Mesopotamian journal of Cybersecurity
Vol. 5, No.2, **pp**. 671–684
DOI: https://doi.org/10.58496/MJCS/2025/040; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

SDN-Cloud Incident Detection & Response with Segmented Federated Learning for the IoT

Anas Harchi [1, *], Hicham Toumi [2], Mohamed Talea [1]

[1] *Information Processing Laboratory, Faculty of Sciences Ben M'sik, University Hassan II Casablanca, Morocco*

[2] *Higher School of Technology-Sidi Bennour, Chouaïb Doukkali University, El Jadida, Morocco*

ARTICLE INFO

Article history
Received 1 Dec 2024
Revised: 3 Aprl 2025
Accepted 15 Jun 2025
Published 14 Jul 2025

Keywords
Federated learning
IOT
IDS
Cloud Computing
SDN

ABSTRACT

The accelerated proliferation of Internet of Things (IoT) apparatuses has rendered intrusion detection and incident response progressively arduous owing to device diversity, constrained resources, and concerns regarding data confidentiality. Addressing these challenges is paramount to sustaining secure and resilient IoT ecosystems. This manuscript introduces an innovative framework that amalgamates software-defined networking (SDN) with segmented federated learning (SFL) to augment the effectiveness and reactivity of anomaly detection within the IoT. The proposed methodology delineates the federated learning (FL) process, facilitating lightweight, localized model training customized to the capabilities of individual IoT devices. The SDN is utilized to dynamically regulate network flows and implement real-time incident response measures. The proposed architecture is structured to reduce communication overhead, safeguard data privacy, and support participation from resource-limited nodes. A simulation-based evaluation strategy is proposed, with both execution and empirical substantiation anticipated in forthcoming stages. This integrated SFL-SDN paradigm provides a scalable and privacy-conscious solution for fortifying IoT infrastructures and is anticipated to surpass conventional centralized and nonsegmented FL methodologies in intricate, real-time threat scenarios.

1. INTRODUCTION

The phrase "Internet of Things" refers to a future in which physical things that are not typically associated with computers are linked to the internet in some way. [1] The expansion of IoT devices has fundamentally transformed numerous dimensions of modern existence, providing unmatched levels of connectivity and convenience. Nevertheless, the extensive incorporation of the IoT also introduces significant security challenges. A significant proportion of these devices are deficient in substantial intrinsic security protocols, thereby rendering them susceptible to cyber assaults. Additionally, the diverse and constantly evolving nature of IoT environments introduces layers of intricacy in the identification and mitigation of intrusions.

Traditional FL systems fail to adapt to heterogeneous device constraints and lack real-time adaptability, which is essential in dynamic IoT ecosystems. Conventional intrusion detection systems (IDSs) encounter constraints in adequately securing IoT endpoints because of their fixed and centralized characteristics. Addressing these challenges, SDN has emerged as a promising framework that delivers centralized management and flexibility, enabling dynamic network administration and security reinforcement. By harnessing SDN, in conjunction with advancements in FL and cloud computing, a compelling strategy unfolds to enhance IoT intrusion detection and incident response capabilities.

This work proposes an integration of SFL and cloud-based SDN for IoT intrusion detection and response. SFL promotes collaborative learning among IoT devices while ensuring data privacy and reducing bandwidth constraints. By segmenting the IoT network into clusters, SFL enhances model training and updates while preserving sensitive data confidentiality. Additionally, cloud resource integration enhances the scalability and robustness of the IDS. Cloud platforms offer significant computational and storage capabilities to support intensive intrusion detection processing tasks. Moreover, the cloud's elasticity facilitates scalable responses to varying workloads and evolving threats.

By amalgamating the capabilities of SDN, FL, and cloud computing, our study aims to contribute to the advancement of resilient and adaptable security measures for IoT environments. The suggested framework can help improve rapid threat identification, expedite response to incidents, and strengthen the robustness of IoT infrastructures against evolving cyber hazards.

*Corresponding author. Email: anas.harchi@gmail.com

Initially, the core Foundational Knowledge will be presented. An examination of the pertinent literature will be subsequently carried out in the following section. The following section will focus on the methodology with a subsequent discourse, delving into prospective avenues for research.

2. CHALLENGES AND LITERATURE REVIEW

2.1 Existing challenges in IoT environments

In contemporary times, there has been a notable escalation in both the volume and severity of aggressions aimed at IoT endpoints and cloud-based infrastructures. The matter of cybersecurity has ascended to prominence, considering the vulnerability of interconnected devices to cyberattacks and breaches of data integrity. The sheer scale of IoT deployments, as illustrated by the projected growth of connected devices in Figure 1, exacerbates these vulnerabilities.

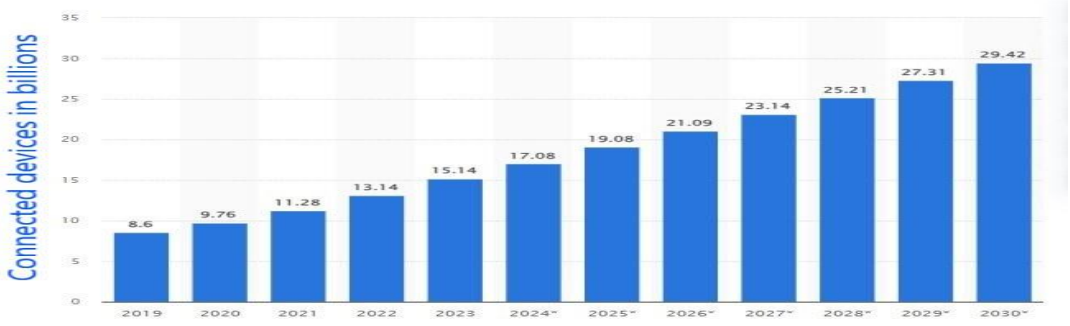

Fig. 1. Global Growth of Connected Devices (in Billions), 2019--2030. [1]

Furthermore, the challenge of interoperability arises, as a wide array of IoT devices frequently encounter difficulties in establishing efficient communication channels. The task of overseeing a vast number of interconnected devices poses a significant challenge within the current swiftly developing technological environment. With the continuous growth of the IoT, the intricacy of coordinating these interlinked systems has also increased. The provision of smooth communication, compatibility, and protection throughout such an extensive array of devices presents substantial obstacles. The increasing interconnectivity of a multitude of devices has resulted in the continuous generation of a substantial volume of data, encompassing both sensor information and user engagement activities. The increase in data volume projected to surpass 500% from 2019--2025, as shown in Figure 2, poses challenges in storage, processing, and analysis. Dealing efficiently with this vast quantity of data requires a robust infrastructure and advanced analytical skills.

