International Conference on Current Research Trends
ICCRT 2025 - Hybrid (Hafizabad, Pakistan & Online)
20-21 December 2025

RESEARCH PROPOSAL

Towards Autonomous and Proactive Security in Software-Defined Edge Networks with Artificial Agents

Fatima Abbas [1*], Muhammad Anas Khalid [2], Awais Rasool [3]

[1]Riphah International University Faisalabad, Pakistan
[2]University of Management & Technology Lahore, Pakistan
[3]University of Lahore, Lahore, Pakistan
* Corresponding Email: fatima.abbas@riphahfsd.edu.pk

Published Online: 24 January 2026 by JCPP *DOI: https://doi.org/10.64060/ICPP.03*

ABSTRACT

Edge computing is transforming latency-sensitive systems such as autonomous vehicles, Industrial IoT, and smart infrastructure. Yet, when managed by centralized Software-Defined Networking (SDN) controllers, these environments face complex security risks. Existing defenses are largely reactive, acting only after damage occurs. This research introduces a proactive, multi- agent AI security framework in which distributed agents monitor system status, detect anomalies, and recommend real-time policy adjustments. A novel coordination mechanism enables adaptive reconfiguration of SDN policies through programmable APIs. To address resource limitations at the edge, the framework employs federated learning and lightweight, self-optimizing models, delivering efficient and scalable security for resource-constrained environments. Prototyped on open-source platforms and tested against real-world attack scenarios, the framework will be evaluated for detection latency, resilience, and response efficiency. The evaluation should show that the framework provides a scalable, context-aware defense that strengthens the resilience of critical infrastructure in heterogeneous domains such as smart cities, healthcare, and energy.

Keywords*:* Proactive Security; Autonomous Security; Artificial Agents; Software-Defined Edge Networks

1. Motivation

Edge computing has brought processing closer to data sources, boosting responsiveness and reducing bandwidth use. Yet decentralization complicates efforts to maintain a unified and robust security posture, especially when dynamic reconfigurations are managed by SDN controllers. This architecture increases the attack surface, allowing adversaries to exploit controller vulnerabilities or compromise edge nodes. As cyberattacks targeting edge infrastructure, including ransomware, botnets, and distributed denial-of-service (DDoS) campaigns, become increasingly prevalent, security architectures must evolve to both defend against and proactively anticipate emerging security threats.

Most existing approaches to edge network security remain reactive, detecting threats only after damage occurs. This research proposes a proactive AI-driven framework that employs adaptive agents to detect anomalies and vulnerabilities, isolate malicious traffic, and dynamically reconfigure routing through SDN programmability. By integrating proactive mitigation strategies, the framework delivers scalable and adaptive protection tailored to the demands of secure and efficient edge environments.

2. State of the Art

This manuscript surveys the state of the art in securing SDN-enabled edge environments from eight complementary perspectives. It spans topics including architectural integration, the evolution of security threats, AI-driven intrusion detection, federated learning, and multi-agent defense systems. The review also explores lightweight frameworks for resource-constrained devices, programmable controller architectures, and trust management in distributed networks. Collectively, these themes trace the field’s progression from initial capability scarcity toward *risk-aware resilience*, highlighting design principles that enable edge systems to be fast, adaptive, and inherently trustworthy.

2.1 Edge Computing and SDN Integration

Edge computing brings compute and storage closer to data sources, improving responsiveness and reducing backbone bandwidth. This shift is crucial for latency-sensitive applications such as autonomous systems, Industrial IoT, and augmented reality, where milliseconds matter. Surveys of mobile/edge computing document architectural patterns and deployment models aimed at real-time processing and tighter QoS compared with centralized cloud approaches [1] [2].

Integrating edge computing with Software-Defined Networking (SDN) adds network-wide programmability for traffic steering, policy enforcement, and resource optimization.

Programmable control can improve service delivery and resource allocation compared with static, distributed architectures, enabling dynamic adaptation to workload and context [3]. This convergence underpins low-latency paths, bandwidth efficiency, and rapid roll-outs of new services across heterogeneous edge sites.

SDN logically separates concerns into planes that interact via well-defined interfaces: the data plane forwards packets; the control plane computes and installs forwarding rules; and the management (or orchestration/application) plane monitors, configures, and coordinates services across the infrastructure [4] [5]. This separation increases flexibility and automates network management while exposing new dependencies between planes in resource-constrained edge settings. Figure 1 illustrates the SDN architecture across management, control, and data planes.

