

Integrating Machine Learning–Driven Threat Detection with Advanced Cryptographic Solutions for Secure Cloud and Web Applications

Tanu Sharma*

School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi, Delhi, India

E-mail: sharmatan41@gmail.com

ORCID iD: <https://orcid.org/0009-0009-3311-7671>

*Corresponding Author

Farheen Siddiqui

School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi, Delhi, India

E-mail: fsiddiqui@jamiyahamdard.ac.in

ORCID iD: <https://orcid.org/0000-0002-0051-9094>

Khyati Chopra

University School of Automation and Robotics, Guru Gobind Singh Indraprastha University (GGSIPU), New Delhi, Delhi, India

E-mail: khyati.usar@ipu.ac.in

ORCID iD: <https://orcid.org/0000-0002-8852-8234>

Jawed Ahmed

School of Engineering Sciences and Technology, Jamia Hamdard, New Delhi, Delhi, India

E-mail: jahmed2047@jamiyahamdard.ac.in

ORCID iD: <https://orcid.org/0000-0001-6218-5301>

Received: April 3, 2026; Revised: May 10, 2026; Accepted: July 15, 2026; Published: August 8, 2026

Abstract: With the accelerated proliferation of cloud services and web-based applications, exposure to sophisticated cyber threats like zero-day vulnerabilities, advanced persistent threats, and application-layer attacks, has sharply increased. Conventional intrusion detection systems, along with cryptographic security mechanisms, often do not fulfill the requirements of adaptive detection, privacy preservation, and variety of scalability within distributed systems. To alleviate these problems, this paper suggests a cross-layer adaptive security model, which includes, in the secure cloud and web applications, machine learning-based anomaly detection complemented with advanced cryptographic security. The model combines, in this context, lightweight local anomaly detection, federated learning, selective privacy, and a deep reinforcement learning-based threat detection and security orchestration. Through federated learning, active participation in the learning process is assured, while the selective privacy mechanism preserves the model parameters. The deep reinforcement learning agent adjusts the interaction, aggregation, and privacy settings according to demands of the adaptive system and the environment. The assessment of the model is realized through the CSE-CIC-IDS2018, CIC-IDS2017, and the CSIC 2010 HTTP benchmark datasets to verify the model in detection, generalization, and operational effectiveness. The results of the performed tests reflect an accuracy of 97.9%, a F1 score of 97.5%, a false positive rate of 1.8%, and a detection latency of 36 ms, surpassing performance of conventional federated and centralized state-of-the-art models. Cross-dataset testing validates the model effectiveness in the presence of highly variable traffic. The results suggest that adaptive orchestration, federated learning, and selective privacy preservation, when combined, substantially boost intrusion detection, decrease communication overhead, and ensure privacy preservation. Therefore, this framework is a scalable and robust approach to intrusion detection within contemporary cloud and web settings.

Index Terms: Federated Learning, Deep Reinforcement Learning, Privacy-Preserving Security, Intrusion Detection Systems, Cloud Computing Security, Adaptive Threat Detection, Web Application Security, Distributed Cybersecurity

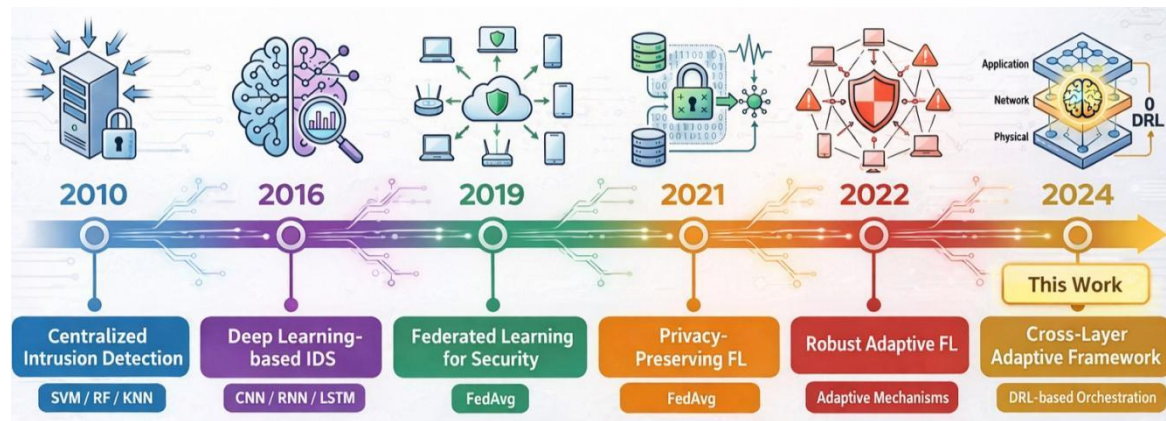


Fig. 1. Evolution of intrusion detection and privacy-aware learning approaches from centralized machine learning to the proposed cross-layer adaptive federated framework (2010–2024).

