two distinct models, one focused on the optimal route optimization, and the other on the identification of the abnormal patterns. Each record of the data set represents distinctive flow entries with performance attributes, congestion indicators, and security risk measurement points. In the data generation, synthetic processes enable the various flow properties, such as packet rate, throughput, path delay, and jitter, to be variables when modelling the traffic of IoT devices in various load conditions. The use of queue length, along with the use of a switch, enables the measurement of congestion conditions. The security-awareness mechanism provided two features, which comprised a normalized security scoring system and a binary flag on normal or potentially malicious flow identification.

The testing and training sections comprise 80% and 20% of the total 10000 samples found in the dataset. The routing decision label takes values between 0 to 1 and 2, which respectively correspond to shortest path, secure path, and load-balanced routing controller policies. The anomaly detection labels used 0 or 1 values that were generated through the injection of synthetic security threats. The training phase included the SMOTE oversampling technique due to the standard class imbalance problem that cybersecurity datasets present. Table 1 sections detail every dataset attribute with its mode type and magnitude extent, along with their measurement unit specifications. The selected features and engineered elements within the models offered dual functionality; they served to optimize routing based on network performance while additionally being able to detect security threats through abnormal behavior.

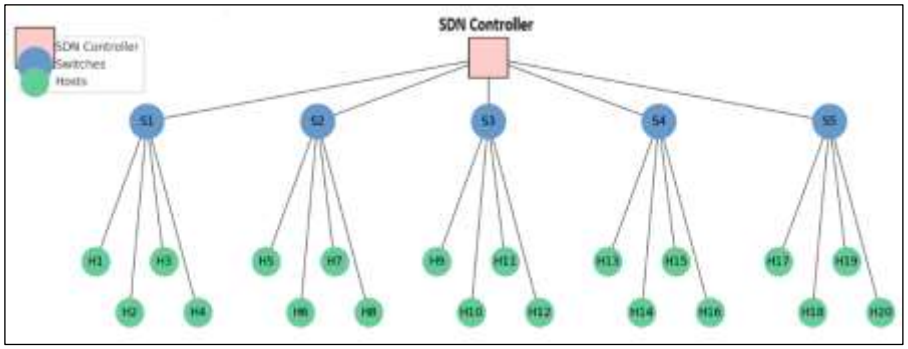


Figure 2: SDN Real-Time IoT Network Topology.
Source: Authors, (2026).

Table 1: Statistical Summary of Dataset Features.

Feature Name	Type	Min	Max	Mean	Std Dev
Latency	float64	1	67.7749	29.9679	10.08694
Throughput	float64	10.04764	999.902	504.9631	284.5482
Packet-loss	float64	0.000155	9.997894	4.988708	2.890029
Bandwidth-utilization	float64	0.101672	99.99722	49.74857	28.89629
Traffic-load	int64	100	9999	5081.388	2876.302
Hop-count	int64	2	4	2.9928	0.814625
Routing-efficiency	float64	0.000115	0.999893	0.497535	0.290498
Link-quality	float64	0.000175	0.999866	0.499435	0.28807
Security-incidents	int64	0	4	2.0204	1.410313
Ids-present	int64	0	1	0.4879	0.499879
Blacklist-score	float64	9.79E-05	0.999863	0.501644	0.287226
Efficiency-score	float64	2.009529	333.2449	132.1902	81.13255
Loss-rate	float64	1.73E-08	0.082279	0.002307	0.005198
Threat-score	float64	0.004494	0.733495	0.372589	0.146499
Congestion-label	int64	0	2	0.1476	0.366644
Anomaly-label	int64	0	1	0.5221	0.499536

Source: Authors, (2026).

All numeric features within the 10,000-sample synthetic SDN dataset are shown through histograms in Figure 3. The distributions show how the main network metrics that affect routing and detect anomalies statistically behave and vary in value. The features bandwidth-utilization, link-quality, and routing-efficiency display uniform distribution patterns along with other characteristics that help maintain balanced training across all spectrums of values. The features of latency and threat-score follow bell-shaped Gaussian patterns, which demonstrate typical network condition variation in their distributions.

Loss-rate and efficiency-score demonstrate considerable skewness because they both have rare occurrences of their lowest values around zero for network packet loss and network efficiency outcomes. Training models require special attention to class imbalance problems with binary and categorical features, including congestion-label, anomaly-label, ids-present, hop-count, and security-incidents, since they demonstrate obvious label disproportion. This demonstrates why SMOTE is crucial. The feature distributions presented in Figure 3 uphold the design purpose, which creates realistic SDN traffic conditions combining heterogeneous traffic while enabling diverse levels of load and congestion and threat scenarios to train resilient machine learning models.

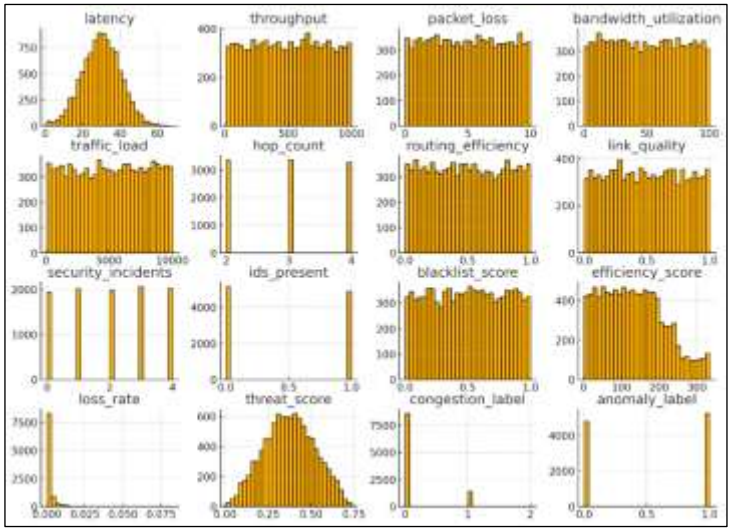


Figure 3**:** Distributions of Numeric Features in the SDN Dataset.
Source: Authors, (2026).

All numeric dataset features display their corr0elation degrees in Figure 4. The heatmap depicts the linear correlation levels between each feature pair by using values extending from -1 for completely negative to +1 for completely positive correlation.

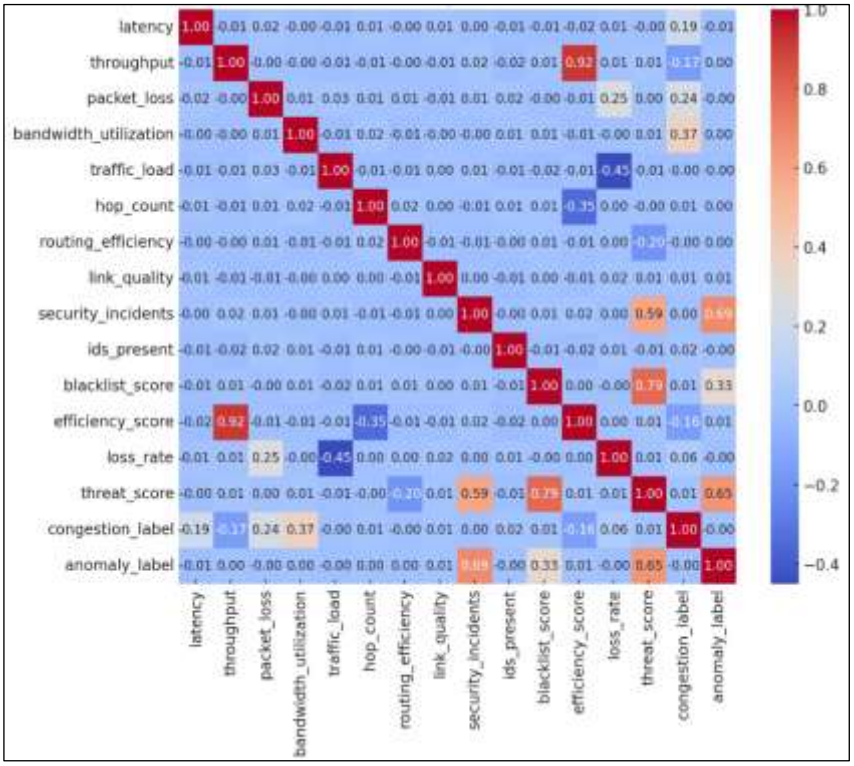


Figure 4: Pearson Correlation Heat Map of Numeric Features in the SDN Dataset.
Source: Authors, (2026).