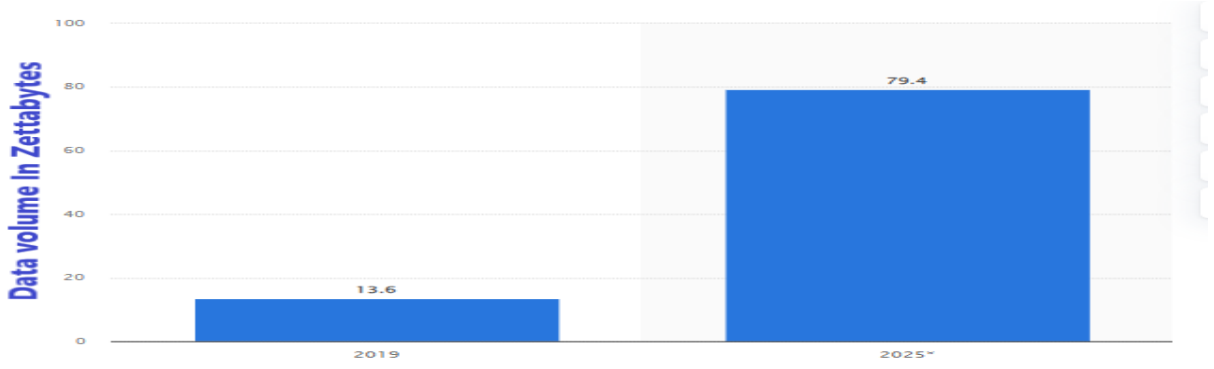

Fig. 2. Projected Growth of IoT Data Volume (in Zettabytes), 2019--2025. [2]

Ensuring user privacy in the face of extensive data collection remains a crucial issue, demanding clear policies and strong encryption protocols to countermeasure the interoperability and security challenges of the IoT.[3] Resource constraints on many IoT endpoints further complicate the integration of sophisticated security procedures directly on devices.

2.2 Literature Review on Security Approaches for the IoT

2.2.1 SDN and the Cloud for IoT Security

When considering the combination of SDN and the Cloud for enhancing IoT security, one crucial aspect to explore is the interoperability between SDN controllers and cloud-based security solutions. By leveraging the dynamic programmability of SDN in conjunction with the scalability and resource availability of the cloud infrastructure, a robust security framework

can be established for IoT devices. This cooperative synergy enables immediate monitoring, recognition of potential threats, and prompt response strategies to safeguard IoT ecosystems from imminent cyber risks, encompassing zero-day vulnerabilities and advanced persistent threats [4]. Furthermore, the enhanced security features are caused by the integration of SDN and the Cloud for IoT security; another critical aspect to consider is the utilization of artificial intelligence (AI) algorithms in threat detection and mitigation strategies. By incorporating AI-driven solutions into the security framework, IoT devices can benefit from advanced anomaly detection capabilities, predictive analysis of potential security breaches, and adaptive response mechanisms. These AI-powered tools can continuously learn and adapt to new cyber threats, ensuring a proactive defense mechanism that stays ahead of malicious activities targeting interconnected IoT networks [5].

2.2.2 Intrusion Detection in IoT

In cybersecurity, IDSs play a crucial role in safeguarding interconnected devices within the IoT. These systems are vital for monitoring network traffic, detecting potential vulnerabilities, and issuing alerts when unauthorized access or malicious activities are identified. By leveraging advanced algorithms and Machine Learning (ML) techniques, IDSs can effectively analyse patterns and anomalies in data flow to thwart cyber threats before they escalate [6]. As the IoT landscape continues to expand, robust and adaptive IDS solutions are paramount. Innovations such as blockchain for secure data transactions and decentralized storage are being explored to construct more resilient frameworks against data breaches and network vulnerabilities [7]. However, traditional IDSs often struggle with the scale and heterogeneity of IoT data and may impose significant computational loads, making them unsuitable for direct deployment on resource-constrained devices.

2.2.3 Securing IoT with FL

FL in IoT security has emerged as a revolutionary approach for processing and securing data within interconnected devices. By leveraging FL techniques, IoT networks can now collectively learn from decentralized data sources without compromising individual privacy or security. This methodology facilitates the creation of resilient models that augment the comprehensive resilience of systems in the face of threats to actors while simultaneously upholding data integrity among the diverse nodes within the network [8]. The implementation of FL in IoT security has not only enhanced data processing and security measures within interconnected devices but also paved the way for a more collaborative and privacy-preserving approach toward ML. This innovative technique enables IoT networks to collectively learn from distributed data sources without jeopardizing the confidentiality of individual information or network security. By adopting FL, robust models have been developed that enhance the comprehensive robustness of systems in the face of cyberattacks, thereby fortifying data integrity across different nodes in the network [9].

2.3 Incident Response Mechanisms

Traditional incident response mechanisms have long been the cornerstone of cybersecurity practices. However, as technology evolves and threats become more sophisticated, there is a growing need to adapt and innovate in this space. One emerging trend is the use of AI and ML algorithms in incident response strategies. By leveraging AI capabilities, organizations can improve their ability to detect, analyse, and respond immediately to security incidents, thereby strengthening their overall cyber-defense posture. This shift towards AI-driven incident response not only enables quicker threat identification but also empowers teams to proactively mitigate risks before they escalate [10].

The amalgamation of SDN with cloud-based systems has revolutionized the way in which cybersecurity incidents are handled. By leveraging the flexibility and centralized control offered by SDN in conjunction with the scalability and resource optimization of cloud computing, organizations can now respond to security threats with unprecedented speed and efficiency. This innovative methodology not only improves the identification and management of incidents but also optimizes the comprehensive incident response procedure, ultimately bolstering the resilience of modern digital infrastructures [11]. Furthermore, the combination of SDN and cloud-based incident response allows for real-time threat intelligence and automated responsive measures, enabling organizations to proactively defend against evolving cyber threats.

2.4 Related Works and Gap Analysis

2.4.1 Related Works: Overview of FL Approaches in IoT Security

The landscape of FL for IoT intrusion detection has evolved significantly, with early foundational works establishing core privacy-preserving principles while revealing fundamental challenges, as summarized in the comparative analysis in Table 1. Pioneering studies by Sun et al. [12] introduced segmented FL for large-scale networks, which demonstrated adaptability across diverse network participants but encountered stability issues and efficiency limitations for resource-constrained devices. Rey et al. [13] advanced the field by developing FL specifically for malware detection, showcasing real-world applicability through comprehensive performance comparisons with traditional approaches, yet exposing critical vulnerabilities to adversarial attacks and substantial synchronization requirements that hindered scalability. The integration of FL with software-defined networks (SDNs) gained prominence through Duy et al. [14], who achieved remarkable accuracy in anomaly detection for the Industrial IoT while maintaining privacy preservation, although their approach suffered from inadequate performance consumption optimization and persistent interoperability challenges.