1. Introduction

Increasingly, services such as Software as a Service (SaaS), online services, digital commerce, fintech, healthcare, and other web and cloud-based services rely on rapidly scalable and accessible frameworks. Trust, privacy, and service reliability concern the client and regulatory requirements as well as the continuity of business operations [1, 2, 3]. Expanding cloud ecosystems and interconnected web applications comprise a widening range of available attacks. Modern web applications can be easily compromised through cross-site scripting (XSS), SQL injections (SQLi), and cross-site request forgery (CSRF) [4, 5, 6, 7]. Within the cloud, configuration errors, insecure APIs, multi-tenancy, and insider threats further extend the reach of the attack methods[8, 9]. and the web application can be difficult to secure. Recently, the industry identified that cloud service configurations account for over nearly 60% of incidents involving cloud services' compromised security, with web application services remaining one of the most exploited attack vectors [1, 10]. For this reason, there is a growing need for cybersecurity that is intelligent, adaptive, and privacy-preserving.

We can pinpoint developments in intrusion detection and privacy-preserving learning technologies over the decades. The early systems had centralized machine learning models. Data were collected and processed in a central location. The centralized systems were good at finding attack patterns, but had major issues, like privacy, bottlenecks in communications, and scalability. The problems became even more evident in cloud deployments. Centralized machine learning needed a lot of network traffic and user data, which meant both privacy problems and communication issues. Also, centralized systems had a lot of problems adapting to different environments. They also showed problems generalizing attack patterns that they hadn't seen before.

Federated Learning (FL) solved a lot of the problems centralized systems had. In FL, raw data don't need to be exchanged to collaboratively train models. Participating clients only share updates to the model, which greatly lessens the risks to privacy. Emerging research in FL intrusion detection shows that the systems can maintain a good detection level of performance, even when a lot of data is exposed. A lot of existing FL systems use the same privacy settings and are inflexible and unresponsive to changes. Privacy-preserving techniques based in cryptography often result in a lot of extra calculation and communication to be done, which limits their use in systems that are resource-constrained.

It is very challenging to detect intrusions when cyber attacks become more technical. Polymorphic, obfuscated, adversarial, and zero-day attacks, which are on the rise, avoid detection by signature-based Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). These approaches do identify many traditional cyber attacks. However, they struggle to identify new attack behaviors. The same applies to traditional cryptographic solutions. They focus primarily on the confidentiality and integrity of the protected data. They fall short in the area of proactive threat detection. These combined factors have resulted in a gap in real-time threat detection, and private, secure data within distributed cloud environments.

Sophisticated intrusion detection systems take advantage of developments in machine and deep learning with Support Vector Machines, Random Forests, Convolutional Neural Networks, Autoencoders, Transformers and other architectures [11, 12, 13, 14]. These systems are effective at detecting anomalous behaviors, including zero-day attacks. There are many challenges, including adversarial evasion attacks, and the problems of concept drift, data heterogeneity, and slow model updates, all of which affect the accuracy and reliability of detection. Many methods are also static and operate within inflexible frameworks for making detection decisions. Therefore, there are significant gaps in research and implementation regarding the systems' ability to adapt to changing network conditions and volatile threat environments [11, 12, 5]. Research published in the years 2024–2026 is increasingly focused on adaptive security systems that combine learning with the ability to make decisions autonomously and preserve user privacy [15, 16, 17].

Deep Reinforcement Learning (DRL) has an edge since it can optimize during the process. Cybersecurity systems have a lot of DRL-based systems for adaptive management. Other optimization methods are mostly static. These systems

can change the aggregation intervals, the strategies of the participants, the privacy parameters, and the communication policies. In a federated learning system, the state of the system is always changing. Client reliability is changing, and attacks can evolve. The flexibility of DRL is a great fit for the situation. However, the combination of DRL, privacy-preserving, and federated intrusion detection has not been addressed much.

Newer cryptography systems can protect data in the cloud and allow secure and controlled computation and data retrieval. Examples include homomorphic encryption and post-quantum cryptography. Modern cryptography methods suffer from a high cost in computation, managing secret keys, and an increase in communication. Because of that, real-time applications can suffer from a poor security and performance trade-off. This shows that enhanced cryptography systems can protect a system, computation, and data in the cloud but they can also limit security needs in other areas that require it, especially real time applications.