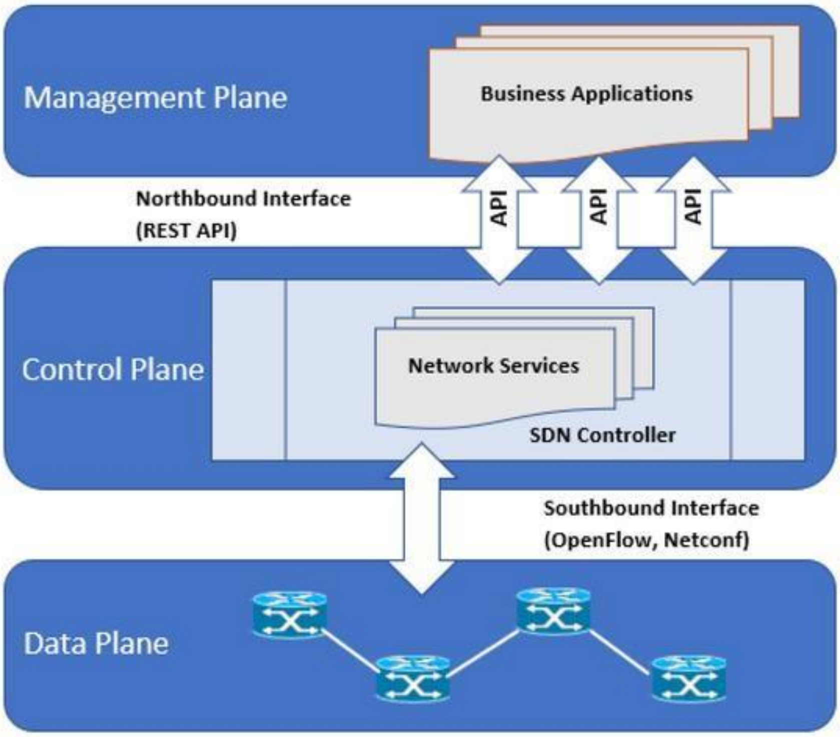

Figure 1. *SDN architecture with management, control, and data planes. Reprinted from* [5]

Several critical threats can affect the SDN–edge ecosystem, including man-in-the-middle attacks, interception of control plane traffic, and data poisoning of edge nodes [6]. These threats underscore the necessity for further development of security mechanisms tailored to the unique characteristics of Edge–SDN systems and may serve as the foundation for future research into artificial intelligence–based detection and mitigation strategies.

2.2 SDN Security Threats in Edge Environments

The security environment of SDN managing edge networks offers a very complicated combination of threats that are significantly diverse relative to conventional network security problems. The innovative architecture features of the centralized control complemented by the edge processing introduces new attack vectors that need a specific security response. Awareness of such threats is key to creating robust security structures that will secure the edge infrastructures without interfering with their performance benefits. [3] provide the detailed taxonomy of known attacks on SDN controller in edge networks which comprise five main categories attackers use: controller hijacking, flow rule manipulation, topology poisoning, denial-of-service (DOS) against a controller, and northbound API misuse.

These categories are illustrated in Figure 2.1, which presents a visual taxonomy of common SDN controller attacks in edge environments. [7] Explain the flow rule manipulation attacks, which was capable of diverting traffic by using attacker-controlled nodes.

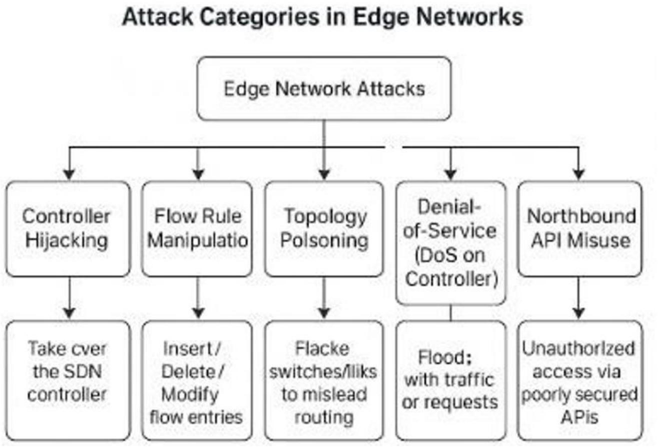
Attack Categories in Edge Networks
Edge Network Attacks
Controller Hijacking
Flow Rule Manipulatio
Topology Poisoning
Denial-of-Service (DoS on Controller)
Northbound API Misuse
Take cver the SDN controller
Insert/ Delete/ Modify flow entries
Flacke switches/liks to mislead routing
Flood: with traffic or requests
Unauthorized access via poorly secured APIs

***Figure 2**: Taxonomy of SDN Controller Attack Categories in Edge Networks* Adapted from [3] and [7]

It further facilitates cyber intelligence gathering by enabling the undetected interception and monitoring of data over a prolonged period. In [8], the authors examine topology poisoning attacks, which involve the injection of false information regarding the network's status. As a result, the controller is misled and may draw incorrect conclusions, leading to potentially hazardous routing decisions.

Conventional security facilities are insufficient when it comes to handling these types of SDN specific threats because edge environments are resource-constrained and time-sensitive. [9] Note that there is an essential shift in paradigm between reactive and proactive security models to the models in which anomalies could be detected and isolated until they cause damage to the system. They demonstrate that conventional security methods are not readily adaptable to the dynamic nature of edge networks managed by SDN, emphasizing the necessity of adaptive security mechanisms that operate effectively within the constraints of edge computing. Their proposed approach leverages AI-based security solutions to address these challenges.

3. Artificial Intelligence-Based Intrusion Detection Systems

The use of artificial intelligence as an intrusion detection tool in SDN-controlled edge networks represents a paradigm shift from traditional signature-based intrusion detection methods to intelligent, learning-based intrusion protection systems. The AI agents provide the potential to identify threats in real-time and with adaptive responses as well as constantly learning new patterns of attack activity in dynamic edge environments, where conventional security systems have been less successful.