TABLE I. SUMMARY OF RELATED WORKS ON FL AND SDN FOR IOT SECURITY, HIGHLIGHTING ADVANTAGES AND LIMITATIONS

Year	ML/DL Method	Ref.	SDN based	Segmentation-based	Advantage	Limitations
2020	FL	[12]	No	Yes	Good adaptability to various network participants	Stability of the learning model, Efficiency for IoT devices
2021	FL	[13]	No	No	Applicability to Real-World IoT Scenarios; Performance Comparison with Traditional Approaches	Limited Number of Clients Vulnerability to Adversarial Attacks; Synchronization Requirements
2021	FL	[14]	Yes	No	Privacy preservation; High-rate accuracy in anomaly detection	No emphasis on Performance consumption; Unsupported interoperability issue
2021	FL, Continual learning	[15]	No	No	Robustness to Hyperparameter Changes; Continual Learning Approaches; Heterogeneous Privacy Framework	Reduced Performance on Rarer Classes; Inherent Limitations of DP Algorithms; Dependency issue in dynamic or unpredictable environments
2022	FL, Energy Flow Classifier, Autoencoders	[16]	No	No	Improved Performance on Non-IID Data Superior to Traditional Methods using ML and DL algorithms	Generalization Capability in achieving satisfactory performance across diverse datasets
2022	FL	[17]	No	No	Privacy Preservation; Improved Efficiency; Collaborative Learning with FL and semisupervised learning	Scalability Issues when dealing with vast amounts of unlabelled data; Communication Overhead
2022	FL	[18]	Yes	No	High-rate accuracy; low power consumption	No emphasis on interoperability issue on general IoT devices
2022	SVM & KNN	[19]	Yes	No	Focus on Known Attack Vectors; Scalability and Robustness; Use of Multiple ML Techniques: Support Vector Machine (SVM), K-Nearest Neighbors (KNN)	Dataset Dependency; False Positive Rates; Performance Overhead
2023	FL	[20]	No	No	Privacy Preservation; Increased Accuracy; Noise considerations are integrated into FL.	Complexity in Implementation; Adaptability to new types of attacks
2023	FL	[21]	No	No	Privacy preservation improved, acceptable computation performance	Scalability with a higher number of devices and complex network
2023	FL	[22]	No	No	High-rate accuracy close to the accuracy of conventional centralized ML models; Improved Model Performance	No emphasis on interoperability; Scalability Issues; Communication Overhead
2023	FL	[23]	Yes	No	High Detection Accuracy; Low False Positive Rate; Enhanced Network Management	Potential for Overfitting; Dependence on Quality of Training Data
2023	Random Subspace Learning, KNN, AFSA, HSAFS	[24]	Yes	No	Efficient Attack Detection: By employing the Harmony Search algorithm based Feature Selection (HSAFS) method; Optimization of Detection Process using Artificial Fish Swarm Algorithm (AFSA) Experimental Validation	Adaptability to New Threats; Scalability Issues; Dependence on Quality of Data; Complexity in Implementation
2023	SVM & Decision Tree	[25]	Yes	No	High-rate accuracy in detecting attacks in industrial IoT.	interoperability issue on general IoT devices; No emphasis on privacy and performance
2023	FL, Deep Belief Networks, Deep Neural Networks	[26]	No	No	Enhanced Data Privacy; Scalability and Performance with Realistic Evaluation Conditions; Improvement with Pretraining	Heterogeneous Data Impact; Realistic Data Distribution Conditions; Data Normalization Challenges; Dependence on Pretrained Models

Contemporary research has focused on sophisticated methodologies addressing privacy, scalability, and performance optimization through innovative architectural designs. Chathoth et al. [15] introduced groundbreaking integration of FL with differential privacy neural networks and continual learning, demonstrating exceptional robustness to hyperparameter changes while establishing heterogeneous privacy frameworks, although significant performance degradation for rare attack classes was encountered. Bertoli et al. [16] developed stacked-unsupervised FL approaches specifically designed for heterogeneous networks, which achieve superior performance on non-IID data compared with centralized methods but face generalizability limitations across diverse datasets. Recent domain-specific implementations have targeted specific IoT operational environments: Friha et al. [18] developed FELIDS for agricultural IoT applications that achieve high detection accuracy with low power consumption, whereas multiple researchers have explored SDN integration with varying degrees of success [19, 20, 22, 23, 24], as detailed in the comparative analysis table showing their respective advantages and limitations.

2.4.2 Critical Research Gaps

The comprehensive analysis reveals a fragmented landscape where individual solutions excel in specific domains but fail to address holistic requirements of modern IoT ecosystems. While privacy preservation has been consistently achieved across multiple studies [12, 14, 15, 17, 20, 21, 26], scalability challenges remain pervasive, with most solutions [13, 15, 17, 19, 21, 22, 24] encountering limitations when dealing with large-scale deployments and complex network topologies. Communication overhead emerges as a critical bottleneck [13, 17, 22, 25], significantly impacting real-time performance requirements essential for effective intrusion detection. Interoperability issues persist across heterogeneous IoT environments [12, 14, 18, 25], with most approaches lacking comprehensive solutions for diverse device capabilities and communication protocols. The analysis demonstrates that no existing approach comprehensively integrates dynamic segmentation, SDN orchestration, real-time response capabilities, and privacy preservation in a unified, scalable framework, necessitating holistic solutions that can dynamically adapt to diverse IoT environments while efficiently managing resources across heterogeneous devices. The critical analysis of these works results in several persistent gaps:

- ☒ Device Heterogeneity and Resource Constraints: Many FL solutions do not adequately cater to the wide variance in the computational capabilities of IoT devices, leading to the exclusion of weaker nodes or inefficient training.
- ☒ Communication Overhead and Scalability: Transmitting full model updates in large-scale IoT networks remains a significant bottleneck, impacting latency and energy consumption.
- ☒ Lack of Integrated Dynamic Segmentation and Orchestration: While some works explore segmentation or SDN independently, a unified framework that combines adaptive model segmentation is needed.
- ☒ Real-Time Adaptability and Response: Traditional FL lacks the ability to respond immediately to detected threats, a capability that SDN can provide.
- ☒ Interoperability and Stability in Diverse Environments: Ensuring stable learning and interoperability across highly heterogeneous and dynamic IoT ecosystems remains a challenge.

A comprehensive solution that effectively merges adaptive segmentation of IoT devices with SDN orchestration for real-time, scalable, and privacy-conscious intrusion detection across diverse IoT ecosystems appears to be an area that warrants further exploration. In the next section, we present the proposed architecture.

3. DESIGN OF THE PROPOSED SCHEME

3.1 Objectives

This paper introduces a novel security framework that integrates **SFL** with **SDN** and cloud computing to enhance detection and response in IoT domains. The proposed design addresses critical challenges in scalability, privacy preservation, and real-time threat mitigation by leveraging the programmability of SDN and the distributed efficiency of the SFL. The key objectives of this study are as follows:

- **To design a hybrid SDN-cloud architecture** that enables centralized, dynamic network control for rapid security incident response in distributed IoT systems.
- **To implement SFL** as a privacy-preserving collaborative learning framework, IoT devices train localized model segments without sharing raw data.
- **To improve intrusion detection accuracy**, model segmentation can be optimized on the basis of device capabilities, ensuring efficient resource utilization.
- **To reduce detection latency** through real-time SDN reconfiguration and automated threat mitigation strategies.
- **To enhance scalability,** we dynamically allocate computational tasks across cloud and edge resources, accommodating heterogeneous IoT networks.

- **To introduce an adaptive model segmentation strategy** that tailors SFL submo0064els to device constraints (e.g., computing power and memory), maximizes participation and detection performance, and directly addresses the noninclusivity of resource-constrained devices
- **To ensure cross-platform compatibility** with existing IoT security protocols and diverse device ecosystems.

The proposed framework advances current approaches by unifying SFL's decentralized, privacy-aware training with SDN's programmable traffic management. Unlike conventional FL, which relies on a single global model, our methodology partitions the learning process into optimized segments, reducing communication overhead and computational strain. The SDN controller orchestrates critical functions—including device clustering, anomaly detection, and network policy updates—to enable an immediate threat response. Additionally, the adaptive segmentation mechanism intelligently distributes model fragments on the basis of real-time device conditions, ensuring equitable participation across resource-constrained nodes. By integrating these innovations, the framework achieves a robust, scalable, and energy-efficient security solution.