The evaluation methods used in the studies undertaken is another important limitation that needs to be addressed. Existing intrusion detection studies focus primarily on a few benchmark datasets such as CSE-CIC-IDS2018, CIC-IDS2017, and CSIC 2010 HTTP. Although these datasets help provide a reproducible and consistent evaluation, they are not as complex and are derived from controlled environments. Therefore, they do not represent the real-world diversity, complexity and the evolving dynamic nature of cloud traffic. Given this, models that have been trained and evaluated using benchmark datasets will have difficulties once deployed to dynamic production environments that involve concept drift, user behavioral changes, and new evolving attack patterns.

There is a considerable amount of studies on federated learning, intrusion detection with adaptation, and privacy-preserving security, however most of these studies focus solely on one of these components. The majority of existing approaches do not have

1. adaptive system-level orchestration
2. dynamic privacy-performance trade-off
3. systematic cross-layer optimization in distributed settings

These constraints demonstrate the necessity of an integrated approach that can deal with all of these factors simultaneously. To cope with some of these issues, a cross-layer adaptive security framework that combines federated learning, selective privacy preservation, lightweight local anomaly detection, and Deep Reinforcement Learning (DRL) orchestration is proposed. The key innovations of this research are:

- Suggested a new method for adaptive security at multiple levels. Included lightweight anomaly detection, federated learning, selective privacy preservation, and deep reinforcement learning (DRL) for orchestration.
- Developed a selective privacy preservation model. In this model, only sensitive model parameters get encrypted. This results in less computation and less communication overhead than a fully encrypted federated system.
- Developed a deep reinforcement (DRL) model for adaptive orchestration. This model dynamically adjusts aggregation intervals, privacy levels, client participation, and communication adaptable to varying network conditions.
- Developed a flexible interaction mechanism to device, edge and global intelligence layers. This enables coordinated security optimization and flexible decision-making.
- Enhanced detection accuracy, privacy protection, communication efficiency, and scalability. This model overcomes the issues present in most centralized and static federated intrusion detection models.
- Used various benchmark datasets (CSE-CIC-IDS2018, CIC-IDS2017, and CSIC 2010 HTTP) to test the developed model and framework. In these tests, this model was shown to perform better with accuracy, the F1 score, false positive rate, and detection latency.

The rest of this paper is structured as follows. Section 2 discusses previous studies about integration of machine learning technologies into threat detection methodologies and cryptographic engineering security mechanisms. Section 3 elaborates on the proposed architecture and method. Section 4 focuses on the specific experimental design and assessment approach employed. Section 5 provides the discussion on the obtained results as well as the assessment of the performance. Section 6 offers the concluding remarks and suggests the pathways for the future studies.

2. Related Work

The rapid growth of Cloud and Web Applications in SaaS, e-commerce, fintech, and health domains exposed a wider attack surface and more advanced cyber threats. Today's attack vectors include cross-site scripting (XSS), SQLI, DDoS, insider threats, and advanced multi-stage attacks. Empirical studies show how cloud environments fall prey to misconfigurations and insecure APIs, accounting for nearly 65% and 50% of the security risks respectively [19, 20]. In addition, large-scale studies of cloud real-life failures show misconfigurations, such as resource violations, dependency violations, and more [21]. Traditional security mechanisms such as rule-based firewalls, intrusion detection systems

(IDS), and intrusion prevention systems (IPS) become less effective against dynamic, contextual, and behavior-driven threats [18].

2.1. Machine Learning and Federated Learning-Based Intrusion Detection

Due to their advanced capabilities in pattern detection across diversified behavioral constructs within network systems and traffic, machine learning (ML) and deep learning (DL) have established themselves as viable technologies for intrusion and anomaly detection. Traditional ML techniques such as Support Vector Machines (SVM), Random Forest (RF), and ensemble methods are serviceable with structured datasets. However, they tend to underperform against advanced attack patterns and large-scale heterogeneous systems. In contrast, deep learning models including Convolutional Neural Networks (CNN), Long Short-term Memory (LSTM) networks, Autoencoders, and Transformers have outperformed in the detection of advanced and novel attack scenarios [22, 23, 24, 25]. Notwithstanding, these techniques still encounter issues such as explainability of high false positive, fragile to adversarial attacks, concept drift, and reliance on evaluation datasets [26, 27, 28, 29, 30, 31].

Federated Learning (FL) has become a useful alternative in dealing with privacy issues for distributed intrusion detections. Since FL does not require sharing raw data for models to learn, it minimizes privacy and regulatory concerns. The usage of FL for intrusion detection systems has been proven useful in IoT, cloud, and edge computing. Rahmati and Pagano introduced an FL-based framework for cybersecurity in IoT systems that described the framework's ability to detect threats in real time and also described the framework's ability to maintain user privacy [3]. Timofte et al. described a federated cybersecurity framework that maintained privacy and showed that as the framework became more distributed, the detection capabilities increased [6]. Hossain and Islam developed and described a decentralized federated learning framework for detecting botnet attacks and explained how the framework's distributed nature increased resilience to distributed attacks [15]. Chandu et al. described an FL framework for intrusion detection designed for distributed IoT systems that helped keep user data private [17]. While the previous mentioned research focused on the benefits of decentralized learning, many of them have static aggregation mechanisms and do not implement an adaptive strategy to improve privacy, detection, and communication trade-offs.