Supervised learning techniques have been proved to be quite effective in detecting attack patterns that are already known. Other studies such as those by [10] evaluate supervised learning approaches systematically and show that performance of ensemble methods like those that include Random Forest and Support Vector Machine (SVM) can perform even better (detection rates above 95%). [11] Provide a review that shows that hybrid solutions that integrate Convolutional Neural Networks (CNNs) with Recurrent Neural Networks (RNNs) are more successful since they achieve more accurate detection and a lower number of false positives as compared to the traditional methods. Nonetheless, [12] highlight barriers to deployment, noting that increased data sharing is essential to facilitate a more seamless and effective implementation.

Integration of Federated Learning techniques helps to deal with both computational and privacy issues of edge security. [13] Illustrate how federated learning presents a potential solution of enabling collaborative threat detection at edge nodes with no centralized-data aggregation, offering an unbalancing yet effective trainer, with privacy and reduced communication overhead. [14] Address the issue of resource constraints by utilizing lightweight neural network architectures, including model pruning, quantization, and knowledge distillation, which makes it possible to process the AI-based detection on the resource-constrained devices. All of these developments pave the way in trying to realize distributed multi-agent systems, which can offer autonomous decision-making systems.

4. Federated Learning for Distributed Edge Security

Federated learning has developed into an extreme methodology of implementation of distributed security systems in the edge networks where they solve inherent problems in privacy preservation, bandwidth ratio, and dispersion of computational resources. The paradigm helps to achieve group learning

The use of the technology also allows network edge machines to process data securely without specializing network in data aggregation making it particularly suitable in applications where sensitivity of the data and efficiency of the network become critical.

The new trends have depicted that there has been a commendable improvement in terms of performance of the system in the detection as well as efficiency. The offered Bidirectional Encoder Representations from Transforms (BERT) based federated intrusion detection system in [15] appears to have better results over 94 percent detection accuracy and a guarantee of privacy since the training is done locally in the fifth generation (5G) ecosystems. The work by

[16] offering a federated structured framework that is specifically assigned to the IOT networks includes self-adaptive aggregation algorithms that can reduce the quantity of utilized bandwidth during a communication process up to 75%. Demonstrating that a zero-trust federated learning system may achieve a 99.5 detection accuracy even when 20 percent of the participants are malicious, [17] also reveal how to overcome this difficulty: by means of a zero-trust federated learning system, one may reach the reported 99.5 detection accuracy.

The issue of model personalization and security is done away with by innovative methods. An ensemble knowledge distillation based federated learning in heterogeneous IOT networks is introduced by [18], and Federated Multi Agent Deep Ensemble (FEDMADE) with dynamic aggregation techniques is proposed by [2]. The work of [19] presents the Secure Federated Deep Neural Network (SECFEDDNN) framework, which embeds differential privacy and profiles of Byzantine fault tolerance with little performance overhead. Development notwithstanding, convergence in heterogeneous environments and privacy versus threat intelligence sharing are issues of concern and multi-agent systems have been seen as potential players in an enhanced coordination.

5. Multi-Agent Systems for Autonomous Network Defense

Multi-agent systems constitute an advanced method to distributed network security that allows a highly decentralized, coordinated security mechanism throughout the complex edge computing environments. These systems use the principles associated with distributed artificial intelligence to form trust networks of intelligent agents that can be used to make independent decisions, collective solver of problems, and adaptive learning, which serves as a scalable, recoverable network protection architecture to manage edge control networks through SDN.

Modern implementations prove to be considerably more beneficial in comparison to centralized methods. The work by [7] introduces a novel, Multi-AgentSystems (MAS)-based firewall system in which the regulations of SDN controllers are dynamically updated by distributed, network-wide agents that decreases the response time to various threats by up to 60 percent and are also more resilient toward Advanced Persistent Threats APTs and insider attacks. [20] Propose Q-learning agents to enable colluding Distributed Denial-of-Service DDoS mitigation with attack success rates reduction and more than 30% compared to static systems. [21] present auction-based systems of coordination that enhance the efficiency of the system via optimal task allocation by 45 percent.

More sophisticated coordination mechanisms are introduced, which includes swarm intelligence and reputation management. Rodriguez and [13] create collective swarm-based intrusion detection systems that are capable of managing the environmental scale of the edge environments. Respecting trust issues, [22] introduce the concept of blockchain based reputation systems which identify and isolate bad actors and reward the good ones, thereby encouraging the cooperative aspect of the interaction. Nevertheless, challenges persist due to the complex nature of coordination in dynamic environments and the trade-offs between autonomous decision-making and centralized control. These issues extend to policy enforcement and highlight the need for lightweight security solutions optimized for resource-constrained edge devices.

6. Lightweight Security Frameworks for Resource-Constrained Edge Devices

The lightweight security frameworks are quite hard to find out in an edge computing environment involving a very limited number of computational resources, power consumption, and memory space. Such limitations necessitate the development of new ways that provide high levels of security and operate on limited resources of edge devices such as IOT) sensors, embedded systems and mobile devices.

The solution that [3] and [23] address is the performance of the Edge Guard as an intrusion detection system that is edge-centered to detect as many as 90 percent of the detected attacks even with the limitation of 1GB RAM available.