3.2 Model Architecture

The architecture presented in Figure 3 exemplifies a hierarchical FL system specifically designed for IoT environments, integrating Cloud, SDN, and IoT layers to facilitate the efficient management of decentralized model training. The Cloud Layer accommodates the Global FL Server (GFLS), which is responsible for the initiation and coordination of the global model. Within this layer, each segmented FL server (SFLS) oversees model training in a cluster (e.g., C1, C2), thereby enabling resource-efficient updates tailored for heterogeneous IoT devices. Performance metrics, including segment accuracy and gradient variance, are routinely evaluated within the GFLS to ascertain uniform learning across various clusters. Each SFLS executes a weighted segment aggregation procedure predicated on the quality of the updates received, employing trust-weighted averaging or momentum-based fusion methodologies to achieve stability in the learning process. The SDN layer functions as an orchestration layer, wherein an SDN controller is tasked with segmentation, network orchestration, and incident response. This controller adeptly routes data, manages traffic, and ensures security through real-time monitoring and threat containment, effectively linking the cloud infrastructure and IoT devices via both northbound and southbound interfaces. The IoT layer encompasses a variety of IoT devices, including robots, vehicles, and sensors, which engage in localized model training on the basis of segmented models received from the cloud. These devices transmit updates via the SDN layer, where aggregation and orchestration processes are executed. This multilayered architecture significantly enhances scalability, security, and adaptability within the FL paradigm, optimizing resource utilization and safeguarding data across IoT ecosystems.

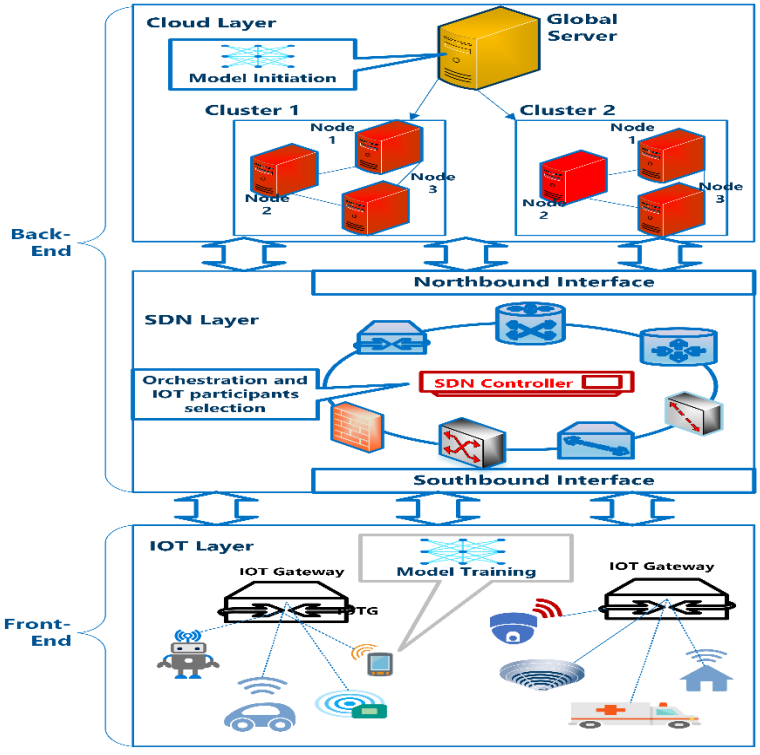

Fig. 3. Proposed Multi-Layered Architecture for SDN-Cloud Incident Detection and Response with SFL for IoT

Each IoT endpoint interfaces with a segmentation engine regulated by the SDN controller, which dynamically assesses a spectrum of parameters, including device functionalities, data pertinence, trustworthiness levels, and communication dependability, to allocate an appropriate subset of model parameters for training. In contrast to traditional FL methodologies that disseminate a uniform global model to all nodes, this context-sensitive and adaptive segmentation guarantees that each device acquires a customized model segment aligned with its operational profile and contribution potential. The system architecture comprises three strata: the IoT layer, which consists of terminal devices; the SDN layer, which is accountable for orchestration, segmentation, and routing; and the Cloud layer, which accommodates the GFLS and oversees centralized aggregation and storage.

3.3 Key Contributions

The proposed SFL model presents multiple significant contributions that effectively mitigate the prevailing shortcomings associated with FL in heterogeneous IoT environments. These contributions serve to increase the efficiency, scalability, and security of distributed learning across various IoT networks:

- **Adaptive Hybrid Segmentation Strategy**: The proposed hybrid segmentation methodology serves to differentiate this framework by correlating each model segment with the authentic operational role of the device and its corresponding trust context. This SDN-oriented approach facilitates customized engagement, which is inclusive of low-resource nodes, while ensuring the preservation of scalability and precision of detection.
- **Privacy and Scalability Optimization**: The suggested architectural framework bolsters privacy by maintaining data in a localized context and augments scalability via the implementation of segmented training, thereby rectifying the constraints inherent in conventional FL and centralized IDS models.
- **SDN-Orchestrated Real-Time Response**: Utilizes SDN for effective clustering, segment allocation, and immediate intrusion response, enhancing capabilities absent in previous FL frameworks.
- **Improved Model Robustness and Fault Tolerance**: The SFL framework aims to ensure stability during device failures or communication disruptions in IoT environments. Segmenting the learning process mitigates the adverse effects of individual device failure on training outcomes. This modular approach enhances the resilience of the global model, enabling it to adapt to the evolving challenges of IoT networks.
- **Hierarchical Model Aggregation**: The proposed framework delineates the deployment of the SFLS and a GFLS, thereby facilitating effective localized training and promoting scalable synchronization on a global scale.
- **Detailed Implementation Plan and Evaluation Strategy**: An elaborate evaluation framework grounded in simulation methodologies is delineated, focusing on critical performance indicators, including latency, device engagement, and communication efficacy.

3.4 Functions & workflow of the proposed SFL-SDN framework

3.4.1 General Workflow of the Proposed SFL-SDN Framework

This segment elucidates the operational dynamics of the proposed SFL framework, explicating the processes involved in model segmentation, training, and incident response as they transpire across the IoT-SDN-cloud layers. Although comprehensive implementation is scheduled for future research endeavors, the present design and algorithm are predicated on pragmatic constraints identified in diverse IoT environments.

The workflow proposed in Figure 4 for SFL within IoT environments encompasses a meticulously organized, multifaceted approach aimed at optimizing distributed learning across diverse devices while simultaneously safeguarding privacy and augmenting capabilities for anomaly detection. Initially, each IoT device autonomously gathers data from its local surroundings, thereby engendering decentralized datasets throughout the network. To accommodate the heterogeneous attributes of IoT endpoints, such as computational limitations, data pertinence, levels of trust, and communication dependability, the proposed strategy incorporates an adaptive hybrid segmentation strategy. This methodology disaggregates the global model into more manageable, context-sensitive segments that are not only congruent with the computational capabilities of each device but also customized to align with its data efficacy and trustworthiness. This approach guarantees substantive engagement from all nodes, irrespective of their constraints, while simultaneously improving training efficacy and the overall robustness of the model. Segmentation is a dynamic process; the SDN controller systematically reassesses the allocation of segments at regular intervals or in response to significant occurrences such as hardware malfunctions, deterioration of trust metrics, or the integration of new devices. This practice facilitates real-time responsiveness in the context of rapidly evolving IoT landscapes.

