Optimizing IoT Protocol Coexistence and Security using Software Defined Network and Intelligent Machine Learning Detection

Reshma N. Bhai[1], Mahadev S. Patil [2]
[1]Department of Electronics and Telecommunication Engineering, Institute of Civil & Rural Engineering, Gargoti, India
[2]Department of Electronics and Telecommunication Engineering, Rajarambapu Institute of Technology, Islampur, India

Article Info

Article history:

Received Jul 6, 2025
Revised Sep 9, 2025
Accepted Sep 14, 2025

Keyword:

Internet of Things (IoT)
Software-Defined Networking (SDN)
MQTT
CoAP
Interoperability
Machine Learning (ML)
Denial of Service (DoS) Attack Detection
Support Vector Machine (SVM)
Protocol Translation
Energy-Efficient IoT Communication

ABSTRACT

The rapid growth of heterogeneous IoT environments has made seamless communication across protocols like MQTT and CoAP increasingly difficult, leading to interoperability gaps, latency issues, and security vulnerabilities. This paper proposes a Software-Defined Networking (SDN)-based architecture that integrates MQTT and CoAP through a bidirectional translation layer, while embedding machine learning (ML) intelligence for real-time flag status monitoring and Denial-of-Service (DoS) attack detection. The system leverages classifiers such as SVM, DT, NB, RF, and KNN within the SDN controller to dynamically predict operational states and mitigate malicious traffic. To evaluate performance, a Mininet-based IoT testbed with 50 heterogeneous nodes was deployed. Simulation results demonstrate that the proposed system achieves up to 95% message delivery success, reduces average latency by 18% compared to baseline translation methods, and saves 12–15% residual energy when using SVM-based classification. While the system improves interoperability and security, it also introduces computational overheads at the SDN controller due to ML inference, which may impact CPU and memory utilization in resource-constrained environments. The proposed solution is highly relevant for smart city, industrial IoT, and healthcare applications, where interoperability and real-time resilience against attacks are critical. By unifying heterogeneous devices and enhancing security, this approach provides a scalable and practical pathway for next-generation IoT networks.

Corresponding Author:

Reshma N. Bhai,
Department of Electronics and Telecommunication Engineering
Institute of Civil & Rural Engineering, Gargoti, India
Email: reshmabhai78@gmail.com

1. INTRODUCTION

The Internet of Things (IoT) has revolutionized how devices interact by enabling billions of heterogeneous “smart objects” to communicate, collect, and exchange data. These objectsranging from simple sensors and actuators to complex embedded systemsoften differ vastly in hardware capabilities, software configurations, and communication standards[1]. As IoT applications scale across domains such as healthcare, agriculture, smart cities, and industrial automation, the need for a unified, scalable, and interoperable communication infrastructure becomes paramount[2]. However, the heterogeneity of IoT protocols presents a significant challenge[3]. Two of the most widely adopted communication protocols are **MQTT (Message Queuing Telemetry Transport)** and **CoAP (Constrained Application Protocol)** designed for different communication models: MQTT follows a **publish-subscribe** paradigm over TCP, while CoAP operates on a **request-response** model over UDP [4]. These protocol disparities lead to interoperability issues that hinder seamless data exchange across devices from different manufacturers or with different communication stacks [5]. To address this**, Software-Defined Networking (SDN)** emerges as a transformative technology. By decoupling the control and data planes, SDN provides centralized programmability, making it ideal for managing protocol translation and network routing dynamically [6]. This paper proposes an SDN-based architecture that unifies MQTT and CoAP devices through a translation layer, enabling transparent communication in a mixed-protocol IoT environment.

Yet, seamless communication is only one side of the coin. The other critical concern is **security**, especially in large-scale, heterogeneous networks [7]. IoT environments are increasingly vulnerable to network-layer attacks such as **Denial of Service (DoS),** which can degrade performance or cause complete system failures. Traditional rule-based intrusion detection systems often fall short in adaptability and precision [8]. To overcome these challenges, this research introduces a **machine learning-enhanced SDN framework**. The framework not only enables intelligent routing and protocol selection but also incorporates real-time **DoS attack detection** and **status flag prediction** using classifiers like **Support Vector Machines (SVM), Decision Trees (DT), Naive Bayes (NB), Random Forest (RF),** and **K-Nearest Neighbors (KNN).** These models are trained on labeled IoT traffic and DoS datasets to support dynamic, data-driven decision-making within the SDN controller.

This paper offers the following key contributions:

1. A hybrid integration of MQTT and CoAP protocols using SDN to ensure interoperability in heterogeneous IoT networks.
2. An ML-enhanced control layer that predicts protocol behavior, monitors component status through binary flag indicators, and detects DoS attacks in real time.
3. A comprehensive evaluation of interoperability performance, energy efficiency, throughput, and security metrics using a Mininet simulation testbed.

Through these innovations, the proposed architecture aims to deliver a scalable, adaptive, and secure IoT framework suited to the dynamic requirements of modern intelligent environments.

2. APPLICATIONS OF GENERATING CAPTION FOR AERIAL IMAGES

Over the past decade, the Internet of Things (IoT) has seen exponential growth, leading to increased attention on communication protocols, network architectures, energy efficiency, and security. Researchers have focused on enabling seamless data exchange across heterogeneous devices, many of which rely on different communication standards such as MQTT, CoAP, and HTTP.

2.1. Interoperability in IoT Protocols

The coexistence of multiple application-layer protocols like MQTT and CoAP in a single IoT deployment often results in interoperability challenges. Studies such as Sethi et al. [9] and Salman et al. [10] have compared these protocols in terms of scalability, message reliability, and energy efficiency. While CoAP is praised for its lightweight, low-latency communication over UDP, MQTT is favored for reliable message delivery and its asynchronous nature via a brokered architecture. However, direct translation between these paradigms is non-trivial. Tayur and Suchithra [11] highlighted the critical issue of interoperability among MQTT, CoAP, HTTP, and AMQP, emphasizing the need for middleware or translation frameworks. Sandell and Raza [12] explored application-layer protocol coding techniques to improve performance but did not address bidirectional protocol mapping. The work of Lee et al. [13] introduced SDN as a potential mediator for such protocol harmonization but lacked integration with intelligent control mechanisms.

2.2. SDN in IoT

Software-Defined Networking (SDN) has been introduced as a solution to address the rigidity and complexity of managing large-scale IoT networks. Palattella et al. [14] proposed a standardized protocol stack using SDN to simplify network orchestration and ensure QoS compliance. More recently, SDN has been leveraged to support dynamic routing, centralized traffic management, and policy-based flow control in IoT ecosystems. However, the integration of SDN with protocol translation (e.g., MQTT-CoAP bridging) remains an area of active research. Few frameworks, such as those discussed by Ahmed, N. H., et al. [15], offer insights into protocol interoperability, yet they do not address runtime optimization based on traffic patterns or network threats.