[14] Introduce the concept of federated learning as an efficient mechanism to reduce the computational in-device requirements by up to 70 percent, which includes the compression of models, quantization of gradients, and asynchronous updates. [12] Propose end-to-end neural network optimisation which included model pruning, quantization, and knowledge distillation to enable advanced detection by designing to run on devices with limited resources.

The optimization of communication and energy efficiency is the most crucial thing when it comes to scenarios using devices with limited resources, including battery-assisted ones. The energy-efficient scheme makes it to the end of regulating the degree of detection dynamically to minimize energy use with the consideration of the remaining battery power level of the gadget and extrapolating it to give the device an additional working period of up to 40 per cent [16] create powerful communication procedures that reduce unnecessary processing and communication load by 60 percent, while maintaining the same level of message delivery assurance. Despite these advancements, challenges remain in maintaining effective security within the constraints of limited resources and an evolving threat landscape. This underscores the renewed relevance of SDN controller-based architectures, which can enable intelligent coordination and dynamic policy enforcement.

7. SDN Controller Architecture and Programmable Network Management

Programmability of networks is based on the SDN controller designs that form the basis of the network control in edge computing by programmability of networks in their entirety as well as providing the maximum flexibility by dynamic network configuration and deployment of network policies. The wide-ranging network topology, different application requirements, and sophisticated security guidelines in the distributed edge architecture are some of the factors that have led to the development of SDN controllers.

Newer SDN controllers have an architecture that is extensible and have open Application Programming Interfaces APIs that notify third party security applications. In a comprehensive comparative analysis of the most common controllers, [7]show that Open Network Operating System ONOS excels in the segment of scalability and developer ease of work since it can scale to over 1000 of the switches and registers sub-millisecond flow set up times. In transitioning to the new paradigm shift, the intent-based networking architectures, introduced by [20] have assisted to save the 80 percent workload of policy configuration chores and since the translation of the security requirements of the high level into the network level configurations are automatic, it can be said that consistency is enhanced.

Sophisticated architectures address the edge requirements with distributed control planes and AI is a part of the latter. [4] provide hierarchical SDN plans that lead to the creation of new SDN control planes that have 70 per cent less latency because of local edge controllers as well as global coordination. The article suggests novelty in implementing a new AI-based controller and machine learning to gather controllers and optimize policy choice, as well as to learn optimal network policies, lowering errors made in the process by 30 percent and 60 percent, respectively[1]. However, there are still risks that security services may be penetrated, as well as issues with scale, and they have an interest in trust and reputation systems of distributed edge networks.

8. Trust and Reputation Management in Distributed Edge Networks

Trust and reputation management systems have become foundational in terms of providing reliable and secure operations of distributed edge networks, especially when multiple agents that are autonomously operating are required to cooperate without any centralized management. The systems enable quantifiability and control of uncertainty in distributed interactions, and the ability to make informed decisions regarding collaboration, resource sharing and information exchange in dynamic edge environments.

The study by [19] introduces a detailed blockchain-based trust system in SDN edge networks that keeps the immutable trust records and stops the malicious attack on the trust judgments. Their mechanism supports opaque audit records and decentralized agreement on levels of trust and is an effective way of discovering and quarantining malicious to maximize the level of collaboration in a group of legitimate interactors. [7] come up with lightweight equivalences that utilize reputation aggregation and cryptographic verification to combat the computational expenses and deliver an effective trust control technique that can assist in resource-limited settings.

Although some of the issues facing trust-based security mechanisms have been resolved, several problems still remain such as computational complexity of blockchain based systems in constrained settings, at the onset of trust inconsistencies in partitioned networks, and balancing trust accuracy with system very responsiveness.

An examination of existing literature has highlighted research gaps in self-organizing security systems whereby agents can self-learn how to protect systems in spite of changing network topologies and adversary tactics and strategies. A 2019 survey by Ismail and wazir khan confirms all of the above, but also strongly underlines the necessity of adopting proactive methods of threat prevention that concern itself with not only trust management but also real-time, adaptive defense mechanisms, and there is a related strong need to consider developing fabricated solutions that simultaneously apply multi-agent reasoning, federated learning, and lightweight trust management to the area of real-world network security.

9. Objectives

9.1 Primary Objective

Design, develop, and validate a proactive, intelligent, and distributed security framework for SDN-orchestrated edge networks. The framework will employ learning agents that adapt to evolving threats in real time while preserving latency, throughput, and overall network performance.

9.2 Main Objectives

1. Architecture design: Create a multi-agent proactive security architecture with agents deployed at strategic edge nodes to autonomously monitor traffic, detect anomalies, share insights, and recommend real-time policy updates to the SDN controller.
2. Learning-based detection: Embed lightweight machine learning within edge agents (e.g., federated

learning, LSTM, reinforcement learning) to enable real-time threat detection and behavior prediction with minimal computational overhead.