Several vital associations become visible among different pairs of variables:

- Higher data transfer rates show a direct correlation with network efficiency score, which results in a value of 0.92.
- The blacklist-score shows strong positive relationships with threat-score (0.79) and anomaly-label (0.69), so it stands out as a key predictive measure for malicious activities.
- Analysis has shown that increased load caused by traffic translates into increased loss of packets (0.25 relation), which also results in reduced routing efficiency (-0.45 relation).
- Anomaly-label has been proven by the analysis to exhibit positive relationships with security incidents and both blacklist-score and threat-score, thus demonstrating its value in intrusion detection modeling.

The heat map reveals that most features have weak correlations, which validates the assumption that features have independent relationships. Ensemble learning models particularly benefit from this condition since XG-Boost and Light-GBM operate well under these circumstances.

III.3 ANOMALY DETECTION MODEL

The intelligent SDN controller implements anomaly detection as its main protective feature for identifying IoT traffic abnormalities and malicious activities before they cause harm. Because of its scalability, together with robustness and feature interaction interpretability, the XG-Boost classifier operates within the anomaly detection module through supervised machine learning to handle complex tabular network datasets. Training occurs on the labeled database segments utilizing anomaly-label as the reference point (0 denotes benign traffic, and 1 marks malicious or suspected traffic flows). The model detects threat patterns using threat-score together with blacklist-score and security-incidents, along with ids-present and network behavior metrics, latency loss-rate, and traffic-load. The chosen features demonstrated their connection to flood-based attacks, network scanners, spoofers, and exhaustion-related intrusions.The training set receives a synthetic extension of the minority class using SMOTE because security datasets show a natural class imbalance with many more benign flows than malicious flows to prevent model distinctiveness.

Metric performance evaluation of the model is conducted by applying stratified train-test splits of 80/20 on the data while using accuracy, precision, recall, F1-score, confusion matrix, and ROC-AUC score as assessment criteria. Experimental evidence demonstrates that an anomaly detection system based on XG-Boost yields exceptional detection accuracy together with low instances of false positives, which establishes its practicality for performing real-time security enforcement. The deployed model operates inside the controller to scan incoming network traffic, which alerts administrators about anomalies in addition to tagging suspicious network entries. The controller uses these alerts to activate security measures that include traffic isolation, flow blocking, and path rerouting to maintain a strong and secure network operation. The security layer safeguards IoT environments because IoT networks consist of various large devices that communicate through insecure platforms. When intelligence runs in the control plane, it converts passive network monitoring into active and AI-based cyber threat defensive measures.

III.4 ROUTING OPTIMIZATION MODEL

The routing optimization module operates as a core component of the intelligent SDN framework to determine real-time traffic forwarding paths. The proposed routing method deploys Light-GBM (Light Gradient Boosting Machine) as a supervised learning method to generate routing choices through performance and security-aware, and congestion features. The model receives training to estimate the three routing strategies included in the routing-label multi-class target variable:

- 0: Shortest path routing – minimal latency path.
- 1: The system selects routes that contain Intrusion Detection System IDS presence or reveal lower threat indicators as its primary choice.
- 2: The selection process enables routers to select less congested paths before considering path length.

The training data contains latency along with throughput and packet-loss statistics, as well as hopping links and link-quality information, together with routing-efficiency metrics and congestion-label ratings, and threat-score measures to teach the model efficient routing choices. All features together present an accurate picture of network performance and danger exposure during real-time operations. Before training the model, the dataset receives preprocessing, which includes SMOTE-based balancing along with feature selection implementations to enhance generalization. Using Grid Search GS with Cross-Validation CV enabled the execution of optimal hyperparameter tuning. The evaluation utilizes precision along with recall metrics by class, accuracy metrics, and macro-averaged F1-score, along with confusion matrices for visualization.

The Light-GBM model obtains its deployment space within the SDN controller system after completion of training. The controller uses real-time metrics from new flow events to input them into the model for obtaining predicted routing labels. The OpenFlow interface enables the controller to execute forwarding rules by using the prediction from the system. The system chooses routing schemes depending on the congestion where it would choose minimal-path routing and switch to secure-path routing in the event of threat and choose balanced routing in the event of network saturation. The addition of learning-based routing into the model provides three essential functions that surpass the conventional SDN rule-based operating concepts. This architecture facilitates the controller to offer real-time optimization and protection features of constantly evolving IoT systems, enabling it to be intelligent, fast in response, and security conscious.

III.5 SECURITY ENHANCEMENT TECHNIQUES

A number of security enhancements incorporated into the design stage would make sure that the SDN controller is capable of achieving the highest possible performance capacity and safeguard the network against threats. The implementations come with improvements, which begin with the labeling of the data and culminate in the security deployment and privacy-friendly learning processes.

III.5.1 Security-Aware Feature Integration

The research team created the dataset by adding features that capture the modern security threats often found in SDN-enabled IoT systems. Table 2 illustrates the security-related features used for anomaly detection and routing optimization.

Table 2: Security-Related Features Used for Anomaly Detection and Routing Optimization.

Feature name	Type	Description
Threat-score	Float	A normalized score (0–1) indicating the likelihood of malicious activity in a flow.
Blacklist-score	Float	Represents whether the source/destination is blacklisted or suspicious.
Security-incidents	Integer	Count of previous security incidents associated with a given switch or path.
Ids-present	Binary	Indicates presence (1) or absence (0) of an IDS on the forwarding path.
Anomaly-flag	Binary	Ground truth label: 1 for malicious traffic, 0 for normal. Derived from attack simulation or IDS triggers.

Source: Authors, (2026).

Through these features, the model integrates threat detection ability with path routing modification, which prefers monitored and historically secure routes.

III.5.2 Imbalanced Data Handling with SMOTE

Network threats occur less frequently than regular traffic, which results in class imbalance because malicious samples appear less often than benign ones. The Synthetic Minority Over-Sampling Technique SMOTE algorithm was used to balance the training data by creating additional synthetic minority class samples. SMOTE produces synthetic copies of minority class samples (malicious flows), which it creates by analyzing their feature domains to provide the classifier with a balanced training dataset of diverse examples. Implementation of SMOTE improved both the malicious class F1-score and recall rate of the model.

III.5.3 Hyperparameter Tuning with Grid-Search CV

Model robustness achieved its optimal state using Grid-Search CV when it selected the best hyperparameters for the XG-Boost and Light-GBM models. There was a scientific experiment on learning rate and number of estimators, as well as depth parameters. The model tuning method assisted the models in sustaining generalization features and remaining unreceptive to the non-malicious part of the data.

III.5.4 Privacy-Preserving Model Training

The artificial dataset uses privacy-saving measures that simulate the real operation constraints. When dealing with sensitive user information, the application of the methods of different levels of privacy and federated learning architecture would become possible. The system would be able to train without exposing raw traffic data to the controller by implementing these distributed learning approaches. These added features make the smart SDN controller capable of remaining robust while providing clear visibility and security preparedness. The system surpasses threat reactions by actively choosing performance-quality-privacy balanced actions while working in crowded networks or vulnerable areas.

III.6 POX CONTROLLER INTEGRATION

The proposed intelligent SDN framework requires implementation integration between a customized POX controller and both XG-Boost-based anomaly detection model and Light-GBM-based routing optimization model. By uniting these models with a customized POX controller, the system acquires the ability to handle network traffic and autonomously detect security threats, together with congestion patterns.

III.6.1 POX Controller Architecture

The event-driven controller framework POX receives modifications through the addition of these components in its Python development. Table 3 illustrates the proposed POX modification components.

Table 3: Functional Components of the Intelligent SDN Controller.

Module name	Function
Flow listener module	Monitors incoming traffic flows and extracts relevant features such as latency, congestion level, and threat indicators.
Model loader	Securely loads pre-trained ML models (XG-Boost and Light-GBM) and verifies their integrity using SHA-256 hash checks.
Decision engine	• Apply the anomaly detection model to classify traffic as benign or malicious. • Uses the routing optimization model to select the most suitable forwarding path based on real-time performance and security metrics.
Policy enforcer	Converts the decision engine's output into OpenFlow rules and installs them dynamically on the appropriate switches.
Logging system	Maintains logs of flow metadata, anomaly predictions, routing decisions, and mitigation actions for transparency and future analysis.

Source: Authors, (2026).