This workflow is designed on the basis of insights and methodologies established in our earlier work [27], which provided the foundational principles for FL in IoT environments. Building upon that framework, we integrate segmentation and SDN-based incident response to address scalability and interoperability challenges.

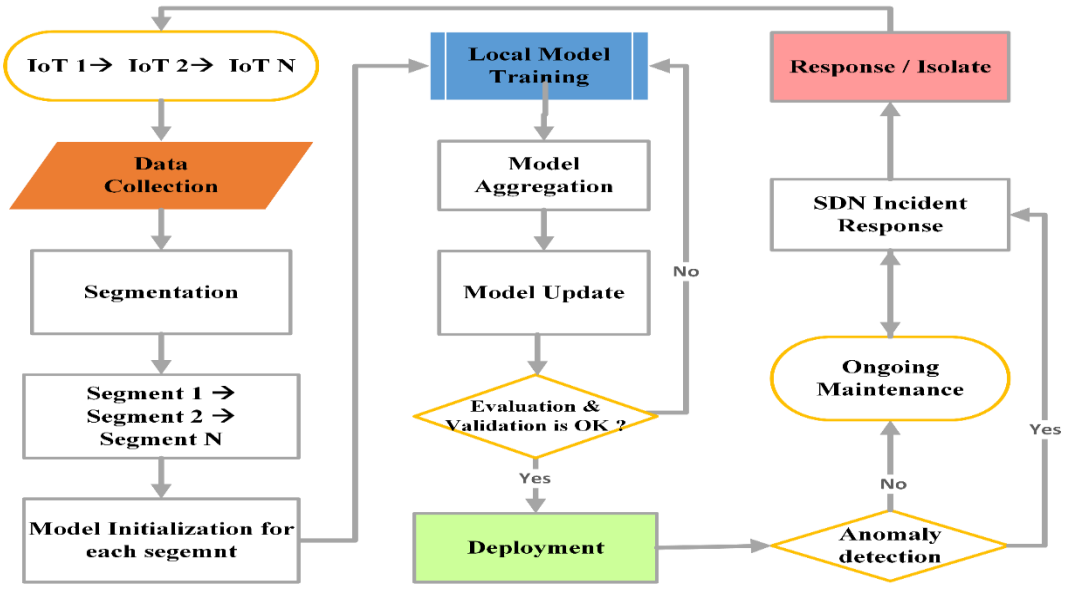

Fig. 4. General workflow of the proposed SFL-SDN framework for IoT intrusion detection and response

The overarching workflow comprehensively exemplifies the complete end-to-end process of the proposed SFL-SDN framework. It distinctly articulates the interactions among IoT devices, the SDN controller, the federated server, and the segmentation logic.

3.4.2 Parameter-Driven Segmentation and Trust-Oriented Allocation Strategy

Our framework employs an adaptive segmentation strategy based on a weighted score function, which is implemented in accordance with the guidelines established in [28]. This approach enables the precise allocation of model segments tailored to device capability, trust, and data context. Each model parameter p_j is evaluated for a given device d_i via the following scoring function:

$$Score(p_j,d_i)=\alpha_1 \cdot CompMatch(p_j,d_i)+\alpha_2 \cdot Relevance(p_j,d_i)+\alpha_3 \cdot Trust(d_i)+\alpha_4 \cdot DataAffinity(p_j,d_i)$$

where:

- CompMatch: computational compatibility (based on CPU/RAM/energy)
- Relevance: importance of the parameter to the device's task/data type
- Trust: node's historical integrity and behavior score
- DataAffinity: match between the parameter's function and the device's dataset

The coefficients $\alpha_i \in [0,1]$ control the influence of each factor:

- **Empirical tuning** is applied during simulation to find combinations that optimize accuracy, latency, and overhead.
- **Contextual adaptation** in deployment prioritizes trust (α_3) in adversarial settings or compatibility (α_1) in heterogeneous environments.

$$S_i=\{p_j \in P \mid Score(p_j,d_i) \geq \theta_i\}$$

Here, θ_i represents a variable threshold derived from the capabilities of the device and the established training priorities.

The trust metric is calculated as follows:

- SDN-flagged **anomaly reports,**
- **Update coherence** with expected gradients,
- Historical **participation reliability.**

Low-trust devices may receive fewer critical segments or be excluded entirely, reinforcing the system's resilience to poisoning or failure. This methodology significantly augments the resilience of the model and fosters substantial engagement from a diverse array of devices operating within the SFL framework. **Table II** illustrates this allocation across device types.

TABLE II. ILLUSTRATIVE EXAMPLE OF SCALABLE PARAMETER ALLOCATION AND TRAINING FREQUENCY IN THE SFL FOR DIVERSE IOT DEVICE TYPES

Device Type	**Resources**	**Assigned Segment**	**# Parameters**	**Training Frequency**
Sensor Node	Low (CPU, RAM)	Segment 1	5,000	Once per 3 rounds
Smart Camera	Medium	Segment 2	10,000	Once per 2 rounds
IoT Gateway	High	Segment 3	50,000	Every round

This table illustrates a singular result of the hybrid scoring methodology. While the dimensions of the segments align with the capabilities of the devices depicted in this illustration, the actual allocations are determined through the hybrid scoring mechanism, which additionally takes into account factors such as trust, task pertinence, and data affinity.

This dynamic, SDN-orchestrated process signifies a significant shift from conventional FL methodologies that depend on a static and homogeneous distribution of models. It guarantees that each IoT endpoint plays a substantial role, commensurate with its capabilities and its contextual relevance within the learning ecosystem. Upon the identification of an anomaly, the SDN controller commences the process of updating flow rules to isolate the compromised node effectively and subsequently reallocates roles in the forthcoming training cycle. These responsive interventions are implemented in real time, thereby minimizing latency and preserving the continuity of training.

3.4.3 Parameter Determination Details

The precise calibration of the weighting coefficients (α_i) is planned through an iterative optimization methodology executed within the simulation phase. This approach systematically assesses various αi combinations, potentially utilizing techniques such as grid search or more sophisticated Bayesian optimization, against key performance indicators such as detection accuracy, response latency, and resource utilization under diverse simulated IoT scenarios. The contextual adaptation of these coefficients, for instance, prioritizing trust (α_3) in suspected adversarial conditions, will be guided by predefined policies triggered by network state analytics provided by the SDN controller, allowing for dynamic adjustment on the basis of the operational context.

Determining the adaptive threshold (θ_i) for each device involves a dynamic calculation performed by a dedicated module, likely residing in the SDN controller or a management plane component. This calculation will directly map real-time device resource metrics (e.g., processing capacity, memory availability, reported energy levels) and current network trust assessments against the overarching strategic training priorities, such as balancing model segment complexity with device participation rates. This ensures that θ_i is responsive to both the instantaneous capabilities of individual devices and the broader objectives set for the learning cycle, facilitating more nuanced and effective segmentation.