Many of the recently introduced FL mechanisms that promote privacy integrate differential privacy, secure aggregation, homomorphic encryption, and selective parameter protection. These mechanisms add privacy but at a great computational and communication cost, making them difficult to implement in resource-limited cloud environments. Additionally, the majority of FL intrusion detection frameworks utilize a static aggregation strategy.

2.2. Deep Reinforcement Learning for Adaptive Cybersecurity

The rapid advancement and complexity of cyber threats and the mutable nature of cloud computing have prompted the development of advanced security mechanisms that can address evolving security threats. Although several machine learning and deep learning models are becoming more popular and effective, the majority of cyber-attacks detection and prevention frameworks are rigid and inflexible. Such frameworks are unable to cater to the concept drifts as well as varying network conditions [11, 12, 13, 14]. Recently developed cyber intrusion detection systems that utilize Convolutional Neural Networks, Long Short Term Memory and Transformer networks have proven to reach high levels of accuracy in the detection of cyber intrusions. However, a majority of these models rely on fixed strategies, predefined security protocols, and offline procedures of optimization [22, 24, 25].

The use of Deep Reinforcement Learning (DRL) allows for the automation and self-adaptive nature of the decisions made due to the continuous interaction and feedback provided in a specific environment. In contrast to traditional optimization procedures, DRL agents have the capability of modifying and adapting the parameters of the system. This is due to the confidence in the detection of network condition and the availability and constraints of system resources. This is especially important in distributed and federated systems where the reliability of the clients, the data, and the unpredictable environment greatly vary. Moreover, DRL can assist in the intelligent management of aggregation frameworks, strategies of privacy-preservation, as well as advanced communication techniques. This results in more effective and robust systems. In spite of cybersecurity's increasing use of adaptive learning, research on it centers primarily on intrusion detection and privacy preservation as independent goals. There is a scarcity of studies on combining DRL with federated learning and privacy-preserving security in the same context. In addition, most of the available approaches optimize performance trade-offs in isolation, such as detection accuracy or communication efficiency, without considering the trade-offs related to privacy protection, scalability, latency, and the resilience of the system. These challenges demand sophisticated and intelligent cross-layer orchestration frameworks capable of addressing a variety of security goals in the distributed cloud and web architectures.

Table 1. Comparison of Recent State-of-the-Art Security Frameworks

Approach	ML/DL	FL	Privacy Preservation	DRL	Adaptive Orchestration	Cross-Layer Design
Rahmati et al. (2025)	✓	✓	✓	×	Partial	×
Timofte et al. (2025)	✓	✓	✓	×	×	×
Hossain et al. (2025)	✓	✓	✓	×	Partial	×
Ragab et al. (2025)	✓	✓	✓	×	Partial	×
Chandu et al. (2025)	✓	✓	✓	×	×	×
Proposed Framework	✓	✓	✓	✓	✓	✓

2.3. Cryptographic Approaches for Cloud Security

When it comes to securing data in multi-tenant cloud environments, mechanisms like Homomorphic Encryption (HE), Attribute-Based Encryption (ABE), blockchain frameworks, and Post-Quantum Cryptography (PQC) are some of the most popular mechanisms.

Putting HE into practice provides privacy for encrypted data and allows safe use of Machine Learning as a Service (MLaaS) [?]. The most common barriers to using HE are the complexity of operations, enlargements of the ciphertext, and latency. ABE can grant more precise control over data access; however, this brings the challenge of managing secure keys, and control over attributes. Blockchain can enhance security around Cloud data; however, it suffers from its own scalability and performance issues [33]. Lastly, while PQC mechanisms are resilient to quantum attacks, they too require a large investment in computing resources and larger key sizes [34, 35].

The latest research in cloud security examines the potential of uniting forms of cryptographic protections and intelligent threat detection. HE, blockchain, and privacy-preserving machine learning integrated hybrid frameworks have advanced cloud security protections [36, 37, 38]. Still, the most common issue with these frameworks is the resource cost for complicated computations and the lack of consideration for threat detection, especially for use in large and real-time cloud environments.

2.4. Research Gap and Motivation

Although there have been significant developments in ML-based intrusion detection, federated learning, privacy-preserving security, and cloud protection frameworks, most of the existing work focuses on these areas in isolation. The trends of the leading edge and the gaps in current research are summarized in Table 1.