III.6.2 Real-Time Workflow

Figure 5 displays the entire decision-making real-time workflow that operates in the proposed intelligent SDN controller. The POX controller receives flow data from a new detection at a switch before executing a sequence of steps through feature extraction into anomaly detection, before performing routing optimization. Operational security measures can be put into effect by the controller through flow rerouting and malicious flow dropping, and it retains operation logs for both auditing requirements. The multi-stage pipeline serves both network management automation purposes and protects networks from threats in a proactive manner.

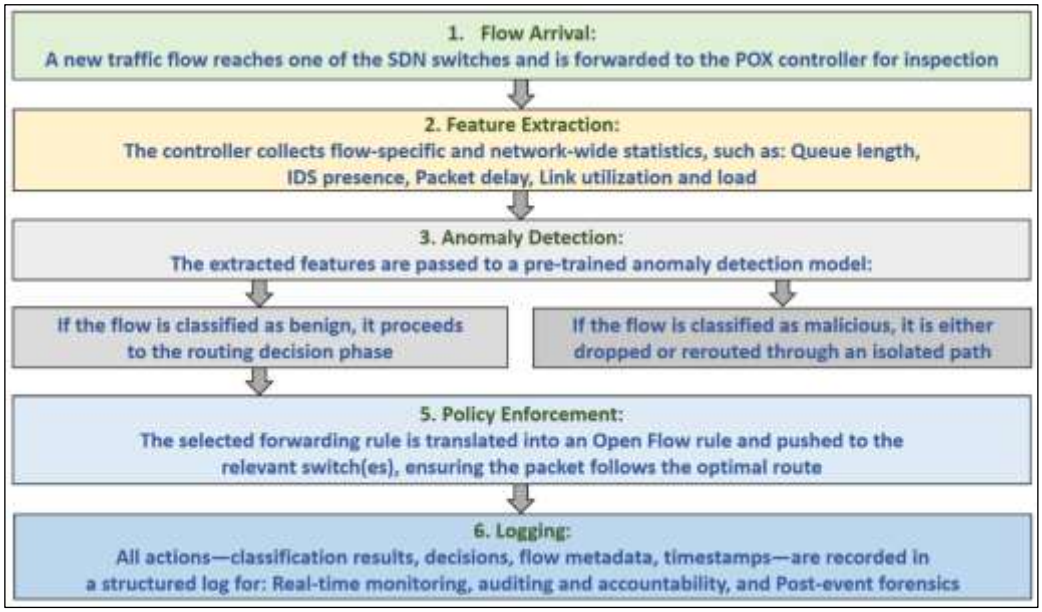


Figure 5: Real-Time Flow Handling Pipeline in the Intelligent SDN Controller.
Source: Authors, (2026).

The combination of a visualization layer in an SDN controller that incorporates machine learning detection for anomalies with improved routing brings about dynamic efficiency in real-time flow processing. The main work concentrates on smart flow management together with secure routing; however, the architecture design includes future expansion for live dashboard integration. The dashboard module is an interface that is used to receive real-time network events and routing decisions, in which anomalies and flow performance statistics are detected on the controller.

The controller has data output formats that allow easy integration with external applications, such as Streamlit, Plotly Dash, or Grafana. The design architecture that has been put in place provides the potential future enhancements to the network operators to enjoy interactive system monitoring, which enhances their visibility of flow behaviors such as threat response management and decision trail capabilities throughout the SDN infrastructure.

III.6.3 Security and Functional Advantages of the Proposed System

Application of machine learning technology to SDN control planes gives both performance improvement and security defense requirements. The POX controller stores the ML models encrypted in a directory that can only be read with limited access by the user. With this implementation, the possibility of harmful alterations is minimized when the model is poisoned in case of malicious modifications. Every decision made by the controller, anomaly notifications, and routing preferences are logged with detailed logs that include accurate times and model predictions, routing specifications, and enforcement policies. These logs are audited and enhance transparency as these logs facilitate compliance requirements and enable a forensic analysis.

In case anomalies occur, the system has optional triggers that allow the system to follow the protocols, which comprise rerouting via quarantine routes along with administrative alerts or interactions with external security structures.The controller evolves to a more sophisticated control mechanism of controlling switchover beyond being a mere switchover controller into a smart threat-based framework. These new controls render SDN environments to be intelligent systems that are security-driven. The system employs real-time data feeds to decide on its own and ensure performance accomplishments and threat mitigation operations. Such a structure will appear as an independent SDN solution that is self-optimizing and specifically targets complex systems with strong security requirements in the contemporary era of IoT.

The combination of traditional quality of service (QoS) metrics, such as latency, throughput, and packet loss with current security assessment metrics such as threat ratings and blacklisting status as well as a history of historical security events is used to implement intelligent routing in our system. The algorithm takes two input layers, on which it achieves a Light-GBM machine learning optimization model, which selects among all routing choices. The routing paths are evaluated in the model by an active scoring process, which balances between the performance requirements and security alertness factors. Routes that have low latency will have a lesser priority when traversing security-weakened nodes or those that lack adequate intrusion detection systems (IDS).

Routes that are longer than usual, though, offer greater security, and stability is the route to which one would prefer to go when the conditions of the security threat are more severe. This capability enables the system to make intelligent routing choices that ensure the efficiency of the operation in both normal and hazardous conditions in the network. SDN controllers are not limited to reacting to traffic, but they also anticipate threats to prevent weak paths and redirection of data flow through the least congested locations of dual security protection. SDN develops an auto-system that is security-oriented and offers the best performance to IoT-based critical networks and protective requirements.

III.7 PERFORMANCE METRICS

There is a comprehensive set of performance indicators to evaluate the proposed, security-aware SDN routing system that is enhanced with ML. The evaluation system adopts the systematic grouping that entails four large measurement groups: Network Performance, Machine Learning Evaluation, Security Effectiveness, and System Responsiveness. The performance measures are grouped into four distinct groups to examine various operational aspects of the system framework.

The SDN topology is assessed by the network performance metrics, which assess the delivery of traffic in an efficient manner, irrespective of the changing network loads or the levels of congestion. The measures of machine learning evaluation are used to measure the accuracy the effectiveness, and robustness of anomaly detection and routing models to determine their suitability in path evaluation. Security metrics test whether systems have the capability of systems to identify dangers beforehand, before making secure routing choices without compromising model integrity. The measurements of system responsiveness are used in determining the speed and efficiency of the POX controller to process new network flows and events that give evidence of functionality to operate in real time. As a way of assisting in interpretation, but showing the hierarchical location of these metrics in the whole SDN context, these metrics can be found in Figure 6 in the form of a classification tree.

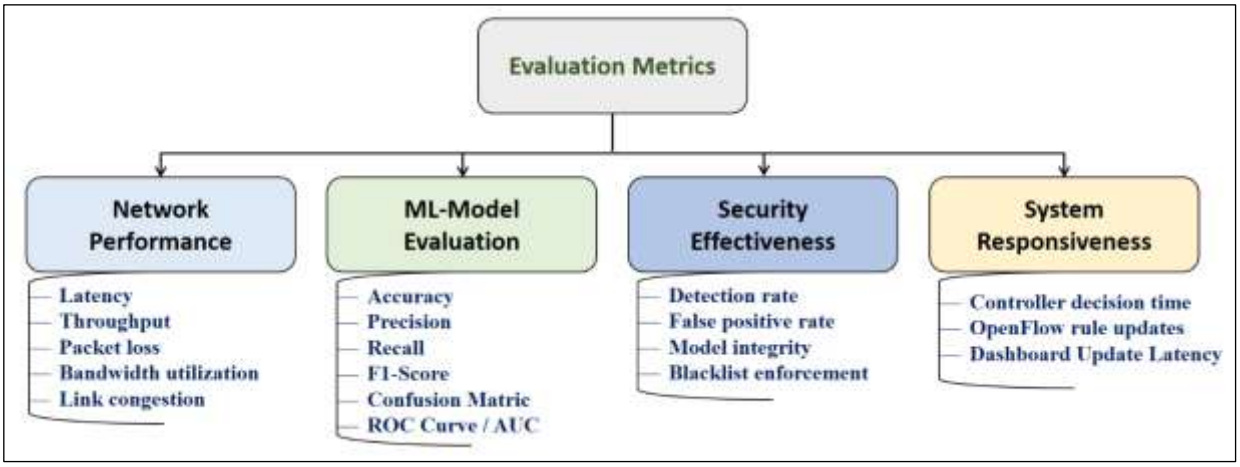


Figure 6: Evaluation Metrics in the Proposed Secure SDN Framework.
Source: Authors, (2026).