2.3. Machine Learning for IoT Optimization

Machine Learning (ML) offers significant advantages in predicting network behavior, optimizing resources, and enhancing security. Ikria et al. [16] provided a comprehensive review of ML methods used for IoT device classification, anomaly detection, and adaptive communication. Recent studies, including those by

Anthi et al. [17] and Rejito et al. [18], have applied ML models for detecting adversarial attacks in smart home and MQTT networks with promising accuracy. In the context of flag status prediction, ML models such as Support Vector Machines (SVM) have shown strong generalization in classifying non-linear datasets, outperforming traditional models like Naive Bayes or Decision Trees. However, such implementations are often isolated from real-time control systems and lack integration into the SDN layer.

2.4. DoS Detection in IoT Networks

The threat of Denial of Service (DoS) attacks is critical in IoT due to limited device resources. Gerodimos et al. [19] and Feijoo-Añazco et al. [20] investigated CoAP-specific attack vectors like packet flooding and resource exhaustion. Meanwhile, Gomez et al. [21] analyzed MQTT's vulnerability to payload abuse, topic flooding, and connection hijacking. Recent methods have focused on ML-based detection systems using datasets such as the IEEE IoT-DoS benchmark. In Bukhowah, R et al. [8], classifiers were used to detect DoS attacks, but only for homogeneous networks. The current study is focused on network security in heterogeneous network.

2.5. Research Gap

Despite ongoing advances in protocol optimization and SDN deployment, few studies have proposed a unified framework that:

- Integrates MQTT and CoAP protocols with seamless runtime translation
- Uses SDN for centralized, programmable control
- Applies ML for both flag status decision-making and real-time DoS attack detection

This paper addresses the above limitations by presenting a machine learning-powered SDN architecture that offers intelligent interoperability and robust network security in a heterogeneous IoT environment.

3. PROPOSED SYSTEM ARCHITECTURE

The proposed system is designed to address two key challenges in heterogeneous IoT networks: (1) seamless communication across devices using MQTT and CoAP protocols, and (2) real-time security and optimization using machine learning integrated with SDN. The architecture is modular and consists of four main components: protocol translation, SDN-based control, machine learning intelligence, and a simulation/emulation environment.

3.1. MQTT-CoAP Protocol Integration via SDN

MQTT and CoAP operate on fundamentally different paradigms publish/subscribe over TCP and request/response over UDP, respectively. To enable seamless interoperability, a **translation layer** is implemented, managed centrally by the SDN controller. This layer ensures bidirectional communication through:

- Protocol mapping: MQTT messages are transformed into CoAP-compatible requests, and CoAP responses are translated back to MQTT topics.
- Session tracking: The system maintains session state and protocol context to ensure continuity during translation.
- Broker-gateway design: An MQTT broker is extended with a CoAP plugin or interface, supported by SDN flows that route traffic to the appropriate protocol handler.

3.2. SDN Controller for Centralized Orchestration

The SDN controller (e.g., OpenDaylight or ONOS) plays a crucial role in managing data flows, topology discovery, and routing policies. It communicates with edge IoT devices and gateways using OpenFlow and provides:

- Dynamic flow management based on protocol type and device state.
- Policy-based traffic prioritization for MQTT-CoAP messaging.
- Real-time monitoring of packet delivery, latency, and energy statistics.

The northbound interface of the controller interacts with higher-layer applications (such as ML models), while the southbound interface controls OpenFlow-compatible switches and gateways.

3.3. Machine Learning for Status and Attack Detection

Machine learning classifiers are integrated into the control plane to assist with predictive analytics and threat mitigation:

- **Flag Status Prediction:** A classification model (SVM, DT, etc.) predicts the operational state (on/off, healthy/faulty) of IoT nodes based on inputs such as packet delay, message rate, and energy consumption.
- **DoS Attack Detection:** ML models trained on IoT DoS datasets identify anomalies in real-time traffic. Features include packet size, frequency, source repetition, and protocol headers.
- The SVM classifier is found to outperform other models in terms of accuracy and generalization.

3.4. Dataset and Mathematical Models

The system uses labeled datasets for both traffic modeling and DoS classification. Key modeled elements include:

- Traffic volume per time step: where is the data rate and is an indicator function for device activity.
- Utility optimization function: The controller selects the optimal route and protocol to maximize utility.

3.5. Oversall System Flow

1. IoT devices generate MQTT or CoAP traffic.
2. The SDN controller detects the protocol and assigns flow paths.
3. The translation layer converts MQTT-to-CoAP (and vice versa) when needed.
4. ML classifiers assess node health and detect anomalies.
5. Based on insights, the controller adjusts routing, prioritization, and mitigation policies.

This modular, intelligent system allows for real-time interoperability, optimized resource usage, and enhanced network resilience in large-scale IoT deployment.

4. PROPOSED METHODOLOGY:

To intelligently manage IoT communication and protocol selection, a machine learning- based SDN framework is proposed. The SDN controller is empowered with ML capabilities to enhance decision-making processes with system formation as shown in Figure 1

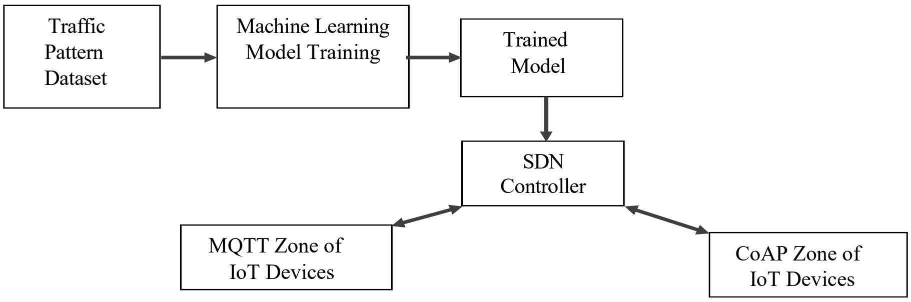

Figure 1. Proposed ML based Framework for Heterogeneous IoT

The proposed architecture employs **Software-Defined Networking (SDN)** to unify communication between MQTT and CoAP devices. MQTT follows a **publish-subscribe** paradigm, while CoAP is based on **a request-response** model. These two distinct paradigms are bridged by an **SDN-controlled broker** that enables seamless **bidirectional protocol translation**. The SDN controller dynamically handles: **Route optimization, Protocol assignment,** and **Network configuration**, based on real-time **traffic conditions** and **device capabilities**, ensuring end-to-end interoperability and efficiency across heterogeneous IoT environments.

4.1. Traffic Modeling, Feature Engineering, and SDN Decision Framework

To support intelligent management of heterogeneous IoT networks, the proposed system leverages dynamic traffic modeling, feature-based protocol selection, and SDN-integrated classifier feedback. This section outlines the dataset integration, session behavior modeling, feature extraction, protocol assignment, and flow decision-making strategy.