The establishment of these training priorities is envisioned as a configurable aspect of the system on the basis of strategic operational goals such as maximizing detection coverage across diverse device types, minimizing false positives in critical segments, or explicitly favouring energy conservation on battery-powered nodes. These high-level priorities are translated into quantifiable target functions or constraint sets that directly influence the dynamic calculation of θ_i and the optimization objectives for the α_i coefficients. Furthermore, initial baseline values and permissible operational ranges for both α_i and θ_i will be established from domain knowledge, literature on FL in heterogeneous IoT environments, and refined through preliminary simulation experiments to ensure a robust starting point for the detailed, adaptive optimization processes.

3.4.4 Algorithm workflow for the SFL-SDN framework

The provided algorithm outlines the framework's core functions—model segmentation, localized training, secure aggregation, anomaly detection, and SDN-based incident response—serving as a foundational blueprint for its future implementation. While this algorithm captures the methodology's key rationale, the actual execution and detailed parameter refinement are planned for subsequent research phases. The immediate goal is to evaluate the framework's effectiveness across various IoT devices, with a focus on metrics such as detection accuracy, training efficiency, communication load, and responsiveness in dynamic settings. This algorithmic design is crucial for building a comprehensive system whose later execution is expected to validate the model's scalability, security, and operational efficiency within complex IoT environments.

Algorithm 1: Adaptive Segmented Federated Learning with SDN-Based Real-Time Threat Response

```
Input: IoT_devices (D1, D2, ..., DN), initial_global_model
Output: aggregated_global_model_Mglobal_ready_for_deployment
//1. Data Collection
Function DataCollection(devices):
    collected_data_phi = {}
    For each device d_i in devices:
        D_i_data = CollectLocalData(d_i)
        collected_data_phi[d_i] = D_i_data
    Return collected_data_phi

//2. Model Segmentation and Initialization
Function InitializeSegments(devices, global_model):
    For each device d_i in devices:
        segment_i = SegmentModel(global_model, D_i_resources)//Assumes D_i_resources is known
        InitializeModel(d_i, segment_i)

//3. Local Model Training
Function LocalTraining(devices, data, epochs):
    local_models = {}
    For each device D_i in devices:
        w_i = InitializeLocalWeights()//Or get from segmented initialization
        For e in 1 to epochs:
            For batch b_data in data[D_i]://Assuming data is structured per device
                g = ComputeGradient(D_i, w_i, b_data)
                w_i = ClientOptimizer(w_i, g, learning_rate, etc.)//Optimizer like SGD
        local_models[D_i] = w_i
    Return local_models

//4. Model Aggregation
Function ModelAggregation(local_models):
    M_global = Aggregate(local_models)//e.g., Federated Averaging
    Return M_global

//5. Model Update
Function UpdateGlobalModel(devices, M_global)://This seems to imply distributing the new global model
    For each device D_i in devices:
        UpdateModel(D_i, M_global)//Client updates its local model to new global model

//6. Evaluation and Validation
Function ValidateModel(devices, M_global, data):
    isValid = True
    For each device D_i in devices:
        If not ValidateModelOnDevice(M_global, data[D_i])://Assuming data[D_i] is validation data
            isValid = False
            Break//Exit early if any device fails validation
    Return isValid

//Main Algorithmic Execution
Devices = {D1, D2, ..., DN}
Data = DataCollection(Devices)
InitializeSegments(Devices, GlobalModel)//Initial GlobalModel

Repeat:
    LocalModels = LocalTraining(Devices, Data, epochs)
    M_global = ModelAggregation(LocalModels)
    UpdateGlobalModel(Devices, M_global)//Distribute new M_global for next round or for validation

    If ValidateModel(Devices, M_global, Data) then//Assuming Data contains validation subsets
      //Proceed to deployment if validation is OK
        DeployModel(Devices, M_global)//Or mark M_global as ready
        Break//Exit loop if model is validated and deployed
    Else:       //Continue training or adjust parameters

//7. Anomaly Detection and Maintenance
Function AnomalyDetectionAndMaintenance(devices):
    For each device D_i in devices:
        If DetectAnomaly(D_i) then
            SDNIncidentResponse(D_i)
        Else:         PerformOngoingMaintenance(D_i)

//8. SDN Incident Response
Function SDNIncidentResponse(device):
    IsolateDevice(device)
    TriggerIncidentResponse(device)//Broader response actions
End Algorithm
```

3.5 Implementation and evaluation plan

The principal aim of the empirical assessment is to assess the SFL framework's effectiveness for IoT intrusion detection and incident response. Key goals include demonstrating improved detection accuracy, a reduced communication load, enhanced device interaction, and rapid responsiveness through SDN. Consequently, we outline essential performance metrics and expected results to guide our empirical analysis:

TABLE III. SUMMARY OF ASSESSMENT CRITERIA AND ANTICIPATED ADVANTAGES OF THE PROPOSED SFL FRAMEWORK

Metric	**Expected Impact**	**Justification**
Detection Accuracy	Increased	Segmentation allows devices with valuable local data to contribute effectively.
Incident Response Time	Decreased	SDN enables dynamic reconfiguration and real-time isolation of threats.
Training Time	Reduced	Devices train only on lightweight model segments tailored to their capacity.
Communication Overhead	Reduced	Only segment updates are shared instead of full model parameters.
Participation Rate	Increased	Even constrained devices can join training due to adaptive segmentation.
Model Robustness	Improved	Segment redundancy and SDN recovery reduce the impact of device failure.
Privacy Risk	Lowered	Raw data never leaves devices; segmentation further limits exposure.

The SFL-SDN framework is tested in a controlled simulation environment via tools such as Mininet for network emulation and TensorFlow for FL implementation. This evaluation focuses on key performance indicators, including detection accuracy (precision, recall, and F1 score), training duration per round, overall convergence time, communication overhead (bytes transmitted), device participation rates (especially for constrained devices), and incident response latency.

A synthetic IoT dataset, incorporating realistic network traffic and diverse temporal anomalies (e.g., DDoS, malware propagation, data exfiltration), will be utilized. Publicly available IoT security datasets (e.g., Bot-IoT, N-BaIoT) will be considered and potentially augmented to fit the specific SFL-SDN scenario. Emulated IoT devices with heterogeneous resource profiles perform local model training as federated clients. The SDN controller will manage network flows and implement real-time responses on the basis of alerts from the IDS components. The federated servers (SFLS and GFLS) use adaptive aggregation algorithms and track convergence across communication iterations. Metric trends are analysed, and comparative analyses against baseline standard FL models and centralized IDS approaches are conducted.

As part of the implementation strategy, the intrusion detection component will be enhanced by integrating new approaches inspired by recent advancements in the field [29], [30]. While these techniques have shown promising results in improving detection accuracy and robustness, their integration within the SFL-SDN framework—particularly under IoT constraints of heterogeneity and resource limitations—requires careful exploration. The plan is to investigate how best to adapt these methods in a way that preserves system scalability, minimizes overhead, and aligns with the adaptive segmentation and trust logic already established in the architecture. This exploration ensures that the IDS component is both effective and compatible with the distributed, segmented learning paradigm.