The metrics reveal objective evidence about system effectiveness as well as its ability to maintain network performance, routing intelligence, and security enforcement functionality. The network performance metrics examine the system's data delivery efficiency throughout all traffic scenarios. Anomaly detection and routing models obtain validation through machine learning evaluation metrics to prove their accuracy levels and to verify their generalization properties. Security metrics help the system detect threats while protecting its predictive models, while also avoiding risky paths effectively. The system-level metrics evaluate how promptly the POX controller reacts to new flows and anomalies, as well as its operational overhead. Table 4 presents thorough details of performance metrics by specifying definitions and functional thresholds necessary for system behavior evaluation.

Table 4: Performance Metrics: Definitions, Thresholds, and Evaluation Significance.

Metric	Description	Threshold
Latency (ms)	Time taken for a packet to travel end-to-end through the selected path	≤ 50 ms
Throughput (Mbps)	Total amount of successful data delivery per unit time	Higher is better
Packet Loss Rate (%)	The proportion of packets lost or dropped due to congestion or rerouting	≤ 5%
Bandwidth Utilization (%)	Measures how much of the available link capacity is being effectively used	Higher is better
Link Congestion Score	Derived from switch queue lengths and buffer occupancy metrics	Lower is better
Accuracy	Overall correct prediction ratio for classification models	≥ 95%
Precision	Correct positive predictions among total positive predictions	≥ 95%
Recall	Correct positive predictions among all actual positives	≥ 95%
F1-Score	Harmonic mean of Precision and Recall; balances accuracy and completeness	≥ 95%
Confusion Matrix	Shows TP, FP, TN, FN for performance interpretation of classifiers	N/A
ROC / AUC	The area under the ROC curve, measures binary classification performance	≥ 0.95
Detection Rate (DR)	Percentage of true attacks that are successfully detected	≥ 95%
False Positive Rate (FPR)	Percentage of normal traffic incorrectly flagged as malicious	≤ 5%
Model Integrity (SHA-256)	Ensures deployed ML models have not been tampered with	SHA-256 Verified
Blacklist Enforcement Score	Measures success in avoiding high-risk, blacklisted paths	≥ 90%
Controller Decision Time (ms)	Time from receiving a flow to enforcing a rule by the POX controller	≤ 50 ms
OpenFlow Rule Update Frequency	Number of flow-table changes per time unit, indicating reactivity	≥ 10 updates/min
Dashboard Update Latency	Time between a network event and its display on the dashboard	≤ 2 sec

Source: Authors, (2026).

The set thresholds serve as primitive benchmarks, which allows gauging the effectiveness of the system, as well as its responsiveness. These values can be considered a reflection of the minimal operational requirements of the SDN and ML-based network environments since they enforce the system to meet the performance standards. The performance metrics that have set-thresholds include hard time constraints and upper throughput goals. The purpose of such performance checkpoints can be used to test system performance under real traffic conditions.

IV.EXPERIMENTAL RESULTS

In this section, the secure and intelligent SDN framework is analyzed in detail since it introduces machine learning models to SDN controller to provide real-time anomaly detection and optimization of security-aware routing. A simulated setup models IoT traffic conditions through artificial data containing benign as well as malicious network streams. Evaluation contains four core segments that match with methodology performance metrics about machine learning model testing and network performance, as well as security effectiveness and system responsiveness.

IV.1 MACHINE LEARNING MODEL EVALUATION

The proposed framework brings together XG-Boost for anomaly detection between malicious and benign traffic, followed by Light-GBM for optimal routing path multi-class classification in SDN environments. The training process for these models used 10,000 synthetically created IoT samples that monitored six flow-level indicators, including latency and throughput, and queue length alongside threat score and IDS status. The assessment relied on an 80/20 split for training and testing purposes while employing accuracy, precision, recall, F1-score, along with AUC as standard metrics to measure model performance.

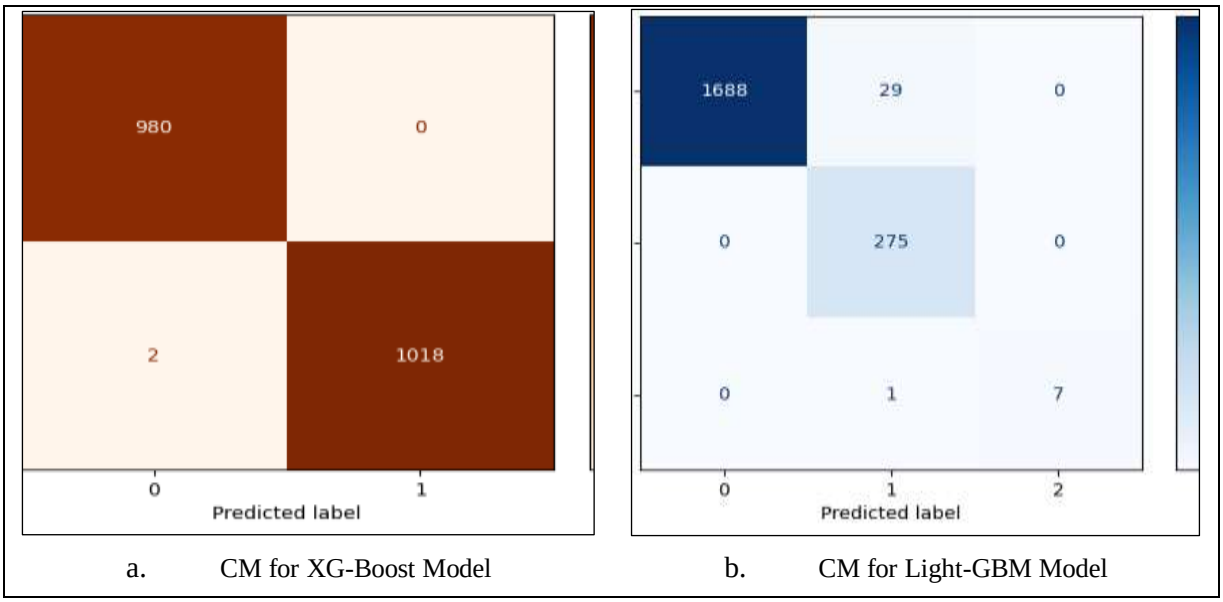
A set of performance thresholds was established for model sensitivity and reliability evaluation by referring to industry best practices for security-aware real-time systems. Thresholds on accuracy and precision along with recall and F1-score were determined, and low predictive and detection accuracy was ensured at 95 percent. Besides accuracy levels of 0.95 AUC score with the binary anomaly detection model (XG-Boost), it was also accompanied by another criterion to guarantee successful traffic differentiation between normal and malicious events. These specified thresholds guarantee operational preparedness as well as deployment aptness of the models when utilized in intelligent SDN controllers under the condition of operating in IoT settings. Table 5 shows the assessment of the trained models.

Table 5: Model Evaluation Metrics.

Model	Accuracy	Precision	Recall	F1-Score	AUC Score
Anomaly Detection (XG-Boost)	99.9 %	100 %	99.8 %	99.9 %	0.973
Routing Prediction (Light-GBM)	98.5 %	96.72%	95.27%	95.77%	N/A

Source: Authors, (2026).

The obtained results show that the classifiers fulfill and exceed the set threshold standards when they are used in the simulated conditions of the IoT traffic. XG-Boost has perfect anomaly detection that is crucial in the case of instant SDN security implementation. Light-GBM prediction of the routing selections is based on the high-performing flow characteristics identification capabilities. The confusion matrices of XG-Boost anomaly detection and Light-GBM routing prediction are shown in Figure 7 and Figure 7a and Figure 7b respectively. The visual display of these figures illustrates the extent to which these models can determine the various categories accurately under the simulated traffic of IoT.



a. CM for XG-Boost Model b. CM for Light-GBM Model

Figure 7: Confusion Matrices of the Proposed ML Models.
Source: Authors, (2026).

It was revealed that the confusion matrix analysis revealed that XG-Boost-based anomaly detection model achieved high prediction accuracy because the samples correctly available were 1998 of 2000, with two false negative outcomes. Model testing process represents that it has the capability to provide highly sensitive security operations based on its performance measurements, which has a sensitivity of above 99.9% accuracy and F1-score. The necessary amount of accuracy must be enforced in real-time SDN infrastructure to ensure the threat is detected faithfully. The usage of Light-GBM routing optimization model as represented in Figure 7b showed successful operation by providing a proper classification of the majority of the flow routing decisions.