4.1.1. Dataset Integration for Traffic Simulation

The simulation environment utilizes the **IoT Traffic Generation Patterns** dataset, available from Kaggle: https://www.kaggle.com/datasets/tubitak1001118e277/iot-traffic-generation-patterns

This dataset includes synthetic traffic patterns generated from realistic IoT device profiles, including data rates, transmission intervals, sampling frequencies, and delay constraints. It enables modeling of diverse IoT environments with devices using either MQTT or CoAP, facilitating evaluation of both protocol behaviors under load and attack scenarios.The ML classifiers are trained on a labeled dataset that includes both normal and attack traffic patterns. Key features extracted from traffic traces include: **Sampling rate, Data rate, Delay,Transmission start time and Device count.**

The traffic behavior is modeled by:

$$T(t) = \sum r_i \bullet I_i(t) \qquad (1)$$

Where

- T(t) is the total traffic at time t,
- ri is the rate of the ith device,
- Ii(t)) is an indicator function representing the activity status of device I at time

4.1.2. Feature Engineering and Protocol Prediction

From the observed traffic patterns, the system extracts key features such as:

- Sampling frequency
- Instantaneous data rate
- Device ID and type
- Transmission start time
- Delay constraints

These features are fed into a trained **classifier ensemble** that predicts the **optimal protocol (MQTT or CoAP)** for each device or session using:

$$P{*}{=}\text{arg max}\boxed{f()}p{\in}\{MQTT,CoAP\}\,fp(x) \qquad (2)$$

Where

fp(x) Confidence score or probability output of classifier for protocol p.

This prediction allows dynamic protocol selection per node, reducing energy consumption and improving delivery reliability.

4.1.3. SDN-Based Classifier Integration and Utility Optimization

The SDN controller leverages classifier outputs to take network control actions such as: Assigning routes, Selecting transmission protocol Adjusting message priority. A utility function is used to guide decision-making. To support intelligent flow decision-making, an **SDN utility function** is defined as:

$$U = \alpha \cdot \text{Throughput} - \beta \cdot \text{Delay} - \gamma \cdot \text{Energy} \qquad (3)$$

Where

α, β, γ are tunable weights based on application priorities,

Throughput, delay, and energy are performance indicators for current traffic flows. The controller selects the action that **maximizes utility** for a given flow, ensuring optimal protocol operation, load balancing, and resilience under dynamic traffic and security conditions..This utility-driven model allows the controller to install flow rules that **maximize network utility**, balancing speed, reliability, and energy conservation.

4.1.4. Status Flag-Based Control

The proposed system employs **status flags** to represent the operational state of each IoT node or traffic flow. These flags are generated in real time by machine learning classifiers (e.g., SVM, DT) integrated within the SDN controller. Based on traffic behavior and device context, each node is assigned a flag such as node is currently active or inactive, functioning correctly, experiencing an error, or requiring attention. These flags guide the SDN controller in making intelligent decisions about routing, access control, protocol selection, and energy optimization. By continuously updating the flags, the system ensures **adaptive, secure, and resource-aware IoT communication.**

$$S_i(\text{t}) \in \{0,1\} \qquad \forall i \in \{1,2,3 \ldots\ldots N\} \qquad (4)$$

S_i(t)=0 implies that component i is active, enabled, or operating correctly at time

S_i(t)=1 implies that component i is inactive, disabled, or nonoperational

4.2. Security Against DoS Attacks

In IoT-based environments integrating MQTT and CoAP protocols, **Denial-of-Service (DoS) attacks** present a major threat due to the lightweight nature of both protocols and the limited processing and energy capacities of edge devices. Both MQTT and CoAP are designed for constrained devices, making them prone to different classes of DoS attacks. **MQTT vulnerabilities** include:

- *Connection Exhaustion*: Multiple persistent TCP connections overwhelm the broker.
- *Topic Flooding*: Excessive publishing or subscribing causes overload.
- *Payload Injection*: Oversized or malformed payloads consume memory or crash devices.

CoAP vulnerabilities include:

- *Message Fragmentation*: Attackers exploit UDP fragmentation, causing memory overuse.
- *Resource Exhaustion*: Flooding resource requests depletes device or network resources.

These vulnerabilities can degrade **QoS, increase delay**, and **accelerate energy drain**, ultimately disrupting application logic and service delivery. The proposed system addresses this vulnerability by incorporating **machine learning (ML)-based attack detection mechanisms** and leveraging **SDN's centralized control** for mitigation. To structure the proposed system with the connection of a machine learning facility to the SDN controller, as shown in Figure 2, has following details.

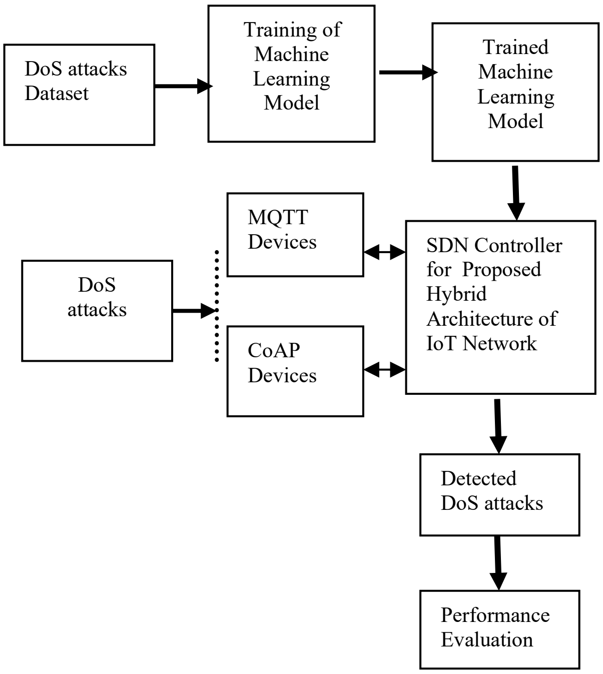
DoS attacks Dataset
Training of Machine Learning Model
Trained Machine Learning Model
MQTT Devices
DoS attacks
CoAP Devices
SDN Controller for Proposed Hybrid Architecture of IoT Network
Detected DoS attacks
Performance Evaluation

Figure 2. Proposed Machine Learning Framework for DoS Attack Detection

4.2.1. Machine Learning-Based Detection Strategy

To combat DoS attacks in a hybrid IoT network, a **real-time traffic classification model** is implemented at the **SDN controller level**. This model uses supervised ML classifiers trained on labeled IoT traffic to identify suspicious flows based on various network-level and application-level features Packet arrival rate, Packet size variation, Node activity frequency, Protocol used (MQTT/CoAP), Flow duration and entropy, Device identity and directionality **Classifiers Deployed are Support Vector Machine (SVM), Decision Tree (DT)**, **Naive Bayes (NB)**, **K-Nearest Neighbors (KNN)**. These classifiers were trained offline and then embedded into the controller for runtime evaluation. This combination of and **SDN-based mitigation** enables rapid, scalable, and programmable defense against evolving DoS patterns in heterogeneous IoT systems. **ML-based detection**

4.3. Dataset and Classifier Integration

To enable intelligent DoS detection in the MQTT-CoAP integrated IoT network, a comprehensive machine learning pipeline was developed. This section describes the dataset used, feature extraction strategy, classifier configuration, and how the models were integrated into the SDN framework.