3.6 Results and Discussion

This segment delineates the expected advantages and efficacy of the proposed SFL framework, as inferred from its foundational architectural principles. Leveraging the literature review articulated within this manuscript, a concise comparative assessment is offered in the ensuing Table IV:

TABLE IV. CONCEPTUAL PERFORMANCE COMPARISON OF THE PROPOSED FRAMEWORK AGAINST BASELINE INTRUSION DETECTION METHODS

Method	Comm. Overhead	Device Inclusivity	Privacy Level	Response Latency	Energy Efficiency	Real-Time Support
Centralized IDS	High	Low	None	Fast	Low	Moderate
Standard FL	Medium	Medium	Moderate	Moderate	Medium	Moderate
Proposed SFL-SDN	Low	High	High	Very Fast	High	High

As demonstrated in Table IV, the SFL-SDN framework is anticipated to offer significant advantages over traditional centralized IDS approaches and standard FL methodologies across multiple critical dimensions for IoT security:

- Communication Efficiency (Low Overhead): The SFL-SDN framework is expected to achieve low communication overhead because devices transmit only updates for their assigned, potentially smaller, model segments instead of full model parameters (as in standard FL) or raw data (as in centralized IDS).
- Enhanced Privacy (High Level): By design, FL keeps raw data localized on IoT devices, which is a fundamental privacy enhancement over centralized systems. SFL may further enhance this, as each device only trains and shares updates for a segment of the global model, potentially limiting the scope of information that could be inferred from any single update.
- Device Inclusivity (High): The adaptive hybrid segmentation strategy is a core innovation designed to achieve high device inclusivity. By tailoring model segments to device capabilities, data relevance, and trust, even resource-constrained IoT devices, typically excluded from complex FL tasks, can meaningfully participate. This contrasts sharply with centralized IDSs, which require powerful devices, and standard FL often assumes more homogeneity.
- Real-Time Response (Very Fast Latency): The integration of SDN is pivotal for achieving a very fast incident response. Upon detection of an anomaly, the SDN controller can dynamically reconfigure network flows in real time to isolate compromised devices or mitigate attacks. This programmable and centralized control allows for much faster reaction times than traditional reactive mechanisms or slower consensus cycles of standard FL without SDN integration.
- Scalability: The combination of segmented learning and hierarchical aggregation (SFLS and GFLS) is designed to support a growing number of diverse IoT endpoints and varied data types without overwhelming central servers or the network. This creates a more sustainable and scalable security framework.
- Energy Efficiency (High): Optimized power consumption is anticipated through reduced communication (smaller segment updates) and potentially reduced local computation. This is vital for extending the operational lifespan of battery-powered IoT devices, which is a significant concern in many IoT deployments.
- Real-Time Support (High): Beyond rapid incident response, the SDN component enables continuous, real-time monitoring and dynamic policy enforcement, which, combined with the adaptive nature of SFL, provides robust real-time security support for dynamic IoT environments.

The SFL-SDN framework directly addresses the limitations identified in prior work by offering enhanced performance and adaptability. While Sun et al.'s segmented FL-IDS [12] achieved good adaptability, it struggled with stability concerns and efficiency limitations for resource-constrained devices. This framework overcomes these challenges by incorporating dynamic segmentation strategies that enable effective participation from devices with diverse computational capabilities. Similarly, Rey et al.'s FL approach [13] and Aouedi et al.'s FLUIDS [17] faced communication overhead and scalability challenges; the SFL-SDN mitigates these challenges by sharing only segment updates instead of full model parameters, significantly reducing communication demands and improving scalability in complex systems. Furthermore, unlike approaches such as that of Alshammari and Alserhani [19], who introduced noise for privacy but encountered implementation complexities and adaptability issues to emerging attack types, the SFL approach prioritizes privacy through data locality while aiming for a more streamlined and adaptive segmentation process facilitated by SDN orchestration. The analysis demonstrates that no existing approach comprehensively integrates dynamic segmentation, SDN orchestration, real-time response capabilities, and privacy preservation in a unified, scalable framework, necessitating the holistic solution proposed through the SFL-SDN approach.

The strength of the proposed framework lies in this synergistic integration. SFL makes distributed learning feasible and efficient for heterogeneous IoT devices, whereas SDN provides the network-level agility and control necessary for dynamic segmentation, efficient communication, and rapid incident response. The cloud layer offers the necessary computational backbone for global model aggregation and complex analytics. This holistic approach is anticipated to provide a more robust, scalable, and responsive security solution than systems relying on FL, SDN, or cloud computing in isolation or in simpler combinations. The planned simulation studies will be crucial in quantifying these expected advantages and empirically validating the framework's performance against existing methods.

4. CONCLUSION & FUTURE WORK

The safeguarding of IoT environments remains a paramount concern within computer information science, which is attributable to the intricate, heterogeneous, and sensitive nature of interconnected devices. This research presents a comprehensive framework that amalgamates SFL, SDN, and cloud computing to facilitate scalable, privacy-preserving mechanisms. By upholding data locality, enabling immediate threat response, and dynamically adapting model segments to align with device profiles, the proposed system proficiently addresses three fundamental security dimensions: (1) data confidentiality, (2) swift detection and containment, and (3) interoperability across various IoT ecosystems. The architecture fosters inclusive participation by tailoring training tasks to correspond with device capabilities, trust levels, and data

pertinence—thereby eliminating the necessity for centralized aggregation or homogeneous models. Although the methodology has considerable potential, its practical application necessitates further scrutiny to confront prospective deployment and orchestration challenges.

In the forthcoming phase of the research initiative, our attention will shift toward the implementation of the proposed architecture to convert the extant theoretical model into a fully operational system. This endeavor will necessitate the coding of the devised algorithms and segmentation logic within an operational framework capable of processing IoT data and executing intrusion detection decisions. Subsequent to the implementation phase, a series of empirical experiments are conducted to evaluate the detection accuracy, training efficiency, and system robustness across a variety of IoT scenarios. Particular emphasis will be placed on juxtaposing the SFL methodology with both conventional FL and centralized intrusion detection systems to ascertain its practical advantages.

Moreover, it is imperative to recognize that the current design predicates a fundamental level of trust in the SDN controller and presently lacks mechanisms to authenticate the integrity of gradient updates, which could mitigate the risk of model poisoning attacks. Furthermore, challenges such as segment drift and latency variability among clusters may adversely impact performance in large-scale deployments—these issues are earmarked for future examination.

Conflicts of interest

The authors declare that they have no conflicts of interest.

Funding

This research did not receive any financial support.

Acknowledgement

We would like to extend our earnest appreciation to the unnamed evaluators for their time, exertion, and perceptive critiques. Their constructive observations and recommendations will indisputably facilitate the enhancement of the quality and precision of this endeavour. We value their contributions to the advancement of this scholarship.

REFERENCES

[1] R. Qamar and B. A. Zardari, “An Analysis of the Internet of Everything,” Mesopotamian Journal of CyberSecurity, vol. 2023, pp. 85–92, 2023, doi: 10.58496/MJCS/2023/013.

[2] Statista Research Department, “Internet of Things (IoT) connected devices installed base worldwide from 2019 to 2030,” Statista, 2024. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

[3] Statista Research Department, “Volume of data created by Internet of Things (IoT) connected devices worldwide in 2019 and 2025,” Statista, 2024. [Online]. Available: https://www.statista.com/statistics/1017863/worldwide-iot-connected-devices-data-size/.

[4] R. zaib and K.-Q. Zhou, “Zero-Day Vulnerabilities: Unveiling the Threat Landscape in Network Security,” *Mesopotamian Journal of CyberSecurity*, vol. 2022, pp. 57–64, 2022, doi: 10.58496/MJCS/2022/007.