3. Dynamic policy adaptation: Develop mechanisms for agents to drive on-the-fly SDN flow reconfiguration via programmable northbound APIs, enabling flexible, automated, and context-aware responses.
4. Resilience and scalability: Engineer robustness against DDoS, topology poisoning, and insider threats, and ensure scalability across heterogeneous edge networks with negligible performance degradation.
5. Evaluation and validation: Use SDN controllers (e.g., Ryu) and emulators (e.g., Mininet) to assess detection accuracy, false-positive/false-negative rates, response time, added latency, throughput impact, resource overhead, and resilience under sustained attack.
6. Open science contribution: Release an open-source prototype and publish best-practice recommendations for deploying proactive, intelligent security in SDN-based edge environments.
These objectives support secure, adaptive, and self-healing edge infrastructures essential to smart cities, autonomous systems, telemedicine, and critical infrastructure management.

10. Research Questions

The proposed research aims to develop a secure, autonomous, and proactive architecture for managing cybersecurity threats in software-defined edge networks. To achieve this goal, the following research questions are formulated. These questions will guide the research process and will be addressed through the development, implementation, and evaluation of the proposed solutions during the PhD study:

- **RQ1: Agent design and deployment:** How can lightweight, autonomous artificial agents be designed and deployed at edge nodes to effectively detect and respond to cybersecurity threats in real-time, without breaching latency and resource constraints typical of edge environments?
- **RQ2: Learning for collaboration and adaptability:** What is the efficacy of integrating federated learning and reinforcement learning into multi-agent systems for enhancingintrusion detection accuracy, adaptability, automatic detection and remediation of system vulnerabilities, and collaborative decision-making in SDN-managed edge networks?
- **RQ3: Learned policy influence via SDN programmability:** To what extent can artificial agents dynamically influence and reconfigure Software-Defined Networking (SDN) controller policies through northbound APIs to enable context-aware, automated mitigation of network security threats?
- **RQ4: Scalability and resilience under attack:** How does a proactive, multi-agent security architecture scale across heterogeneous edge topologies, and how resilient is it against adversarial scenarios such as DDoS, flow-rule flooding, control-plane saturation, and rogue node injection?
- **RQ5: Evaluation metrics and trade-offs:** How scalable and resilient is a proactive, multi-agent security architecture across heterogeneous edge network topologies with eventual high-risk vulnerabilities subjected to diverse adversarial scenarios such as DDoS attacks, flow rule flooding, and rogue node injections?
- **RQ5: Evaluation metrics and trade-offs:** How scalable and resilient is a proactive, multi-agent security architecture across heterogeneous edge-network topologies when faced with eventual high-risk vulnerabilities and diverse adversarial scenarios — such as DDoS attacks, flow-rule flooding, and rogue-node injections — as assessed through quantifiable performance (throughput, latency), security (detection rate, false-positive rate), and adaptability (time-to-mitigation, recovery speed) metrics?
The table below summarizes the current proposal research questions.

11. Summary of Research Questions

RQ	Focus	Core Aim
RQ1	Agent Design & Deployment	Develop lightweight, autonomous agents for edge nodes that can detect and respond to threats in real time without breaching latency or resource limits.
RQ2	Learning Integration	Assess the benefits of combining federated learning and reinforcement learning in multi-agent systems to boost detection accuracy, adaptability, and collaboration.
RQ3	Dynamic Policy Adaptation	Explore how agents can safely and context-sensitively reconfigure SDN controller policies via northbound APIs for automated, low-latency threat mitigation.
RQ4	Scalability & Resilience	Evaluate system performance, scalability, and resilience under diverse topologies and adversarial scenarios (e.g., DDoS, flow-rule flooding, rogue nodes).
RQ5	Evaluation Metrics & Trade-offs	Define and analyze the metrics and trade-offs between detection performance, automatic remediation, overhead, false positives, and quality of service in realistic edge deployments.

12. Research Project Proposal

12.1 Basis for Work Development

The rise of edge computing and SDN as interdependent technologies has created new opportunities for optimizing resource allocation, network control, and service delivery at the edge. However, these advancements also introduce critical security risks, especially due to the centralization of control in SDN and the distributed, resource constrained nature of edge nodes. Research from 2020 to 2025 has demonstrated growing threats like SDN controller hijacking, data injection, botnets, and insider attacks in edge deployments [3] and [23].

While traditional security mechanisms focus on post-attack mitigation or static rule enforcement, recent trends highlight the need for autonomous, intelligent, and proactive systems. Multi-agent systems (MAS), integrated with machine learning (ML) and SDN programmability, offer a way to build adaptable security mechanisms that respond to threats dynamically while preserving edge performance [22] and [1]

This project is built on the premise that distributed artificial agents, equipped with learning capabilities and embedded within SDN-managed edge environments, can collectively detect, report, and respond to security anomalies in real time. These agents can learn from both local and shared experiences to continuously enhance the resilience of the edge network infrastructure.

12.2 Work Description

System Architecture

The proposed architecture will consist of:

- Edge Nodes: Embedded with lightweight agents that collect network and host level Operational status.
- SDN Controller: Receives agent alerts and dynamically updates routing rules or applies mitigation policies.
- Agent Communication Layer: Uses publish-subscribe messaging for efficient sharing of insights.
- AI Engine: Implements machine learning algorithms (e.g., federated learning, RL) for threat classification and adaptive defense.