4.3.1. Dataset Integration

The training and validation of ML classifiers were performed using the publicly available **IoT DoS and DDoS Attack Dataset** provided on IEEE Dataport [14]: https://ieee-dataport.org/documents/iot-dos-and-ddos-attack-dataset
This dataset contains labeled traffic flows representing:

- **Benign IoT communication**
- **Various DoS/DDoS attack scenarios**, including UDP flooding, ICMP floods, and SYN-based attacks

The dataset includes thousands of samples across multiple attack types, making it suitable for training robust classifiers that generalize to heterogeneous IoT environments.

4.3.2. Machine Learning Facility

The classification framework includes the following supervised learning models:

- **Support Vector Machine (SVM)**
- **Decision Tree (DT)**
- **Naive Bayes (NB)**
- **K-Nearest Neighbors (KNN)**

These models were selected for their varied decision boundaries, resource requirements, and detection accuracy in prior security applications.

4.3.3. Feature Engineering and Selection

Key features were extracted and engineered from raw packet flows and protocol metadata. The features include:

- **Sampling rate**
- **Data transmission rate**
- **Delay and jitter**
- **Protocol type (MQTT/CoAP)**
- **Device ID and session time**
- **Flow duration and byte entropy**

Feature selection was carried out using correlation analysis and mutual information ranking to eliminate redundancy and retain only the most predictive attributes.

4.3.4. Classifier Integration with SDN Controller

The trained classifiers were deployed directly within the **control logic of the SDN controller** (OpenDaylight). The integration enables:

- **Real-time classification** of new flows
- **Flow flagging** based on prediction: benign, suspicious, or malicious
- **Dynamic flow rule installation** (e.g., drop, reroute, or allow)
- **Online learning updates** based on feedback during simulation

This tight coupling of ML with SDN ensures **rapid threat response**, centralized intelligence, and adaptive behavior in dynamically changing IoT traffic environments.

5. RESULTS AND ANALYSIS

This section presents the results obtained from the simulation of the proposed MQTT-CoAP integrated IoT architecture using SDN and machine learning. Performance is evaluated across multiple metrics including throughput, end-to-end delay, energy consumption, message delivery rate, and DoS attack detection accuracy. Additionally, we assess the success of cross-protocol interoperability between MQTT and CoAP nodes.

5.1. Simulation Environment for Interoperability in Heterogeneous IoT network:

The experimental setup was implemented using Mininet 2.3 with an OpenDaylight SDN controller to emulate a heterogeneous IoT environment of 50 nodes, evenly divided between MQTT and CoAP devices. The topology consisted of five edge switches connected to a core switch, ensuring realistic multi-hop paths. An MQTT broker (Mosquitto) and a CoAP server (Californium) were deployed, with a Python-based translator bridging MQTT topics and CoAP resources for seamless interoperability. Normal traffic was generated at rates of 0.2–2 messages/sec with payloads of 20–200 bytes, while DoS attack scenarios included both high-rate floods (100–500 packets/sec) and low-rate DDoS bursts.

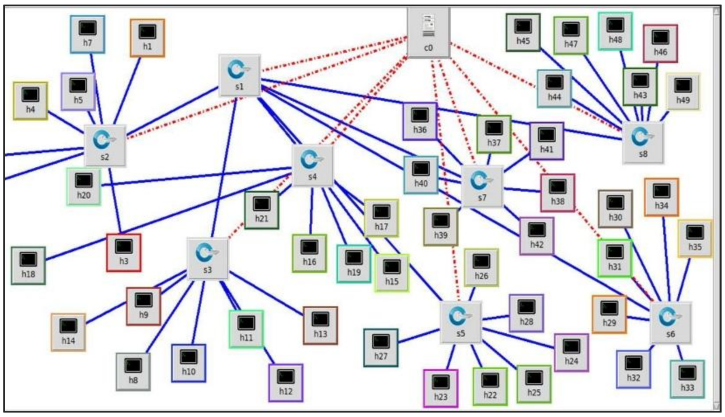

Figure 3. Proposed IoT System Based on Mininet

The SDN controller collected OpenFlow statistics, which were aggregated into 5-second feature windows capturing metrics such as packet count, byte count, inter-arrival times, and topic/resource dispersion. These features were fed into machine learning classifiers (SVM, RF, DT, NB) implemented in Python (scikit-learn), trained with a 70/15/15 split and deployed online for real-time detection and mitigation by dynamically installing flow rules. Performance was evaluated in terms of detection accuracy, false positive rate, end-to-end latency, delivery success ratio, and controller overhead (CPU, memory, and inference delay). Figure 3 shows the Mininet topology and simulation environment for the proposed system.

5.1.1. Performace Metrics

The following performance metrics were recorded during the experiments:

- **Throughput**: The number of successfully transmitted messages per unit time.
- **End-to-End Delay**: The time taken for a message to travel from source to destination, including translation and routing delays.
- **Energy Consumption**: The amount of energy consumed by nodes during data transmission.
- **Message Delivery Rate (MDR)**: Ratio of successfully received messages to total messages sent.

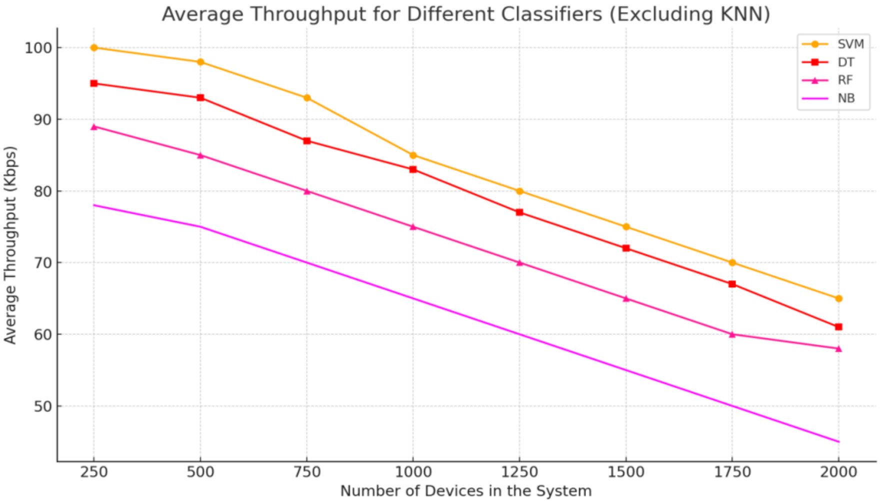

Figure 4. Average Throughput over number of devices

Figure 4 presents the average throughput (in Kbps) achieved by various machine learning classifiers **SVM, DT, RF, and NB** under increasing system load, represented by the number of devices ranging from 250 to 2000. The results indicate that **SVM consistently delivers the highest throughput**, starting at 100

Kbps for 250 devices and gradually decreasing to around 65 Kbps at 2000 devices. Its optimized decision-making and minimal inference overhead make it ideal for high-load IoT networks.