[5] S. Mishra, “SDN-Based Secure Architecture for IoT,” International Journal of Knowledge and Systems Science, vol. 11, no. 4, pp. 1–16, Oct. 2020, doi: 10.4018/IJKSS.2020100101.

[6] A. J. Meera, M. V. V. P. Kantipudi, and R. Aluvalu, “Intrusion Detection System for the IoT: A Comprehensive Review,” *Springer, Cham*, [Online]. Available: https://doi.org/10.1007/978-3-030-49345-5_25.

[7] T. Sherasiya and H. Upadhyay, “Intrusion Detection System for Internet of Things,” International Journal of Advance Research and Innovative Ideas in Education, vol. 2, pp. 2344–2349, 2016, [Online]. Available: https://api.semanticscholar.org/CorpusID:212444575.

[8] C. B, B. M. Sundaram, S. B. Reddy, S. S. K and S. Kotturi, "An Explorative Analysis of IoT Security on Federated Intelligent Networks," 2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2022, pp. 1-7, doi: 10.1109/SMARTGENCON56628.2022.10083746.

[9] M. B. Alazzam, F. Alassery, and A. Almulihi, “Federated Deep Learning Approaches for the Privacy and Security of IoT Systems,” *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–7, Apr. 2022, doi: 10.1155/2022/1522179.

[10] S. Ossenbühl, J. Steinberger, and H. Baier, “Towards Automated Incident Handling: How to Select an Appropriate Response against a Network-Based Attack?,” 2015, doi: 10.1109/IMF.2015.13.
[11] F. Patzer, A. Meshram, and M. Heß, “Automated Incident Response for Industrial Control Systems Leveraging Software-defined Networking,” pp. 319–327, Jan. 2019, doi: 10.5220/0007359503190327.
[12] Y. Sun, H. Ochiai and H. Esaki, "Intrusion Detection with Segmented Federated Learning for Large-Scale Multiple LANs," 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, 2020, pp. 1-8, doi: 10.1109/IJCNN48605.2020.9207094.
[13] V. Rey, P. M. Sánchez Sánchez, A. Huertas Celdrán, and G. Bovet, “Federated learning for malware detection in IoT devices,” Computer Networks, vol. 204, p. 108693, 2022, doi: 10.1016/j.comnet.2021.108693.
[14] P. T. Duy, T. V. Hung, N. H. Ha, H. D. Hoang and V. -H. Pham, "Federated learning-based intrusion detection in SDN-enabled IIoT networks," 2021 8th NAFOSTED Conference on Information and Computer Science (NICS), Hanoi, Vietnam, 2021, pp. 424-429, doi: 10.1109/NICS54270.2021.9701525.
[15] A. K. Chathoth, A. Jagannatha, and S. Lee, “Federated Intrusion Detection for IoT with Heterogeneous Cohort Privacy,” 2021, doi: 10.48550/arXiv.2101.09878.
[16] G. Bertoli, L. Alves Pereira Junior, O. Saotome, and A. Santos, “Generalizing intrusion detection for heterogeneous networks: A stacked-unsupervised federated learning approach,” *Computers & Security*, vol. 127, p. 103106, Apr. 2023, doi: 10.1016/j.cose.2023.103106.
[17] O. Aouedi, K. Piamrat, G. Muller and K. Singh, "FLUIDS: Federated Learning with semi-supervised approach for Intrusion Detection System," 2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2022, pp. 523-524, doi: 10.1109/CCNC49033.2022.9700632.
[18] O. Friha, M. A. Ferrag, L. Shu, L. A. Maglaras, K.-K. R. Choo, and M. Nafaa, “FELIDS: Federated learning-based intrusion detection system for agricultural Internet of Things,” *Journal of Parallel and Distributed Computing*, vol. 165, pp. 17–31, Mar. 2022, doi: 10.1016/j.jpdc.2022.03.003.
[19] T. M. Alshammari and F. Alserhani, “Scalable and Robust Intrusion Detection System to Secure the IoT Environments using Software Defined Networks (SDN) Enabled Architecture,” International journal of computer networks and applications, vol. 9, no. 6, p. 678, Dec. 2022, doi: 10.22247/ijcna/2022/217701.
[20] P. Ruzafa-Alcázar et al., "Intrusion Detection Based on Privacy-Preserving Federated Learning for the Industrial IoT," in IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 1145-1154, Feb. 2023, doi: 10.1109/TII.2021.3126728.
[21] M. Nakıp, B. C. Gül, and E. Gelenbe, “Decentralized Online Federated G-Network Learning for Lightweight Intrusion Detection,” Oct. 2023, doi: 10.1109/mascots59514.2023.10387644.
[22] M. M. Rashid, S. U. Khan, F. Eusufzai, Md. A. Redwan, S. R. Sabuj, and M. Elsharief, “A Federated Learning-Based Approach for Improving Intrusion Detection in Industrial Internet of Things Networks,” Network, vol. 3, no. 1, pp. 158–179, Jan. 2023, doi: 10.3390/network3010008.
[23] M. N. Ali, M. Imran, M. S. u. din, and B.-S. Kim, “Low Rate DDoS Detection Using Weighted Federated Learning in SDN Control Plane in IoT Network,” Applied Sciences, vol. 13, no. 3, p. 1431, 2023, doi: 10.3390/app13031431.
[24] M. Maray *et al.*, “Optimal Deep Learning Driven Intrusion Detection in SDN-Enabled IoT Environment,” vol. 74, no. 3, pp. 6587–6604, Jan. 2023, doi: 10.32604/cmc.2023.034176.
[25] H. Alshahrani, M. S. Al Reshan, A. Sulaiman, and A. Shaikh, “Intrusion Detection Framework for Industrial Internet of Things Using Software Defined Network,” Sustainability, vol. 15, no. 11, p. 9001, Jun. 2023, doi: 10.3390/su15119001.
[26] O. Belarbi, T. Spyridopoulos, E. Anthi, I. Mavromatis, P. Carnelli, and A. Khan, “Federated Deep Learning for Intrusion Detection in IoT Networks,” pp. 237–242, Dec. 2023, doi: 10.1109/GLOBECOM54140.2023.10437860.
[27] A. Harchi, H. Toumi, and M. Talea, “Collaborative Cloud–SDN architecture for IoT privacy-preserving based on federated learning,” pp. 211–221, Oct. 2024, doi: 10.1201/9781032714806-14.
[28] D. J. White, “Multiple Attribute Decision Making – A State-of-the-Art Survey,” Journal of the Operational Research Society, vol. 33, no. 3, p. 289, Mar. 1982, doi: 10.1057/JORS.1982.61.
[29] A. A. Abdulhameed, S. A. H. Alazawi, and G. M. Hassan, “An optimized model for network intrusion detection in the network operating system environment,” Mesopotamian Journal of CyberSecurity, vol. 4, no. 3, pp. 75–85, 2024, doi: 10.58496/MJCS/2024/017.
[30] M. Subhi, O. F. Rashid, S. A. Abdulsahib, M. K. Hussein, and S. M. Mohammed, “Anomaly Intrusion Detection Method based on RNA Encoding and ResNet50 Model,” Mesopotamian Journal of CyberSecurity, vol. 4, no. 2, pp. 120–128, 2024, doi: 10.58496/MJCS/2024/011.