The architecture will use the Ryu controller, Mininet for emulated topologies, and the framework like TensorFlow Lite or PyTorch Mobile to deploy ML models on the edge devices

Agent Design

- Each artificial agent will consist of the following components:
- Monitoring Module: Captures flow stats, packet anomalies, CPU usage, and system logs.
- Feature Extractor: Applies dimensionality reduction and normalization for lightweight inference.
- Detection Engine: Uses LSTM or hybrid CNN-RNN models for anomaly detection.
- Communication Module: Exchanges alerts with peer agents and controller over secure channels.
- Policy Recommender: Suggests policy actions such as rerouting, flow blocking, or quarantine.

Agent learning will be based on recent research in collaborative and federated learning [12], enabling decentralized model updates without transmitting raw data

Threat Scenarios and Response

- The system will be evaluated under multiple real-world inspired attack scenarios:
- DDoS against SDN Controller
- Flow Rule Flooding
- Rogue Edge Node Injection
- Botnet Communication (e.g., Mirai-based)
- Insider Data Leakage

Response strategies will include flow re-routing, dynamic reauthentication, agent based isolation, and policy reconfiguration using Ryu's REST API.

Experimental Setup

A simulation testbed will be built using:

- Mininet to emulate edge nodes and switches
- Ryu SDN controller for routing management
- Wireshark and sFlow for traffic analysis
- Scapy to generate attacks and traffic anomalies
- Python-based ML models for anomaly detection
- Docker for agent containerization
- Edge devices like Raspberry Pi (optional for hardware testing)

Experiments will be conducted across varied topologies (tree, mesh, hybrid) to test scalability, responsiveness, and detection accuracy.

Performance Evaluation Metrics

The system will be evaluated using the following metrics:

- Detection Accuracy: Percentage of true positives vs. false positives
- Threat Response Time: Time between anomaly detection and mitigation
- Network Throughput: Impact on data transmission during defense
- Latency Overhead: Added delay due to agent actions or controller response
- Agent Resource Utilization: CPU, RAM, and energy usage

Benchmark comparisons will be made against centralized IDS (e.g., Snort) and static Rule-based SDN defenses.

13. Key Contributions

This project will provide:

1. A novel multi-agent framework tailored for SDN-based edge environments.
2. Lightweight ML-based anomaly detection methods deployable on edge devices.

3. Real-time integration with SDN controllers for dynamic threat response.
4. Experimental validation through simulations and open-source prototype release.
5. Research publications, workshops, and conference presentations to share findings with the academic and professional community.

Expected Outcomes

The suggested study will provide theoretical and practical findings that will help in intelligent, secure, and autonomous edge networking. The results of these outcomes aim to reflect the literature gaps that have been determined and deliver solutions in real-time and can be scaled to the SDN-managed edge infrastructures.

- An intelligent, self-adaptive security model for SDN edge networks
- Reduced threat mitigation time without compromising performance
- Guidelines for scalable deployment of AI agents in constrained environments
- Increased trustworthiness of edge infrastructures in critical domains

Project Outputs

By the conclusion of the project, the following outcomes are expected, each explicitly addressing gaps in the existing literature:

- A modular, scalable multi-agent security framework for SDN-controlled edge networks

Although the former paradigms primarily focus on centralized, decision-making, this model allows distributed coordination and adaptable options, which enhances resistance and scalability to the changes of dynamic edge environments.

- AI-driven, lightweight intrusion detection agents suitable for real-world deployment

Our agents can be trained on tight edge nodes by leveraging compressed model representations and federated learning unlike traditional deep learning models, which are too resource intensive [3].

- A full-featured simulation testbed for edge security experimentation

The current assessments tend to be non-reproducible or lack emulation to the real world. Our testbed can address this gap since it simulates various topologies and types of attacks using tools such as Mininet and RYU.

- Open-source code repository, including setup instructions and model weights All implementation assets will be published to enhance the reproducibility and promote adoption and this is opposite to closed configurations of most academic prototypes.
- At least three peer-reviewed publications in high-impact venues. This will guarantee the sharing of innovative methods and benchmarks of performance, which will help in the overall discourse in SDN, edge computing, and AI-based cybersecurity.
- A defended and approved PhD dissertation, contributing to the academic and industrial edge security domains.

14. Answers to Research Questions

This section presents the expected answers to the defined research questions, based on the results obtained during the PhD research. These reflect the key contributions and outcomes of the work.

The outcomes of the PhD research are expected to provide well-substantiated answers to the research questions:

- **RQ1 Answer**: By developing a modular and lightweight agent framework optimized for edge resources, the research demonstrates that autonomous agents can be effectively deployed on edge nodes. Using containerization, rule-based threat detection, and distributed inference, the agents maintain real-time response capabilities while preserving latency and resource limits.
- **RQ2 Answer**: The integration of federated learning and reinforcement learning into multi-agent systems significantly enhances detection accuracy and system adaptability. Experimental results show improved responsiveness to novel threats, reduced false positives, and the emergence of cooperative

behaviors that support distributed defense mechanisms in SDN-managed environments.