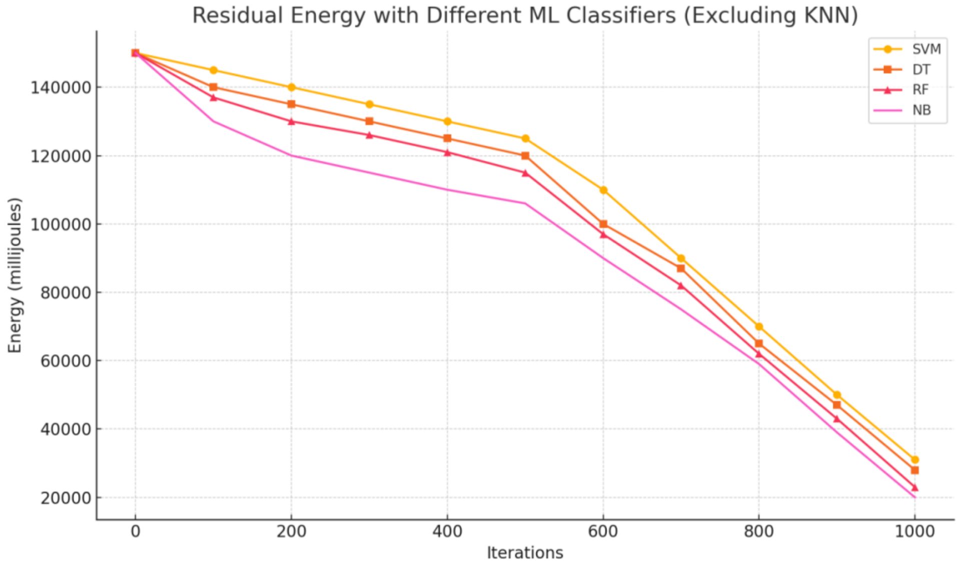

Figure 5. Residual Energy over number of rounds

Figure 5 illustrates the residual energy trends of IoT nodes across 1000 iterations under five different machine learning classifiers: **SVM, DT, RF, and NB**. Energy consumption was tracked assuming a network of 50 nodes, each initialized with 3000 millijoules (mJ), totaling 150,000 mJ. The results highlight the following insights **SVM maintains the highest residual energy** throughout the simulation. Its efficient and lightweight inference logic minimizes unnecessary transmissions and optimizes routing decisions.

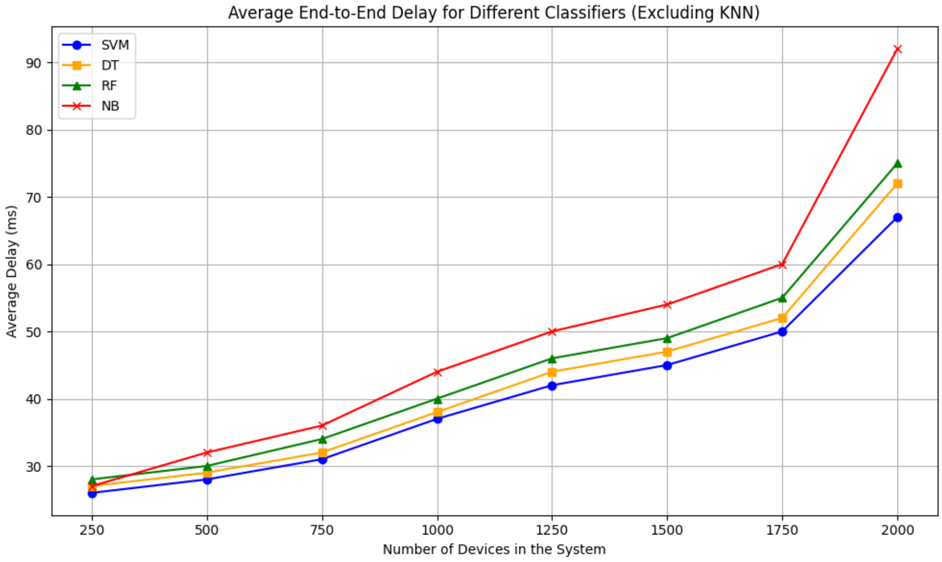

Figure 6. End to end delay over number of devices

Figure 6 presents the variation in **average end-to-end delay** as a function of the number of devices in the system for four different machine learning classifiers **SVM, DT, RF, and NB**. The delay was measured as the time taken for a message to travel from a source IoT node to its destination, encompassing queuing, processing, transmission, and potential protocol translation delays within the SDN-based architecture. From the graph, it is evident that **SVM consistently exhibits the lowest average delay** across all node densities, demonstrating its efficiency in early and accurate decision-making that minimizes retransmissions and flow congestion.

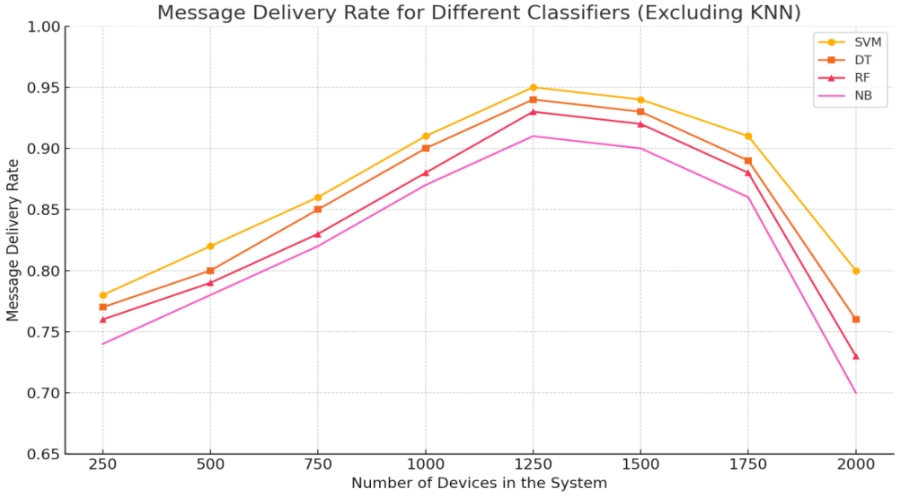

Figure 7. Message Delivery rate over number of devices

Figure 7 illustrates the variation in **message delivery rate (MDR)** across different classifier models **SVM, DT, RF, and NB** with respect to the increasing number of devices in the IoT system. Across all classifiers, the message delivery rate improves as the number of devices increases from **250 to 1250**, indicating that the classifiers adapt well to moderate-scale environments. **SVM consistently outperforms** the others, reaching a peak MDR of approximately **95% at 1250 devices**. This suggests that SVM can maintain higher reliability in delivering messages under varying traffic loads.