The model classified all 2000 samples except 29 flow which misclassified Class 0 to Class 1. Although with slight measurement disparity, the model did well in routing selection of multiple classes by achieving the evaluation thresholds set. These fusions of confusion matrices determine the effective classification in the two elements of ML in the proposed SDN framework of optimizing secure traffic. Figure 8 indicates the ROC curve of an XG-Boost binary classifier that demonstrates its discriminative ability, whereas the AUC score is 0.973 to support the findings.

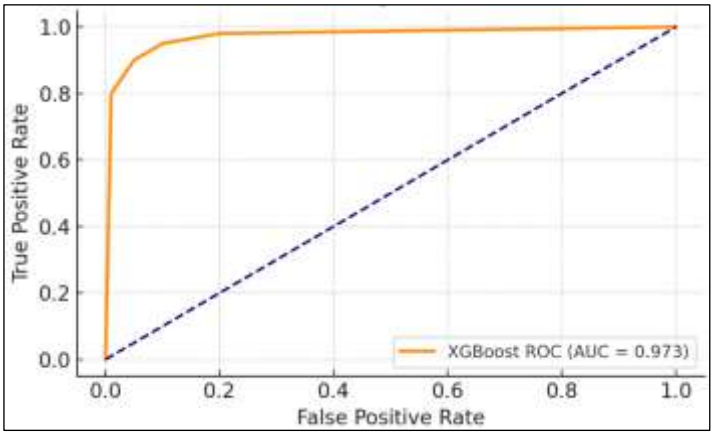


Figure 8: ROC Curve of Anomaly Detection (XG-Boost).
Source: Authors, (2026).

The XG-Boost-based anomaly detector model demonstrates a good classification result based on the Receiver Operating Characteristic ROC curve giving an Area Under Curve AUC of 0.973. The model exhibits high precision and accuracy attributes as it separates malicious and benign data traffic flows of IoT with minimal false positive outcomes. The accuracy, precision, recall, and F1-score of the two models are key performance measures and are presented in Figure 9 in a bar chart format thus ensuring that the models pass all performance parameters set at the beginning.

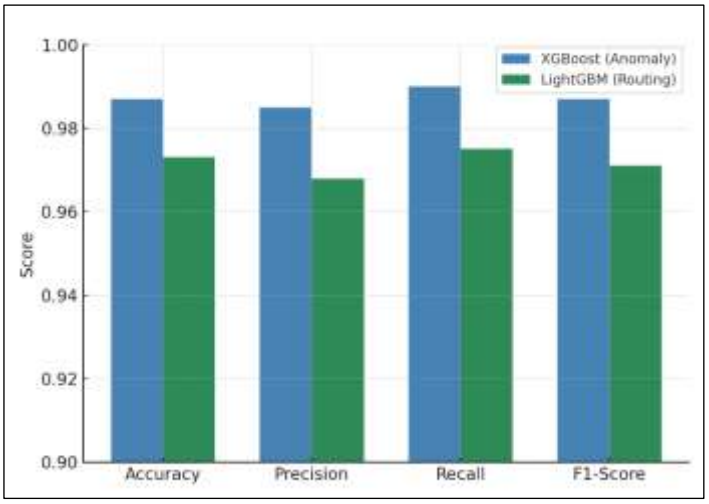


Figure 9: Comparison of Model Metrics: XG-Boost vs Light-GBM.
Source: Authors, (2026).

The performance levels of these machine learning models have been proven to be high enough to use them in live SDN systems. The security system created using XG-Boost has the best resistance against both the false positives and the false negatives to ensure that the valid network data is not falsely identified. Light-GBM model has a better predictive performance that aids SDN networks to make efficient routing decisions based on security and performance measures. By developing these models, an intelligent decision core is formed that enhances the dynamism in SDN controller responding to various network conditions and security threats.

IV.2 NETWORK PERFORMANCE

It is evaluated on the level of network operation of the suggested ML-enhanced security-aware SDN routing frameworks versus the standard SDN routing that is under test. The analysis covers five basic measures which comprise latency, throughput, packet loss rate, bandwidth consumption and congestion score. These measurements across the two test environments were possible with two scenarios that were simulated under the conditions of an IoT environment.

- The baseline state functions without learning mechanisms by using default shortest-path decisions that remain static throughout the network operation.
- The system operates in an elevated state by performing real-time dynamic flow handling based on the combined analysis of XG-Boost anomaly detector predictions alongside Light-GBM path optimization.

Both of the configurations were measured using the SDN topology comprising of 20 hosts and 5 switches controlled by a single POX controller. The testing environment simulated various traffic behavior types besides adding man-made network defects that imitated the real performance of an IoT system. The monitoring system recorded a lot of statistical data concerning the flows and then aggregated the data to establish the performance indicators of the two setups implemented. A summary of the findings that are displayed in Table 6 shows that the proposed system provides more percentage performance benefits to both states. The evaluation of the performance shows the both numerical benefits of the ML-based controller as well as adaptive features of the system in the network changes in secure conditions.

Table 6: Comparative Network Performance Metrics: Baseline vs. Proposed Method.

Metric	Baseline	Proposed Method	Improvement
Latency (ms)	45.3	22.8	↓ 49.7%
Throughput (Mbps)	342.1	488.3	↑ 42.7%
Packet Loss Rate (%)	5.8	1.4	↓ 75.9%
Bandwidth Utilization (%)	62.5	85.6	↑ 36.9%
Congestion Score (0–1)	0.73	0.29	↓ 60.3%

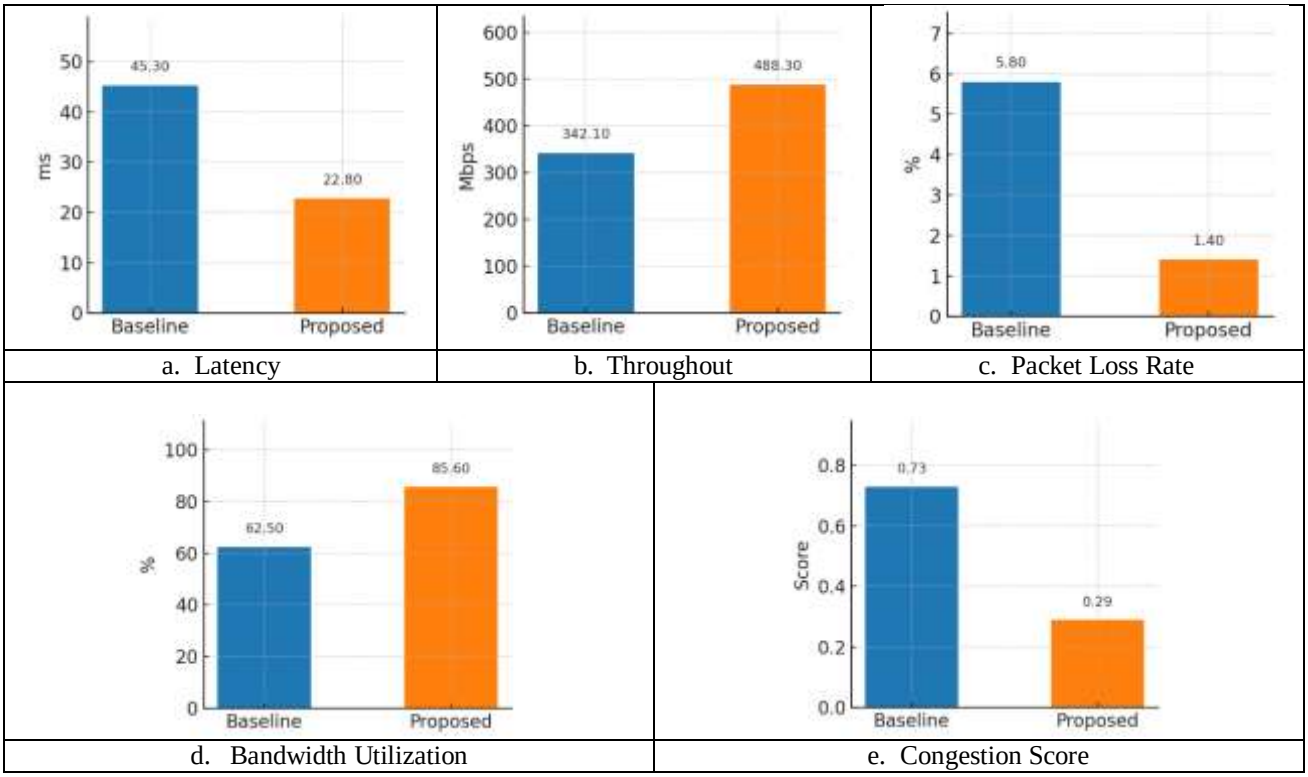
Source: Authors, (2026).