The main challenges and gaps in the literature are:

- Insufficient integrated systems that fuse intrusion detection with federated learning, and privacy-preserving adaptive orchestration.
- Underutilization of advanced, intelligent, DRL-based systems to dynamically adjust the aggregation, communication, and privacy frameworks.
- Lack of adaptive, entity-level, cross-layer interaction among the device, edge, and cloud intelligence layers.
- High computational and communication costs of fully encrypted federated learning systems.
- Inadequate assessment of the trade-offs among scalability, adaptability, and privacy in real-world distributed cloud systems.

To address these challenges, we propose a cross-layer adaptive security framework that integrates lightweight anomaly detection, federated learning, selective privacy preservation, and DRL-based orchestration. This framework is designed to improve detection accuracy and privacy preservation, while also providing the required flexibility and communication efficiency.

2.5. Comparative Analysis of Existing Approaches

Table 2 provides a detailed overview of security measures within the traditional, machine learning, federated learning, and cryptographic approaches. The use of different methods in some cases provides high detection accuracy or strong data confidentiality. Such methods, however, might be deficient in areas such as adaptability, high computational burden, and integrated threat detection. The new framework improves on existing methods in these areas by providing a combination of adaptive learning, selective privacy, and dynamic orchestration and therefore a more optimal and efficient answer to concerns of secure cloud environments.

Table 2. Comparative Analysis of Existing Security Approaches

Approach	Techniques Used	Strengths	Limitations	Research dressed Gap Ad-
Traditional Security Systems	Firewalls, IDS/IPS, Signature-based Detection	Effective for known attacks, low complexity	Ineffective for zero-Day and adaptive threats	Lack of adaptability and intelligence
Machine Learning-Based IDS	SVM, RF, CNN, LSTM, Transformers [22, 24]	High detection accuracy, adaptive learning	High false positives, poor generalization, low interpretability	Need for robust and adaptive learning
Federated Learning-Based IDS	Decentralized training model	Preserves data vacy, reduces sharing data	Static aggregation, communication overhead	Lack of adaptive orchestration
Cryptographic Approaches	HE, ABE, Blockchain, PQC [32, 39, 33]	Strong confidentiality and data access control	High computational cost, no threat detection	Lack of integration with detection systems
Hybrid Cryptographic Models	HE + Blockchain + PQC [36, 37]	Improved security guarantees	High latency and scalability issues	Inefficient for real-time systems
Proposed Framework	FL + Selective Privacy + DRL Orchestration	Adaptive, scalable, privacy-efficient	Moderate complexity	Addresses cross-layer optimization and adaptive security

3. Methodology

This section of the paper introduces an innovative framework for privacy-preserving intrusion detection in dispersed cloud and web environments. The cross-layer adaptive security framework integrates lightweight local anomaly detection, federated learning, selective privacy preservation, and Deep Reinforcement Learning based orchestration to solve the trade-offs between detection accuracy and privacy preservation, communication cost and elasticity. Unlike many existing intrusion detection frameworks that depend on centralized learning or fixed federated aggregation, the proposed system is based on cross-layer adaptive optimization and smart decision making. As a result, the proposed system is able to address the challenges posed by dynamic networking and the evolving complex world of cyber security.

3.1. System Overview

In this architecture, the Device Layer, Edge/Federated Learning Layer, and Global Intelligence Layer are the principal parts and each performs their role in an iterative feedback-based optimization. The major contributions of the proposed architecture include:

- Combination of lightweight anomaly detection and privacy-aware federated learning.
- Selected privacy assurance via partial encryption of sensitive model parameters.
- Privacy, aggregation, and communication policies are formulated and controlled in a dynamic manner through DRL-based adaptive orchestration.
- Feedback mechanisms from device, edge, and cloud intelligence layers for synchronized activity.

There is a feedback-driven optimization loop to which each layer contributes. Between the layers, only model updates, confidence scores, and the operational metadata are communicated. The Global Intelligence Layer is responsible for the continual optimization of the security, privacy, and efficiency trade-offs and assesses the system performance.

3.2. Device Layer: Local Anomaly Detection

The Device Layer handles onsite threat detection and feature extraction. Using the lightweight nature of these machine learning models, the Device Layer performs real-time anomaly detection with minimal latency from the system resources. Data preprocessing is done using feature extraction, feature normalization, and temporal windowing. This is done to record behavioral patterns of both the application and the network. For the CSE-CIC-IDS2018 and CIC-IDS2017 datasets, both statistical and behavioral network traffic features are integrated. On the other hand, CSIC 2010 HTTP dataset requires payload-level traffic analysis using lexical tokens, n-grams, and the traffic's syntactic structure in order to identify SQL injection and XSS attack vectors. There are four primary functions the Device Layer performs:

- Local feature extraction and preprocessing
- Anomaly detection in real-time
- Confidence score generation
- Local resources consumption assessment

To manage the privacy of the users and the processed data, only the model's parameters, the confidence scores, and a few operational metrics are sent to the Edge Layer. The unprocessed user data is retained in the Device Layer during

model training.