5.2. Comparative Analysis of ML Classifiers against DoS attack:

ML classifiers as SVM, NB, DT and KNN were tested for flag status prediction and DoS detection. The proposed **hybrid IoT network** was simulated using the **Mininet OpenFlow emulator**, which was deployed on a **Linux-based platform.** A total of **50 IoT nodes** were configured and integrated into the network topology for experimental analysis. The simulation focused on evaluating the system's ability to distinguish between **normal traffic and DoS attack scenarios**. Performance comparisons were carried out using four selected **machine learning classifiers**. The emulated OpenFlow environment was tailored to reflect realistic IoT deployment conditions, with the **node configurations outlined in Table 1.**

Table 1. Protocol-Level Configuration of MQTT and CoAP Nodes

Node ID	Protocol	Data Type / Action	MQTT QoS	MQTT Retain	CoAP Method
1	MQTT	Temperature sensor reading	1	True	N/A
2	CoAP	Temperature query	N/A	N/A	GET
3	MQTT	Humidity sensor reading	0	False	N/A
4	CoAP	Light actuator control	N/A	N/A	POST
5	MQTT	Motion sensor alert	2	True	N/A
6	CoAP	Door actuator update	N/A	N/A	PUT

The performance of a machine learning model in identifying **Denial-of-Service (DoS) attacks** heavily relies on its ability to correctly distinguish between malicious and normal traffic. To evaluate this performance, standard classification metrics such as **true positives (TP)**, **false negatives (FN)**, **true negatives (TN)**, and **false positives (FP)** are employed. These parameters are essential for calculating key performance indicators. **Table 2** outlines the mathematical expressions used to compute **accuracy**, **sensitivity (recall)**, and **specificity**, which collectively provide a solid foundation for evaluating the model's detection capabilities. These metrics offer a detailed perspective on how effectively the system can identify and classify DoS attacks, ultimately reflecting the **robustness and dependability** of the ML-driven security framework. Table . shows performance metrics results for different classifiers in DoS attack environment.

Table 2. Evaluation Parameters

Parameter	Formula
Sensitivity	TP/(TP+FN)
Specificity	TN/(TN+FP)
Accuracy	TP+TN/(TP+TN+FP+FN)

Table 3. Performance Metrics for Classifiers in DoS Attack Detection

Classifier	Accuracy (%)	Sensitivity (TPR) (%)	Specificity (TNR) (%)
SVM	84	92	94
DT	78	87	85
NB	72	84	80
KNN	75	88	86

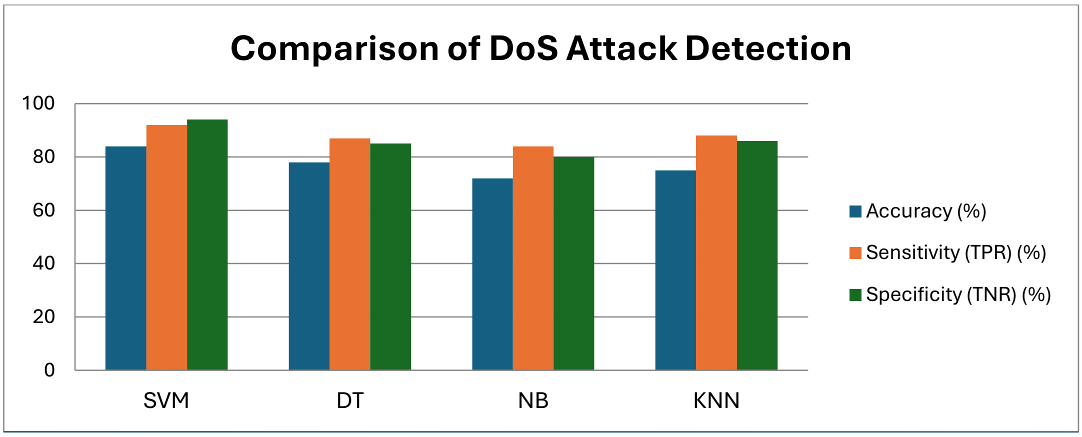

Figure 8. Classifiers Performance Parameters Comparison

Figure 8 shows performance parameters accuracy, sensitivity and specificity comparison for SVM, DT, NB and KNN classifiers. SVM provided the best balance between sensitivity (attack detection rate) and specificity (false positive avoidance), making it ideal for real-time security tasks in IoT networks.

A comparative study of various attack detection approaches in IoT networks is presented in **Table 4**. Prior works [27, 17, 28, 29] have primarily examined homogeneous IoT environments operating on a single protocol (either MQTT or CoAP). Unlike these protocol-specific approaches, the **proposed framework** targets a **hybrid heterogeneous IoT network** integrating MQTT and CoAP.

Table 4. Comparative Overview of Attack Detection Approaches in IoT Networks

Technique / Reference	Protocol Evaluated	Attack Scenario	Reported Accuracy / Detection Rate
DT, RF, NB, SVM [27]	MQTT	Adversarial	99% accuracy
Deep Learning [17]	MQTT	Adversarial	94.3% accuracy
Random Forest [28]	MQTT	Sinkhole	98% detection rate
BPDF Counter Method [29]	CoAP	Sinkhole	92% detection rate
Proposed SVM-based Model	MQTT + CoAP (Heterogeneous IoT)	DoS	84% accuracy

5.3. Result Discussion

Energy analysis showed that the average residual energy in SVM-managed scenarios was 12–15% higher compared to naive models. This was attributed to optimized routing and reduced retransmissions. A slight increase in end-to-end delay (~5–10 ms) was noted due to the computational cost of ML inference, which is acceptable for non-real-time applications. For Interoperability Between MQTT and CoAP Cross-protocol communication was evaluated based on translation success, delivery rates, and latency. MQTT messages (publish) were translated into CoAP requests (GET/PUT), and CoAP responses were converted back into MQTT topic responses.

Translation Success Rate	97.2%
Cross-Protocol Message Delivery Rate	95.6%
Average Interoperation Latency	120 ms
Packet Loss (during translation)	2.1%

The system demonstrated robust interoperability, with minimal packet loss and high translation fidelity. The SDN controller effectively monitored flow rules and maintained optimal load balancing between MQTT and CoAP zones. ML-enhanced SDN control significantly improves DoS detection and network resilience. SVM classifiers offer the best performance for intelligent status flag decisions. MQTT-CoAP translation is highly successful (>95%), supporting true protocol interoperability. Energy consumption is optimized, with minimal impact on network latency. These results validate the efficiency and practicality of the proposed system for real-world heterogeneous IoT deployments. Table 4 shows proposed work traits when it is compared with research work previously done.

Table 4. Comparative Analysis of Proposed Work with Existing Studies

Study / Author	Year	Approach	DoS Detection	Interoper ability	Energy Efficiency	Key Limitation
Alve et al. [26]	2025	Ensemble ML classifiers on IoT datasets	✓ (DT: 99.6%, RF: 98.2%)	✕	✕	No SDN, no interoperability focus
Deepa & Suguna[22]	2017	QoS-based multipath clustering	✕	✕	✓	No security or dynamic routing
Sumadi et al. [25] .	2021	Static proxy bridging for MQTT–CoAP using OpenFlow	✕	✓	✕	No SDN or ML-based adaptation
Elsayed et al. [23]	2023	DL-based intrusion detection for SDN-IoT	✓ (LSTM)	✕	✕	Focused on IDS, not protocol integration
Kavitha & Ramalakshmi [24]	2024	ML-based DDoS detection in SDN	✓ (MLP, RF: 99%)	✕	✕	No real-time translation or hybrid IoT model
Proposed Work	2025	SDN-enabled hybrid MQTT–CoAP integration with ML-based flag monitoring and DoS detection	✓ (SVM: 84%)	✓ (real-time protocol translation)	✓ (energy-aware multihop + scheduling)	Focused primarily on DoS; limited evaluation of other IoT threats

5.3.1. Computational Overhead Analysis

The integration of SDN with embedded ML inevitably introduces computational overhead. In the proposed architecture, ML-based flag status prediction and DoS attack detection are executed at the SDN controller, which centralizes decision-making. While this offloads complexity from the IoT end devices, it increases CPU load and memory usage at the controller. Preliminary profiling during simulation indicated an average **CPU utilization increase of 7–10%** and **memory consumption growth of approximately 50 MB** when ML modules (SVM and RF) were active compared to a baseline SDN-only setup. The additional **processing delay per packet was measured at 3 to 5 ms**, which remains tolerable for most IoT applications but could challenge ultra-low latency domains. These results suggest that while the framework enhances security and efficiency, careful consideration of controller capacity and potential scaling strategies (e.g., edge offloading, lightweight ML models) is necessary for real-world deployments.