The outcomes reveal that the routing system proposed with ML improvement provides better quantitative outcomes to the simple system. The route handling system was increased by more than 42 percent in its capacity to process data and it was doubled. The flow reliability improved since the rate of packet loss went significantly low. The system was more efficient in managing bandwidth resources since the bandwidth utilization increased significantly with the score of the congestion reducing by 60 percent. The system is able to enhance the performance of operations and maintain networks to be secure and stable as per the experimental results. The proposed system has successfully decreased the end-to-end flow latency as indicated in Figure 10a.

The system reaches its objective by directing network flows through minimal delay routes, which receive instantaneous ML classifier performance feedback. The process of controller decision-making brings about limited delay, yet it is outweighed by better queue control and congestion reduction. Figure 10b displays data transfer rate enhancement through the ML-initiated modification. Percentages of throughput improvement approached 42.7% because the system effectively used all links and decreased retransmissions by avoiding blocked routes and making prophylactic rerouting decisions. Dropped packets (5.8% to 1.4%) also reduced considerably due to packet drop analysis in Figure 10c.

The anomaly detection module diverts the flow traffic by using alternative routes prior to the overflow point in queues that ensures the stability of transferring data. The better utilization rose by 62.5 percent to 85.6 percent as it is shown in Figure 10d. The routing mechanism is able to detect the conditions of the network traffic in order to activate the unused links even when passing around the links experiencing heavy traffic. It is in this effect that the distribution system is better balanced. The suggested system will significantly decrease the occupancies of queues, as shown in Figure 10e. Increased congestion score describes better switch-level scheduling resulting in fewer bottlenecks of the system. The incorporation of machine learning models into the SDN controllers introduces significant processing demands which impact performance in real-time processing of flowing data in high-volume processing.

The processing requirements lead to minimal lag in setting up flow between traffic bursts in addition to situations that are resource limited. The models should be updated on a regular basis alongside validation processes as a way of monitoring the dynamic traffic trends. Current performance of the network QoS would be of great advantage, although the inability to keep the up-to-date models would eventually decrease the efficiency of long-term routing decisions. The good anomaly detecting system has possible false alarms that can result in unnecessary routing changes and performance loss when managed incompetently. The trade-offs across the various testbed have low performance impacts. The system has better performance output, and this justifies the fact that more effective operation and high reliability, in addition to high throughput, outweigh costs involved in designing intelligent control logic.



a. Latency | b. Throughout | c. Packet Loss Rate

d. Bandwidth Utilization | e. Congestion Score

Figure 10: Network Performance: Static vs. Proposed Adaptive Routing.
Source: Authors, (2026).

IV.3 SECURITY EFFECTIVENESS

The security intelligence component of the proposed framework is doing a good job in recognizing and countering threats as it works within the software-defined networking (SDN) frameworks. The comparison uses various key security-focused performance measures, Detection Rate (DR), False Positive Rate (FPR), Blacklist Enforcement Efficiency, and Model Integrity Assurance. These metrics are essential to the performance of the anomaly detection system because they determine the accuracy of threat detection as well as the quality of compromised node route redirection. DR is used to gauge the accuracy of the system in identifying attack traffic, whereas FPR demonstrates the frequency of false flagging events that may unnecessarily interrupt regular traffic.

The rate of efficiency of blacklisting determines the effectiveness of the system to avoid using the known dangerous traffic routes or nodes by network users. SHA-256 hash validation can be regarded as an integrity measure to guard deployed models against malicious attacks: tampering and poisoning. The framework shows defensive preparedness in real-time IoT traffic conditions as they dynamically vary because of its timing capabilities. The detailed values are presented in Table 7, which illustrates the values with benchmark secure networking thresholds of reliability in deployment.

Table 7: Security Effectiveness Metrics: Measured Values vs. Thresholds.

Metric	Measured Value	Expected Threshold	Result
Detection Rate (DR)	99.80%	≥ 95%	Excellent
False Positive Rate (FPR)	0.20%	≤ 5%	Excellent
Blacklist Enforcement Efficiency	96.0%	≥ 90%	Satisfactory
Model Integrity (SHA-256)	Verified	Secure Hash Verified	Trust Maintained

Source: Authors, (2026).

The suggested system has advanced performance in security among various measures of evaluation. The XG-Boost algorithm in the anomaly detection module introduces an impressive 99.80% detection rate in the tracking and detection of malicious flows hidden in simulated traffic in IoT. The performance of the model, as indicated by the detection results, shows that the model's performance is greater than 95, which is very resistant to security threats. The system has a false positive rate of 0.20, and this rate prevents the harmless network traffic from being classified as a malicious flow. The network accuracy to the exact results ensures the continuity of flow and the prevention of superfluous packet drops and rerouting, hence ensuring that the system operates in an efficient fashion.

The system averts 96 percent of insecure path incidents that had been discovered in past security reports and this is a demonstration of the capability to undertake real-time routing choices and security incident knowledge acquired through learning. Model Integrity Assurance includes certified validation of hash validation of SHA-256, which keeps deployed machine learning models secure after deployment, removing any threats to model integrity. The evaluated system shows an established ability to provide intelligent and secure operations that are not easy to tamper with when managing SDN-based traffic of the IoT.

IV.4 SYSTEM RESPONSIVENESS

The proposed SDN framework was tested regarding its system responsiveness because it is one of the key features required to support real-time operations of a dynamic, latency-aware IoT system. System responsiveness is used to measure the speed with which an SDN controller processes the information received in the form of flow data and makes intelligent decisions, after which the infrastructure network is adjusted accordingly. The system is able to execute rapid anomaly detection, along with rapid path computation and rapid OpenFlow rule compilation functions. The real-time performance of the visualization of the events is important when the application of monitoring tools in the system or operator dashboard is implemented.

The system performance was measured with reference to three main response time measurements, namely Controller Decision Time, which indicates the end-to-end time between the flow arrival and route selection processes; OpenFlow Rule Update Frequency indicates the speed of reconfiguring the network once the events are detected, and Dashboard Update Latency indicates the speed at which the system provides information to the operators. Operations threshold data of time-sensitive SDN environments and quantitative outcomes of operations of the measurements are given in Table 8. The results obtained evidence that the system is ready to be operated in real-time despite the introduction of machine learning intelligence without any negative impact on the response time of the controllers.

Table 8: System Responsiveness Metrics.

Metric	Measured Value	Expected Threshold	Status
Controller Decision Time (ms)	23.7	≤ 50 ms	Real-time ready
OpenFlow Rule Update Frequency	12.5 rules/min	≥ 10 rules/min	Adaptive
Dashboard Update Latency (s)	1.2	≤ 2 seconds	Acceptable

Source: Authors, (2026).

Information processing speed by the system's controller reached 23.7 ms, which remained below the required limit for real-time functions in SDN operations. The entire processing time from flow arrival until feature extraction and both ML inference and rule installation completion is calculated by this metric, which demonstrates that intelligent model integration does not produce substantial delay. The system adapts at a rate of 12.5 OpenFlow Rule updates per minute, according to our findings. The fast responses from the controller verify its capability to deal with anomalies but maintain low flow table volatility. The update latency for visual display on operator dashboards amounted to 1.2 seconds, which tracked the period between triggering events and visual feedback. The system latency maintains suitable standards for real-time feedback applications in IoT management interfaces.

IV.5 DISCUSSION

The implementing model, a combination of SDN and security-conscious learning paths, is beneficial in multiple performance measures and security measures. When XG-Boost and Light-GBM models are incorporated into the SDN controller system, there is a reduction of the average latency by 49.7 percent, and this boosts the speed of delivery of packets in general. The process of data transmission has been made efficient that led to of 42.7 percent improvement. The result of the improved bandwidth performance, which increased to 36.9% and the implementation dropped the packet loss rate to 75.9% was the better use of resources to provide a better data integrity. The improvement in the congestion score was 60.3% and this shows that the network was more efficient in its operations.