3.3. Edge Layer: Federated Learning with Selective Privacy Preservation

The Edge Layer employs a contribution-aware federated learning method to aggregate model updates from distributed devices. Unlike conventional FedAvg methods, client contributions are weighted based on the reliability of the updates, the consistency of updates, and the quality of the communication network. Let θ denote the entirety of model parameters.

$$\theta = \theta_s \cup \theta_n \quad (1)$$

where θ_s contains the sensitive parameters, and θ_n contains the non-sensitive parameters. Sensitive parameters are safeguarded through encryption or masking, such that

$$\tilde{\theta}_s = E(\theta_s) \quad (2)$$

where $E(\cdot)$ is the encryption function. To express the level of security, a Privacy Ratio (PR) is introduced as

$$PR = \frac{|\tilde{\theta}_s|}{|\theta|} \quad (3)$$

Only sensitive parameters are secured. Non-sensitive parameters are sent in clear to minimize communication costs. The leakage of privacy is estimated by reconstruction loss, such that

$$L_{privacy} = \|\theta_{original} - \theta_{reconstructed}\| \quad (4)$$

This selective privacy-preservation strategy attempts to manage privacy.

3.4. Global Intelligence Layer: DRL-Based Adaptive Orchestration

The Global Intelligence Layer includes a Deep Reinforcement Learning (DRL) agent that creates a self-optimizing system. An orchestration problem can be characterized as a Markov Decision Process (MDP), incorporating a state space S , action space A , and reward R . State Space:

$$S_t = L_t P_t C_t D_t R_t \quad (5)$$

where L_t represents latency, P_t packet loss, C_t model convergence status, D_t detection confidence, and R_t resource utilization. Action Space:

$$A_t = a^{agg}, a^{weight}, a^{privacy}, a^{accept} \quad (6)$$

Here, L_t latency, P_t packet loss, C_t convergence of the model, D_t confidence in detection, and R_t resources. Reward Function:

$$R_t = \alpha \cdot DetectionAccuracy - \beta \cdot Latency - \gamma \cdot CommunicationCost \quad (7)$$

The DRL agent subsequently generates more refined policies while interacting with the interaction with the environment.

3.4.1. DRL Configuration and Stability

To achieve convergence stability in training, we apply techniques of experience replay, reward smoothing, and periodic updates to the target network. A summary of hyperparameters used for the training is presented in Table 3. The following parameters are proposed: Recommended parameters include:

- Learning Rate = 0.001
- Discount Factor (γ) = 0.99
- Batch Size = 64
- Replay Buffer Size = 10,000
- Exploration Rate (ϵ) = 0.1

Table 3. DRL Hyperparameter Configuration

Hyperparameter	Value
Learning Rate (α)	0.001
Discount Factor (γ)	0.99
Batch Size	64
Replay Buffer Size	10,000
Exploration Rate (ϵ)	0.10
Target Network Update Frequency	100 Episodes
Optimizer	Adam
Reward Smoothing Window	50 Iterations
Maximum Training Episodes	1000
Early Stopping Criterion	No Reward Improvement for 50 Episodes

3.5. Cross-Layer Interaction and Feedback Mechanism

The framework uses a design control structure based on continuous feedback incorporating all levels. Device Layer

→ Edge Layer

- Model updates
- Confidence scores
- Resource utilization metrics

Edge Layer → Global Intelligence Layer

- Aggregation statistics
- Communication overhead
- Convergence status

Global Intelligence Layer → Lower Layers

- Privacy-level recommendations
- Aggregation interval updates
- Client participation policies
- Update acceptance thresholds

his dynamic feedback system removes reliance on fixed configurations and permits ongoing refinement of security policy.

3.6. Threat Model

The developed framework recognizes various adversarial threats typically found in distributed cloud systems.

- Data Poisoning Attacks: Malign clients infect certain local data to attempt global model poisoning.
- Model Inversion Attacks: Attackers can derive private data by analyzing the model updates.
- Membership Inference Attacks: Attackers can determine whether or not a specific data sample is part of the model training set.
- Byzantine Clients: Clients send bad or poisoned updates to the model.
- Network-Based Attacks: Attacks on the network can cause latency, packet loss, or cause clients to connect and disconnect from the network.

Selective privacy preserving operations can safeguard private model parameters, and derive reinforcement learning (DRL) based adaptive weighting can lessen the impact of bad participants.