- **RQ3 Answer**: The research confirms that agents equipped with policy reconfiguration capabilities via northbound APIs can dynamically adapt the SDN controller's behavior based on contextual threat intelligence. This enables automated and context-aware mitigation strategies, reducing administrative overhead and response time to evolving threats.
- **RQ4 Answer**: The proposed proactive, multi-agent security architecture scales across heterogeneous edge topologies and withstands varied adversarial scenarios — including DDoS attacks, flow-rule flooding, and rogue node injections. Both simulation and prototype testing should confirm the next aspects: i) consistent detection and mitigation under load; ii) quick recovery via collaborative reconfiguration and trust propagation; and

  iii) sustained control-plane performance and service continuity.
- **RQ5 Answer:** The investigation establishes quantitative and qualitative benchmarks for evaluating security, adaptability, and system cost, including: (i) threat detection accuracy, precision, and recall; (ii) control-plane overhead and latency impact; (iii) the cost of false positives to service quality; and (iv) adaptability and recovery time under adversarial conditions. Prior research should suggest that a careful balance of these metrics can achieve high security assurance without imposing excessive demands on network resources.

15. Limitations and Mitigation Strategies

There are several potential shortcomings and risks during PhD work. The table below summarizes them alongside the corresponding mitigation actions.

Risk / Limitation	Mitigation Strategy
Real-world data scarcity	Integrate synthetic traffic generation, open resources (e.g., CICIDS2017 [24], TON IoT [25]), and regulated testbed emulation to generate plausible and heterogeneous training / validation data. Further, we should add some recent surveys: A survey of public IoT datasets in network security research [26], Network traffic classification: Techniques, datasets, and challenges , and others. Such datasets as UNSW HomeNet [27], may also supply realistic IoT traffic to edge security research activities.
Resource constraints at the edge	Use lightweight ML models, federated learning, and selective offloading of complex computation to SDN controllers to fit within CPU, memory, and energy limits.
Evolving threat landscape	Implement adaptive learning with online updates, periodic re-training, and continuous feedback loops between agents and controllers to keep pace with new attack vectors.
Agent coordination and trust issues	Deploy trust-aware mechanisms, fault-tolerant coordination protocols, and fallback policies to ensure graceful degradation during communication failures or malicious agent activity.
Evaluation complexity	Iteratively enhance the testbed and benchmark against state-of-the-art systems to approximate large-scale topologies and realistic adversarial conditions.

References

[1] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, “Edge computing: A survey,” Futur. Gener. Comput. Syst., vol. 97, pp. 219–235, 2019, doi: 10.1016/j.future.2019.02.050.

[2] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, “Mobile Edge Computing: A Survey,” IEEE Internet Things J., vol. 5, no. 1, pp. 450–465, 2018, doi: 10.1109/JIOT.2017.2750180.

[3] X. Zhang, C. Chen, Y. Xie, X. Chen, J. Zhang, and Y. Xiang, “A survey on privacy inference attacks and defenses in cloud-based Deep Neural Network,” Comput. Stand. Interfaces, vol. 83, p. 103672, 2023, doi: https://doi.org/10.1016/j.csi.2022.103672.

[4] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, “Software-defined networking: A comprehensive survey,” Proc. IEEE, vol. 103, no. 1, pp. 14–76, 2015, doi: 10.1109/JPROC.2014.2371999.

[5] A. Hamarsheh, “An Adaptive Security Framework for Internet of Things Networks Leveraging SDN and Machine Learning,” Appl. Sci., vol. 14, no. 11, 2024, doi: 10.3390/app14114530.

[6] M. Raza, M. Jasim Saeed, M. B. Riaz, and M. Awais Sattar, “Federated Learning for Privacy-Preserving Intrusion Detection in Software-Defined Networks,” IEEE Access, vol. 12, no. May, pp. 69551–69567, 2024, doi: 10.1109/ACCESS.2024.3395997.

[7] A. A. Okon, “A Blockchain-enabled SDN Framework for Multi-operator Networks,” no. January, 2025.

[8] J. Chen, Q. Li, H. Wang, and M. Deng, “A machine learning ensemble approach based on random forest and radial basis function neural network for risk evaluation of regional flood disaster: A case study of the yangtze river delta, China,” Int. J. Environ. Res. Public Health, vol. 17, no. 1, pp. 1–21, 2020, doi: 10.3390/ijerph17010049.

[9] A. Rahdari et al., “Security and Privacy Challenges in SDN-Enabled IoT Systems: Causes, Proposed Solutions, and Future Directions,” Comput. Mater. Contin., vol. 80, no. 2, pp. 2511–2533, 2024, doi: 10.32604/cmc.2024.052994.

[10] J. C. Correa Chica, J. C. Imbachi, and J. F. Botero Vega, “Security in SDN: A comprehensive survey,” J. Netw. Comput. Appl., vol. 159, no. November 2019, p. 102595, 2020, doi: 10.1016/j.jnca.2020.102595.

[11] M. Abdallah, N. An Le Khac, H. Jahromi, and A. Delia Jurcut, “A Hybrid CNN-LSTM Based Approach for Anomaly Detection Systems in SDNs,” ACM Int. Conf. Proceeding Ser., 2021, doi: 10.1145/3465481.3469190.

[12] M. Mohammadi, A. Al-Fuqaha, S. Sorour, and M. Guizani, “Deep learning for IoT big data and streaming analytics: A survey,” IEEE Commun. Surv. Tutorials, vol. 20, no. 4, pp. 2923–2960, 2018, doi: 10.1109/COMST.2018.2844341.