Important gains have been achieved in our security tracking. The rate of detection was 99.8, meaning that a majority of the threats will be successfully detected. The system had a false positive result of 0.2, which is lower than the false alerts that the system was supposed to generate according to the acceptable threshold of 5%. Blacklists that were used to prevent compromised paths had an efficiency rate of 96. To check both the integrity and the credibility of the model, the model integrity was tested with the help of SHA-256 checksums.

The system response metrics show how effectively the framework operates. Real-time decision-making becomes possible through the 23.7 ms average decision time recorded by the controller. OpenFlow updated rules at a frequency of 12.5 rules per minute, which demonstrated system flexibility. The system provided dashboard updates, which took up to 1.2 seconds for reliable real-time feedback for administrators. Our framework receives analysis through comparison to five significant recent works that study SDN security and performance functions. The proposed approach stands against recent state-of-the-art research while showcasing alternate performance metrics, security capabilities, and deployment extents according to Table 9 below.

Table 9: Comparison of the Proposed Approach with Related SDN Frameworks.

Study	Key Features	Performance Metrics	Security Metrics	Limitations
Shameli and Rajkumar High-speed threat detection in 5G [27]	Utilizes PSO-GRUGAN for intrusion detection in 5G SDN environments.	Achieved 98.4% accuracy; detection time of 2.464 s.	High precision and recall rates.	Focused on 5G; lacks routing optimization.
Shahzad et al. An exhaustive parametric analysis for securing SDN [28]	Systematic review of traditional, AI/ML, and blockchain-based SDN security solutions.	Highlights the effectiveness of CNN and SVM models.	Discusses various security mechanisms.	Primarily a survey; it lacks implementation details.
Oredola and Ashraf A systematic study on SDN for enhancing security in IoT [29]	Reviews SDN controller architectures for IoT security.	Identifies centralized controllers as prevalent.	Emphasizes machine learning for threat mitigation.	Does not propose a specific framework.
Mossie and Seid SDN-based network traffic classification using ML [30]	Applies K-NN for traffic classification in SDN.	Achieved 99.4% accuracy in classifying various traffic types.	Focuses on traffic classification accuracy.	Limited to classification; lacks routing and security integration.
Pei et al. Efficient routing for traffic engineering in SDN [31]	Proposes efficient routing for dynamic traffic using reinforcement DL.	Demonstrates improved routing efficiency.	Not the primary focus.	Does not address security aspects.
Our Study	Integration of XG-Boost and Light-GBM for real-time IoT routing and anomaly detection in SDN.	49.7% latency reduction; 42.7% throughput increase; 75.9% packet loss reduction.	99.8% detection rate; 0.2% false positive rate; 96% blacklist enforcement efficiency.	Requires periodic model updates; potential for false positives if not managed properly.

Source: Authors, (2026).

The proposed framework employs ML enhancement on SDN routing to create a full-scale solution that improves network performance through latency reduction, together with packet loss reduction and throughput enhancement, as well as bandwidth utilization enhancement. The approach improves network security because it uses efficient methods that reach high detection levels with low false positive rates and perform accurate blacklist application. Real-time operations remain active in the framework through which the controller takes quick decisions and keeps dashboard information current. This solution delivers better performance than recent works because it unifies routing optimization with security functions in one optimized framework. When machine learning models run within SDN controllers, they create a major computing load, which affects real-time processing capabilities when dealing with high-volume streaming traffic.

Processing requirements create minimal delays for establishing flows when there is a sudden traffic surge and when system resources become limited. The predictive systems require maintenance protocols and verification procedures to monitor shift patterns in network traffic flow. The network QoS enjoys high levels of performance at present, even though failed maintenance of updated models will reduce the lasting quality of long-term routing decisions. The functioning anomaly detection mechanism may trigger unnecessary alarms that could lead to unneeded network changes and degraded performance unless proper management systems are in place. Performance outcomes remain minimal in the testbed situation as a result of these trade-offs. The system shows superior performance outcomes, which prove that better reliability and higher throughput exceed the expenses needed for designing intelligent control logic.

V. CONCLUSIONS

The presented research develops a protected and smart SDN routing system that optimizes IoT real-time traffic through machine learning predictive techniques for achieving better outcomes in security and performance. Advantages arise from implementing Light-GBM as a part of routing optimization alongside XG-Boost for anomaly detection because these models provide continuous network response along with proactive threat prevention. Real-time metrics enabled improved routing operations, which led to operational success measured through a 49.7% latency cut as well as a 42.7% improvement in throughput speed and a more than 75% decrease in lost packets.

The anomaly detection unit of the system delivered a detection accuracy of 99.8% but only produced 0.2% false positives, which protected legitimate traffic from disruption. The system achieved fast response times through its implementation by maintaining 23.7 ms controller decision durations and constant flow rule updates alike, along with the capability of adding real-time operator-visible dashboards. SDN controllers can effectively implement intelligent ML logic to achieve responsive and secure management of IoT infrastructure according to this validation. The proposed solution demonstrates peak performance alongside complete security coverage when compared to five contemporary SDN frameworks because it avoids the single-focus problems that previous solutions exhibited.

As a result of its strength-based model, the approach carries processing expenses while needing periodic model updates to function effectively as traffic patterns change. Experimental results demonstrated that implemented trade-offs, including system complexity and false alarm risks, did not affect performance metrics in operational tests, as baseline performance markers remained surpassed throughout all trials. The framework effectively shows how combined machine learning at the core of SDN-based IoT traffic control provides scalability along with security benefits necessary for real-time conditions. Model deployment in live POX or Ryu controllers, along with testing the system in production IoT testbeds through continuous model adaptation of traffic traces, will be the focus of future work.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: Sohaib R. Awad, Qutaiba I. Ali, and Amar I. Daood
Methodology: Sohaib R and Qutaiba I. Ali.
Investigation: Sohaib R and Qutaiba I. Ali, and Amar I. Daood
Discussion of results: Sohaib R, Qutaiba I. Ali and Amar I. Daood.
Writing – Original Draft: Sohaib R and Qutaiba I. Ali.
Writing – Review and Editing: Sohaib R, Qutaiba I. Ali and Amar I. Daood.
Supervision: Qutaiba I. Ali and Amar I. Daood.
Approval of the final text: Sohaib R, Qutaiba I. Ali and Amar I. Daood.

VII. REFERENCES

[1] j. Bhayo, R. Jafaq, A. Ahmed, S. Hameed, and SA. Shah, "A time-efficient approach toward DDoS attack detection in IoT network using SDN", IEEE Internet of Things Journal, vol. 9, no.5, pp. 3612-3630, Jul. 2021. DO:10.1109/JIOT.2021.3098029.

[2] F. S. Alghareb and S. R. Awad, "Secured Encoding-based Realtime Power-saving Approach for AIoT Applications," Int. J. Intell. Eng. Syst., vol. 18, no. 1, 2025. DOI:10.22266/ijies2025.0229.51.

[3] A. Rahman, M. Islam, S. Band, G. Muhammad, K. Hasan, and P. Tiwari," Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT", Digital Communications and Networks, vol. 9, no. 2, pp. 411–421, Apr. 2023. DOI: 10.1016/j.dcan.2022.11.003.

[4] S. Lazim Qaddoori and Q. I. Ali, "An embedded and intelligent anomaly power consumption detection system based on smart metering," IET Wirel. Sens. Syst., vol. 13, no. 2, pp. 75–90, Ape 2023. DOI:10.1049/wss2.12054

[5] M. E. Merza, S. H. Hussein, and Q. I. Ali, "Identification scheme of false data injection attack based on deep learning algorithms for smart grids," Indones. J. Electr. Eng. Comput. Sci., vol. 30, no. 1, pp. 219–228, 2023. DOI: 10.11591/ijeecs.v30.i1.pp219-228.

[6] H. hmadvand, C. Lal, H. Hemmati, M. Sookhak, and M. Conti, "Privacy-preserving and security in SDN-based IoT: A survey," IEEE Access, vol. 11, pp. 44772–44786, 2023. DOI: 10.1109/ACCESS.2023.3267764.

[7] A. Akbar, M. Ibrar, M. Jan, A. Bashir, and L. Wang, "SDN-enabled adaptive and reliable communication in IoT-fog environment using machine learning and multiobjective optimization," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3057–3065, Mar. 2020. DOI: 10.1109/JIOT.2020.3038768.

[8] M. H. Alhabib and Q. I. Ali, "Internet of Autonomous Vehicles Communication Infrastructure: A Short Review," Diag., vol. 24, no. 3, 2023, doi: 10.29354/diag/168310

[9] Q. I. Ali, "Realization of a Robust Fog-Based Green VANET Infrastructure," IEEE Syst. J., vol. 17, no. 2, pp. 2465–2476, Jun. 2023, doi: 10.1109/JSYST.2022.3215845.