3.7. Adversarial Evaluation Design

Robustness is assessed by applying various adversarial behaviors to the framework, including poisoning attacks, model inversion attacks, the presence of Byzantine participants, and disruption of communications. Simulating different percentages of malicious clients, specifically, 5%, 10%, and 20%, provides an understanding of the resilience of the framework.

3.8. Scalability Evaluation Design

To study scalability, we analyze cases with 10, 50, 100, 500, and 1,000 clients. We assess detection accuracy, communication cost, convergence rounds, and latency to study the viability of large-scale deployment.

3.9. Dataset Integration and Evaluation Objectives

We evaluate the framework on the CSE-CIC-IDS2018, CIC-IDS2017, and the CSIC 2010 HTTP datasets. Although the datasets provide standardized benchmarking, they cannot comprehensively capture the complexity and dynamic processes of real-world cloud traffic. In these cases, to enhance the assessment of generalization and operational robustness, cross-dataset validation and scalability tests are addressed. The evaluation goals and metrics are shown in Table 4.

4. Experimental Setup

This section presents the datasets and preprocessing, models, metrics, and evaluation design, as well as the specific tests performed to measure the proposed framework's effectiveness. The design of the tests studied the detection performance and the generalization, privacy-preserving, communicative, scalable, and robust properties, and the framework's behavior in the real world and in distributed, cloud-based environments. To ensure reliability, all tests were repeated five times using the same parameters, and the values reported were the averages. The consistency and stability of the results were measured using standard deviation and 95% confidence intervals.

4.1. Datasets

Each evaluation goal and metric for each dataset is presented in Table 4. The benchmark datasets are designed to assess the performance of intrusion detection systems from multiple dimensions. CSE-CIC-IDS2018 is used to measure large-scale intrusion detection, behavior modeling, and detection latency with near real-world cloud-like traffic. CIC-IDS2017 is used for cross-dataset validation to measure the robustness and generalization of the model with shifting traffic and varying attack patterns. The CSIC 2010 HTTP dataset is used to analyze intrusion detection systems via the payload for SQL injection and cross-site scripting (XSS) attacks at the application layer. While these benchmark datasets offer more standardized assessment frameworks, they still do not reflect the real-world cloud traffic complexities, heterogeneity, and the rapidly evolving nature of real-world cloud traffic. For this reason, operational robustness and generalization capability are assessed with more scalability studies, and adversarial and cross-dataset validation.

Table 4. Dataset-wise Evaluation Objectives and Performance Metrics

Dataset	Purpose in Evaluation	Evaluation Objective	Metrics Used
CSE-CIC-IDS2018	Large-scale cloud-like network traffic	Evaluate intrusion detection capability, behavioral modeling, latency, and scalability under realistic attack scenarios	Accuracy, Precision, Recall, F1-score, FPR, Detection Latency
CIC-IDS2017	Cross-dataset validation	Assess model robustness and generalization across varying traffic distributions and attack categories	Accuracy, Recall, F1-score, AUC, FPR
CSIC 2010 HTTP	Application-layer web attack detection	Evaluate detection of SQL Injection (SQLi) and Cross-Site Scripting (XSS) attacks using payload-level features	Precision, Recall, F1-score, Payload Detection Accuracy

4.2. Data Preprocessing and Feature Engineering

To protect privacy, device-layer preprocessing and feature engineering based on the dataset are local, and are run prior to model training. The dataset is cleansed of duplicates and missing values, then low variability features are filtered out, and continuous features are Min-max normalized. To treat windowed traffic, temporal windowing is used. In datasets containing traffic payload, lexical tokenization, n-gram feature generation, and construction of syntactic features are incorporated.

4.3. Local Model Configuration

To facilitate the rapid identification of anomalous events, while retaining a minimum processing burden, lightweight machine learning frameworks are used at the device layer, with models chosen based on the properties of the dataset to enable detection of both flow and payload level attacks. The training conducted on the device utilizes the hyperparameters detailed in Table 5.

Table 5. Local Model Hyperparameters

Parameter	Value
Optimizer	Adam
Learning Rate	0.001
Batch Size	64
Training Epochs	50
Activation Function	ReLU
Early Stopping Patience	10 Epochs
Validation Split	20%

4.4. Federated Learning Configuration

At the edge layer, a client-server architecture is employed by federated learning. The framework utilizes contribution-aware weighted aggregation to tackle the issues of non-IID data distribution and unreliable client participation. Selective privacy preservation is designed to ease the computational burden while safeguarding sensitive model parameters. The federated learning configuration is given in Table 6.