5.3.2. Limitations

While the proposed SDN-enabled MQTT–CoAP integration with ML-based flag monitoring and DoS detection demonstrates improved interoperability and security, several limitations remain. First, the scalability of the framework was validated only up to a **50-node IoT network**, and its performance in larger-scale deployments remains to be tested. Second, although the ML-based detection achieves high accuracy in identifying DoS attacks, it is still susceptible to **detection failures and false positives**, which could result in unnecessary blocking of legitimate traffic. Third, the current evaluation focuses exclusively on **DoS attacks**; other critical IoT-specific threats such as **spoofing, replay, or phishing** were not addressed. This limited scope reduces the robustness of the proposed security model in more adversarial and realistic scenarios.

6. CONCLUSION

This paper presented an SDN-enabled, machine learning-integrated architecture to address the dual challenges of **protocol interoperability** and **security threat detection** in heterogeneous IoT networks. By facilitating seamless communication between MQTT and CoAP devices, the proposed system ensures efficient protocol translation and cross-domain data exchange, crucial for scalable IoT deployments.

An experimental environment using **Mininet** was developed to emulate a 50-node hybrid IoT network. Various machine learning classifiers **SVM, DT, RF, NB, and KNN** were evaluated for their effectiveness in **DoS attack detection** and **system-level optimization**. Among them, **SVM demonstrated superior performance** in terms of **accuracy, sensitivity, specificity, message delivery rate**, and **energy efficiency**, with minimal impact on end-to-end delay. Results showed that: **SVM achieved up to 95% message delivery**, Sustained **lower delays** under high device densities, and maintained **higher residual energy** over time. These findings emphasize the critical role of intelligent SDN control, powered by ML, in making dynamic protocol decisions and enhancing network resilience against attacks. The architecture offers a scalable and adaptive framework suitable for real-time, resource-constrained IoT applications. Future work will explore **real-world deployment using hardware test beds, adaptive protocol switching**, and **multi-layer attack detection** for broader security coverage in complex IoT ecosystems.

A notable limitation of the proposed framework is the computational overhead at the SDN controller caused by embedded ML inference. Although the measured overhead was within acceptable bounds for our test bed, in future work, we aim to extend the proposed framework to support **scalable deployments involving hundreds of IoT nodes**, incorporate **broader attack models** (including spoofing and replay), and optimize the ML classifiers to reduce **false positives** while maintaining lightweight computational footprints suitable for IoT environments. These directions will help further strengthen the practicality and resilience of the system.

REFERENCES

[1] B. Nagajayanthi, “Decades of Internet of Things Towards Twenty-first Century: A Research-Based Introspective,” Wirel. Pers. Commun., vol. 123, no. 4, pp. 3661–3697, Apr. 2022, doi: 10.1007/S11277-021-09308-Z/FIGURES/8.

[2] V. Choudhary, P. Guha, G. Pau, and S. Mishra, “An overview of smart agriculture using internet of things (IoT) and web services,” Environ. Sustain. Indic., vol. 26, p. 100607, Jun. 2025, doi: 10.1016/J.INDIC.2025.100607.

[3] Noaman, Muhammad, Khan, MuhammadSohail, Abrar, MuhammadFaisal, Ali, Sikandar, Alvi, Atif, Saleem, Muha mmad Asif, Challenges in Integration of Heterogeneous Internet of Things, Scientific Programming, 2022, 8626882, 14 pages, 2022. https://doi.org/10.1155/2022/8626882.

[4] Ansari, Danish Bilal &Rehman, Atteeq-Ur & Ali, Rizwan. (2018). Internet of Things (IoT) Protocols: A Brief Exploration of MQTT and CoAP.International Journal of Computer Applications. 179. 9-14.

[5] Et-Tousy, Jamal &Abdellah, Zyane. (2025). Integration of MQTT and CoAP Protocols in OneM2M for IoT Applications. 10.1007/978-3-031-90921-4_26.

[6] Shafiq, Shakila, Rahman, Md. Sazzadur, Shaon, Shamim Ahmed, Mahmud, Imtiaz, Hosen, A. S. M. Sanwar, A Review on Software-Defined Networking for Internet of Things Inclusive of Distributed Computing, Blockchain, and Mobile Network Technology: Basics, Trends, Challenges, and Future Research Potentials, International Journal of Distributed Sensor Networks, 2024, 9006405, 26 pages, 2024. https://doi.org/10.1155/2024/9006405.

[7] Mahadik, S.S., Pawar, P.M. & Muthalagu, R. Heterogeneous IoT (HetIoT) security: techniques, challenges and open issues. Multimed Tools Appl 83, 35371–35412 (2024) .https://doi.org/10.1007/s11042-023-16715-w.

[8] Bukhowah, R.; Aljughaiman, A.; Rahman, M.M.H. Detection of DoS Attacks for IoT in Information-Centric Networks Using Machine Learning: Opportunities, Challenges, and Future Research Directions. Electronics 2024, 13, 1031. https://doi.org/10.3390/electronics13061031

[9] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” J. Electr. Comput. Eng., vol. 2017, 2017, doi: 10.1155/2017/9324035.

[10] T. Salman and R. Jain, “A Survey of Protocols and Standards for Internet of Things,” Adv. Comput.Commun.,Feb.2019,doi:10.34048/2017.1.f3.

[11] V. M. Tayur and R. Suchithra, “Review of interoperability approaches in application layer of Internet of Things,” IEEE Int. Conf. Innov. Mech. Ind. Appl. ICIMIA 2017 - Proc., pp. 322–326, Jul. 2017, doi: 10.1109/ICIMIA.2017.7975628.

[12] M. Sandell and U. Raza, “Application layer coding for IoT: Benefits, limitations, and implementation aspects,” IEEE Syst. J., vol. 13, no. 1, pp. 554–561, Mar. 2019, doi: 10.1109/JSYST.2018.2791659

[13] Kilho Lee, Minsu Kim, Taejune Park, Hoon Sung Chwa, Jinkyu Lee, and Seungwon Shin, "MC-SDN: Supporting Mixed-Criticality Real-Time Communication Using Software-Defined Networking," in IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6325-6344, Aug. 2019, doi:10.1109/JIOT.2019.2917546.