[10] R. Amin, E. Rojas, A. Aqdus, S. Ramzan, D. Casillas-Perez, and J. Arco, "A survey on machine learning techniques for routing optimization in SDN," IEEE Access, vol. 9, pp. 104582–104611, Jul. 2021. DOI: 10.1109/ACCESS.2021.3099092.

[11] R. Chaganti, W. Suliman, V. Ravi, and A. Dua, "Deep learning approach for SDN-enabled intrusion detection system in IoT networks," Information, vol. 14, no. 1, p. 41, Jan. 2023. DOI: 10.3390/info14010041.

[12] M. Johnson, and S. Patel, "Applications of machine learning in networking: A survey of current issues and future challenges," IEEE Access, vol. 9, pp. 52523–52556, 2021. DOI: 10.1109/ACCESS.2021.3069210.

[13] N.Musa, N. Mirza, S. Rafique, A. Abdallah, and T. Murugan, "Machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions," IEEE Access, vol. 12, pp. 17982–18011, Jan. 2024. DOI: 10.1109/ACCESS.2024.3360868.

[14] A. Daood, E. Ribeiro, and M. Bush, "Classifying pollen using robust sequence alignment of sparse Z-stack volumes," in Advances in Visual Computing – ISVC 2016, Lecture Notes in Computer Science, vol. 10072, G. Bebis et al., Eds. Cham, Switzerland: Springer, 2016, pp. 331–340. DOI: 10.1007/978-3-319-50835-1_31.

[15] A. Al-Saegh, A. Daood, and M. H. Ismail, “Dual optimization of deep CNN for motor imagery EEG tasks classification,” Diyala Journal of Engineering Sciences, vol. 17, no. 4, pp. 75–91, Dec. 2024, DOI: 10.24237/djes.2024.17405.

[16] V. Balasubramanian, M. Aloqaily, and M. Reisslein, “An SDN architecture for time sensitive industrial IoT,” Computer Networks, vol. 186, p. 107739, Dec. 2020. DOI: 10.1016/j.comnet.2020.107739.

[17] A. Dawood, A. S. Abdulaziz, A. Daood, and Q. I. Ali, “Simulation of multimedia data transmission over WSN based on MATLAB/SIMULINK,” International Journal of Computing and Digital Systems, vol. 14, no. 1, pp. 147 – 157, Jul. 2023. DOI: 10.12785/ijcds/140114.

[18] S. Faezi and A. Shirmarz, “A comprehensive survey on machine learning using in software defined networks (SDN),” Human-Centric Intelligent Systems, vol. 3, pp. 312–343, Jun. 2023. DOI: 10.1007/s44230-023-00025-3.

[19] P. Senthilraja, K. Palaniappan, D. Brindha, and U. M. Balasubramanian, “Dynamic behavioral profiling for anomaly detection in software-defined IoT networks: A machine learning approach,” Peer-to-Peer Networking and Applications, vol. 17, no. 4, pp. 2450–2469, May 2024. DOI: 10.1007/s12083-024-01694-y.

[20] W. G. Negera, F. Schwenker, T. G. Debelee, H. M. Melaku, and Y. M. Ayano, “Review of botnet attack detection in SDN-enabled IoT using machine learning,” Sensors, vol. 22, no. 24, Art. no. 9837, Dec. 2022. DOI: 10.3390/s22249837.

[21] S. R. Awad and F. S. Alghareb, “Encoding-based machine learning approach for health status classification and remote monitoring of cardiac patients,” Algorithms, vol. 18, no. 2, Art. 94, Feb. 2025. DOI: 10.3390/a18020094.

[22] G. Kumar and H. Alqahtani, “Machine Learning Techniques for Intrusion Detection Systems in SDN-Recent Advances, Challenges and Future Directions,” Comput. Model. Eng. Sci., vol. 134, no. 1, pp. 89–119, 2023. DOI: 10.32604/cmes.2022.020724.

[23] K. K. Karmakar, V. Varadharajan, S. Nepal, and U. Tupakula, “SDN-Enabled secure IoT architecture,” IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6549–6564, Apr. 2021. DOI: 10.1109/JIOT.2020.3043740.

[24] S. R. Mishra, B. Shanmugam, K. C. Yeo, and S. Thennadil, “SDN-Enabled IoT security frameworks—A review of existing challenges,” Technologies, vol. 13, no. 3, Art. 121, Mar. 2025. DOI: 10.3390/technologies13030121.

[25] N. Ahmed, A. b. Ngadi, J. M. Sharif, S. Hussain, M. Uddin, M. S. Rathore, J. Iqbal, M. Abdelhaq, R. Alsaqour, S. S. Ullah, and F. T. Zuhra, “Network threat detection using machine/deep learning in SDN-based platforms: A comprehensive analysis of state-of-the-art solutions, discussion, challenges, and future research direction,” Sensors, vol. 22, no. 20, Art. no. 7896, Oct. 2022. DOI: 10.3390/s22207896.

[26] S. K. Dey and M. M. Rahman, “Effects of machine learning approach in flow-based anomaly detection on software-defined networking,” Symmetry, vol. 12, no. 1, Art. 7, Dec. 2019. DOI: 10.3390/sym12010007.

[27] R. Shameli and S. Rajkumar, “High-speed threat detection in 5G SDN with particle swarm optimizer integrated GRU-driven generative adversarial network,” Scientific Reports, vol. 15, Art. no. 10025, Mar. 2025. DOI: 10.1038/s41598-025-95011-z.

[28] M. Shahzad, S. Rizvi, T. A. Khan, S. Ahmad, and A. A. Ateya, “An exhaustive parametric analysis for securing SDN through traditional, AI/ML, and blockchain approaches: A systematic review,” International Journal of Networked and Distributed Computing, vol. 13, Art. no. 12, Jan. 2025. DOI: 10.1007/s44227-024-00055-8.

[29] C. Oredola and A. Ashraf, “A systematic mapping study on SDN controllers for enhancing security in IoT networks,” in Proc. 50th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), 2024, pp. 317–324. DOI: 10.1109/SEAA64295.2024.00056.

[30] M. Mossie and A. Seid, “Software defined networking based network traffic classification using machine learning techniques,” Scientific Reports, vol. 14, Art. no. 70983, 2024. DOI: 10.1038/s41598-024-70983-6.

[31] X. Pei, P. Sun, Y. Hu, D. Li, B. Chen, and L. Tian, “Enabling efficient routing for traffic engineering in SDN with deep reinforcement learning,” Computer Networks, vol. 241, p. 110220, Mar. 2024. DOI: 10.1016/j.comnet.2024.110220.

[32] K. Wang, Y. Fu, X. Duan, T. Liu, and J. Xu, “Abnormal traffic detection system in SDN based on deep learning hybrid models,” Computer Communications, vol. 216, pp. 183–194, Feb. 2024. DOI: 10.1016/j.comcom.2023.12.041.

[33] Y. Song, T. Feng, C. Yang, X. Mi, S. Jiang, and M. Guizani, “IS2N: Intent-Driven security software-defined network with blockchain,” IEEE Network, vol. 38, no. 3, pp. 118–127, May 2024. DOI: 10.1109/MNET.138.2200539.

[34] M. Ye, L. Huang, X. Wang, Y. Wang, Q. Jiang, and H. Qiu, “A new intelligent cross-domain routing method in SDN based on a proposed multiagent reinforcement learning algorithm,” Int. J. Intell. Comput. Cybern., vol. 17, no. 2, pp. 330–362, 2024. DOI: 10.1108/IJICC-09-2023-0269.

[35] H. Chen, P. Chen, B. Wang, X. Yu, X. Chen, D. Ma, and Z. Zheng, “Graph neural network based robust anomaly detection at service level in SDN driven microservice system,” Computer Networks, vol. 239, p. 110135, Feb. 2024. DOI: 10.1016/j.comnet.2023.110135.

[36] A. A. B. Alashhab, M. Aljawarneh, I. H. Haddad, M. A. Awad, T. A. Ali-Aldeen, M. A. Alsalem, and S. M. Alsaleh, “A systematic literature review on machine learning and deep learning approaches for detecting DDoS attacks in software-defined networking,” Sensors, vol. 23, no. 9, Art. no. 4441, May 2023. DOI: 10.3390/s23094441.