[13] T. V. Phan, T. G. Nguyen, N. N. Dao, T. T. Huong, N. H. Thanh, and T. Bauschert, “DeepGuard: Efficient Anomaly Detection in SDN with Fine-Grained Traffic Flow Monitoring,” IEEE Trans. Netw. Serv. Manag., vol. 17, no. 3, pp. 1349–1362, 2020, doi: 10.1109/TNSM.2020.3004415.

[14] S. Ismail, S. Dandan, and A. Qushou, “Intrusion Detection in IoT and IIoT: Comparing Lightweight Machine Learning Techniques Using TON_IoT, WUSTL-IIOT-2021, and EdgeIIoTset Datasets,” IEEE Access, vol. 13, no. February, pp. 73468–73485, 2025, doi: 10.1109/ACCESS.2025.3554083.

[15] M. Rahouti, K. Xiong, Y. Xin, S. K. Jagatheesaperumal, M. Ayyash, and M. Shaheed, “SDN Security Review: Threat Taxonomy, Implications, and Open Challenges,” IEEE Access, vol. 10, no. April, pp. 45820–45854, 2022, doi: 10.1109/ACCESS.2022.3168972.

[16] K. M. Kokila M and S. R. K. Srinivasa Reddy Konda, “DeepSDN: Deep Learning Based Software Defined Network Model for Cyberthreat Detection in IoT Network,” ACM Trans. Internet Technol., 2025, doi: 10.1145/3737875.

[17] Y. Tseng, F. Naït- Abdesselam, and A. Khokhar, “A comprehensive 3- dimensional security analysis of a controller in software- defined networking,” Secur. Priv., vol. 1, no. 2, 2018, doi: 10.1002/spy2.21.

[18] A. Hirsi, L. Audah, A. Salh, M. A. Alhartomi, and S. Ahmed, “Detecting DDoS Threats Using Supervised Machine Learning for Traffic Classification in Software Defined Networking,” IEEE Access, vol. 12, no. September, pp. 166675–166702, 2024, doi: 10.1109/ACCESS.2024.3486034.

[19] Z. Chen, N. Lv, P. Liu, Y. Fang, K. Chen, and W. Pan, “Intrusion Detection for Wireless Edge Networks Based on Federated Learning,” IEEE Access, vol. 8, pp. 217463–217472, 2020, doi: 10.1109/ACCESS.2020.3041793.

[20] A. John, I. F. Bin Isnin, S. H. H. Madni, and M. Faheem, “Cluster-based wireless sensor network framework for denial-of-service attack detection based on variable selection ensemble machine learning algorithms,” Intell. Syst. with Appl., vol. 22, no. December 2023, p. 200381, 2024, doi: 10.1016/j.iswa.2024.200381.

[21] I. Akbari, E. Tahoun, M. A. Salahuddin, N. Limam, and R. Boutaba, “ATMoS: Autonomous Threat Mitigation in SDN using Reinforcement Learning,” Proc. IEEE/IFIP Netw. Oper. Manag. Symp. 2020 Manag. Age Softwarization Artif. Intell. NOMS 2020, 2020, doi: 10.1109/NOMS47738.2020.9110426.

[22] S. Facchinetti, S. A. Osmetti, and C. Tarantola, “Network models for cyber attacks evaluation,” Socioecon. Plann. Sci., vol. 87, no. PB, p. 101584, 2023, doi: 10.1016/j.seps.2023.101584.

[23] A. M. Sheikh, M. R. Islam, M. H. Habaebi, S. A. Zabidi, A. R. Bin Najeeb, and A. Kabbani, “A Survey on Edge Computing (EC) Security Challenges: Classification, Threats, and Mitigation Strategies,” Futur. Internet, vol. 17, no. 4, pp. 1–54, 2025, doi: 10.3390/fi17040175.

[24] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “CICIDS2017: Intrusion Detection Evaluation Dataset,” pp. 1–11, 2017.

[25] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, “A Detailed Analysis of the CICIDS2017 Data Set BT - Information Systems Security and Privacy,” P. Mori, S. Furnell, and O. Camp, Eds., Cham: Springer International Publishing, 2019, pp. 172–188.

[26] N. Moustafa, “A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets,” Sustain. Cities Soc., vol. 72, p. 102994, 2021, doi: 10.1016/j.scs.2021.102994.

[27] A. Azab, M. Khasawneh, S. Alrabaee, K. K. R. Choo, and M. Sarsour, “Network traffic classification: Techniques, datasets, and challenges,” Digit. Commun. Networks, vol. 10, no. 3, pp. 676–692, 2024, doi: 10.1016/j.dcan.2022.09.009.

Declaration

Conflict of Study: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Author Contribution Statement: All authors contributed equally.

Funding Statement: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Availability of Data and Material: Data will be made available by the corresponding author on reasonable request.

Acknowledgement: Not Applicable

Declaration of AI Use: Not Applicable

Author(s) Bio / Authors’ Note

Fatima Abbas *from Riphah International University, Faisalabad, Pakistan. Email:* fatima.abbas@riphahfsd.edu.pk

Muhammad Anas Khalid *from the University of Management & Technology, Lahore, Pakistan. Email:* anaskhalid021@gmail.com

Awais Rasool *from the University of Lahore, Pakistan. Email:* awaisrasool373@gmail.com