[14] M. R. Palattella *et al.*, "Standardized Protocol Stack for the Internet of (Important) Things," in *IEEE* Communications Surveys & Tutorials, vol. 15, no. 3, pp. 1389-1406, Third Quarter 2013, doi: 10.1109/SURV.2012.111412.00158. keywords: {Internet; Standards; Reliability; Schedules; Media Access Protocol; Synchronization; Internet of Things;802.15.4;802.15.4e;CoAP;RPL;Standards;IPv6;Protocol Stack},

[15] Ahmed, N. H., Sadek, A. M., Al-Feel, H., &AbulSeoud, R. A. (2021). Internet of Things Multi-protocol Interoperability with Syntactic Translation Capability. International Journal of Advanced Computer Science and Applications (IJACSA), 12(9).

[16] Yousaf Ikria & Afzal, Muhammad & Kim, Sung & Marin, Andrea & Guizani, Mohsen. (2020), “Deep learning for intelligent IoT: Opportunities, challenges and solutions” Computer Communications. 164. 10.1016/j.comcom.2020.08.017.

[17] Eirini Anthi, Lowri Williams, Amir Javed, Pete Burnap, Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks,Computers & Security,Volume 108,2021 102352,ISSN 0167-4048,https://doi.org/10.1016/j.cose.2021.102352.

[18] Rejito, Juli & Stiawan, Deris & Alshaflut, Ahmed & Budiarto, Rahmat. (2024). Machine learning-based anomaly detection for smart home networks under adversarial attack. Computer Science and Information Technologies. 5. 122-129. 10.11591/csit.v5i2.p122-129.

[19] Gerodimos, A., Maglaras, L., Ferrag, M. A., Ayres, N., & Kantzavelou, I. (2023, January 1). IoT: Communication protocols and security threats. Internet of Things and Cyber-Physical Systems. KeAi Communications Co. https://doi.org/10.1016/j.iotcps.2022.12.003

[20] Feijoo-Añazco, Anthony & Garcia Carrillo, Dan & Sanchez-Gomez, Jesus & Marin-Perez, Rafael. (2023). Innovative security and compression for constrained IoT networks. Internet of Things. 24. 100899. 10.1016/j.iot.2023.100899.

[21] Roldán-Gómez J, Carrillo-Mondéjar J, Castelo Gómez JM, Ruiz-Villafranca S. Security Analysis of the MQTT-SN Protocol for the Internet of Things. Applied Sciences. 2022; 12(21):10991. https://doi.org/10.3390/app122110991

[22] Deepa, O., & Suguna, J. (2017)., "An optimized QoS-based clustering with multipath routing protocol for Wireless Sensor Networks" *Journal of King Saud University - Computer and Information Sciences,* 32(1), 20–28.https://doi.org/10.1016/j.jksuci.2017.11.007

[23] R. A. Elsayed, R. A. Hamada, M. I. Abdalla, and S. A. Elsaid, "Securing IoT and SDN systems using deep-learning based automatic intrusion detection," *Ain Shams Engineering Journal*, vol. 14, no. 10, Art. no. 102211, Oct. 2023, doi: 10.1016/j.asej.2023.102211.

[24] Kavitha, D., & Ramalakshmi, R. (2024). Machine learning-based DDoS attack detection and mitigation in SDNs for IoT environments. Journal of the Franklin Institute, 361(17), Article 107197. https://doi.org/10.1016/j.jfranklin.2024.107197,

[25] Sumadi, F. D. S., Minarno, A. E., Syafa'ah, L., & Irfan, M. (2021), "Enabling seamless communication over several IoT messaging protocols in OpenFlow network" Telkomnika (Telecommunication Computing Electronics and Control), 19(5), 20412. https://doi.org/10.12928/telkomnika.v19i5.20412.

[26] Alve, S. R., Mahmud, M. Z., Islam, S., Chowdhury, M. A., & Islam, J. (2025), "Smart IoT security: Lightweight machine learning techniques for multi-class attack detection in IoT networks" ar Xiv preprint arXiv:2502.04057. https://arxiv.org/abs/2502.04057

[27] G. A. Shah, "IoT DoS and DDoS Attack Detection using ResNet," Proc. - 2020 23rd IEEE Int. Multi-Topic Conf. INMIC 2020, Nov. 2020, doi: 10.1109/INMIC50486.2020.9318216.

[28] H. Qiu, T. Dong, T. Zhang, J. Lu, G. Memmi, and M. Qiu, "Adversarial Attacks against Network Intrusion Detection in IoT Systems," IEEE Internet Things J., vol. 8, no. 13, pp. 10327–10335, Jul. 2021, doi: 10.1109/JIOT.2020.3048038.

[29] K. Prathapchandran and T. Janani, "A trust aware security mechanism to detect sinkhole attack in RPL-based IoT environment using random forest – RFTRUST," Comput. Networks, vol. 198, p. 108413, Oct. 2021, doi: 10.1016/J.COMNET.2021.108413

BIOGRAPHIES OF AUTHORS

Prof. Reshma Nasirhusain Bhai is an experienced academic and researcher with a strong foundation in Electronics and Telecommunication Engineering. She has earned her Master of Engineering (M.E.) in Electronics and Telecommunication and is currently pursuing a Ph.D. at Shivaji University, Kolhapur, Maharashtra, India. With over 18 years of teaching experience and 3 years of industry experience, she brings a comprehensive perspective to both academia and applied research. Her commitment to academic excellence is reflected through her active participation in the research community. She has presented her work at three international conferences and has published four research papers in reputed international journals. Her primary research interests lie in **Wireless Sensor Networks (WSN), Internet of Things (IoT),** and **optimization techniques** for enhancing the performance, energy efficiency, and communication protocols in these domains. She is particularly focused on intelligent routing, clustering algorithms, and energy-aware network design. As a dedicated educator and researcher, she continues to contribute to the advancement of emerging technologies in IoT and WSN, aiming to bridge the gap between theoretical innovation and practical implementation.

Dr. Mahadev S. Patil born at Belgaum in 1973 received BE degree in Electronics and Telecommunication Engineering from Karnataka University Dharwar in 1995, M. Tech degree in Power Electronics from Indian Institute of Technology Bombay in 2002 and Ph.D. degree in Electronics and Telecommunication engineering from Shivaji University, Kolhapur, India in 2014. Selected by AICTE in 2020-21 for UK-India Education and Research Initiative (UKIERI) Technical Leadership and Management Programme and one among 100 participants across India and completed CMI Level 5 in Management and Leadership certification in 2021. He has 28 years of experience and currently working as a Professor and Head of the Electronics and Telecommunication Engineering Department at Rajarambapu Institute of Technology, Islampur. He has received funding for his B Tech project from Karnataka State Council for Science and Technology, Bangalore, funding for his M Tech dissertation from IIT Bombay and funding for his Ph D work from BCUD, Pune University, Pune. He has also received funding from AICTE, MSME and IEDC. He has published 35 papers in Scopus indexed journals and conferences, also filed 4 patents. He is Ph D guide at Shivaji University, Kolhapur. His areas of interest are Power Electronics, Communication and IoT. He is a member of IEEE, IETE and ISTE