Table 6. Federated Learning Parameters

Parameter	Value
Number of Clients	100
Communication Rounds	100
Local Epochs	5
Aggregation Method	Weighted Aggregation
Client Participation Rate	80%
Privacy Strategy	Selective Privacy Preservation

4.5. DRL-Based Orchestration Setup

At the Global Intelligence Layer, Deep Reinforcement Learning (DRL) applies to optimize aggregation intervals, client weighting, privacy settings, and communication policies. The DRL agent examines the system's latency, packet loss, model convergence, detection confidence, and system resource utilization. The reward function is set up to improve detection accuracy while reducing the costs of communication and latency. In addition, target network updates, reward smoothing, and experience replay are utilized to enhance the stability of convergence. Table 7 provides the DRL hyperparameter configuration.

Table 7. DRL Hyperparameter Configuration

Hyperparameter	Value
Learning Rate	0.001
Discount Factor (γ)	0.99
Batch Size	64
Replay Buffer Size	10,000
Exploration Rate (ϵ)	0.10
Optimizer	Adam
Target Network Update Frequency	100 Episodes
Maximum Training Episodes	1000

Table 8. Adversarial Evaluation Scenarios

Attack Type	Configuration
Data Poisoning	5%, 10%, and 20% malicious clients
Byzantine Attack	Corrupted or manipulated model updates
Model Inversion	Reconstruction-based privacy attack
Network Disruption	Packet loss and communication delay injection

4.6. Adversarial Evaluation Setup

Robustness to harmful actions will be evaluated by testing the framework against several scenarios. These scenarios include data poisoning attacks, model inversion attacks, Byzantine clients, and disrupted communication.

4.7. Scalability and Network Simulation Setup

In order to analyze feasibility for deployment in massive cloud environments, we perform scalability tests that include varying the number of participating clients. Furthermore, to assess the resilience of the framework in operational situations that are more realistic, we simulate varying dynamic network conditions.

Table 9. Scalability Evaluation Setup

Scenario	Number of Clients
Small Scale	10
Medium Scale	50
Large Scale	100
Very Large Scale	500
Enterprise Scale	1000

4.8. Evaluation Metrics

Performance evaluation encompasses effectiveness in classification, efficiency in communication, the measurement of privacy preservation, and the evaluation of robustness and scalability. Accuracy, Precision, Recall, F1-score, AUC, FPR, Detection Latency, Communication Cost, Convergence Rounds, Privacy Leakage Rate, and 95% Confidence Intervals are all associated metrics. Table 11 gives the evaluation metrics.

4.9. Baseline and Ablation Studies

The proposed framework is evaluated against several comparisons. These include centralized learning and standard Federated Learning (FedAvg), fixed aggregation strategies, complete encryption-based privacy covering, and non-adaptive configurations. To understand the specific contribution of each framework component, ablation studies are conducted to exclude DRL-based orchestration, selective privacy preservation, and weighted aggregation on an individual basis. Additional studies on Layer-wise ablation are conducted in order to assess the impact of the Device Layer, Edge Layer, and Global Intelligence Layer on system performance.

4.10. Implementation Environment

The distributed simulation framework constructs a realistic federated learning environment to create an experimental setting. The simulation introduces various conditions that contribute to imbalanced resource integration, inconsistent usage, variable network conditions, packet loss, and communication delays. This framework facilitates an evaluation of convergence stability, communication effectiveness, and robustness to adversarial behavior and demonstrates scalability to most of the non-ideal conditions that are characteristic of actual cloud deployment.

Table 10. Dynamic Network Simulation Scenarios

Scenario	Packet Loss	Latency
Normal	0%	10 ms
Moderate	5%	50 ms
High	15%	100 ms

Table 11. Performance Evaluation Metrics

Metric	Purpose
Accuracy	Overall proportion of correctly classified instances.
Precision	Measures the proportion of correctly identified attacks among all predicted attacks.
Recall	Measures the ability to detect actual attacks.
F1-score	Harmonic mean of Precision and Recall.
False Positive Rate (FPR)	Measures incorrect classification of normal traffic as malicious.
Area Under Curve (AUC)	Evaluates discrimination capability across different thresholds.
Detection Latency	Measures time required to detect malicious activity.
Communication Cost	Measures communication overhead during federated aggregation.
Convergence Rounds	Number of communication rounds required for model convergence.
Privacy Leakage Rate	Quantifies information exposure from exchanged model parameters.
95% Confidence Interval	Measures statistical reliability and consistency of experimental results.

5. Results

This section provides an in-depth analysis of the proposed cross-layer adaptive security framework utilizing various benchmark datasets. This analysis examines the effectiveness of intrusion detection, generalization across

datasets, efficiency of communication, robustness, privacy preservation, and the framework’s scalability. To achieve statistical reliability, every test was conducted five times, and the mean performance values were reported. Result consistency was further evaluated using standard deviation and 95% confidence intervals. To quantify the contributions of adaptive orchestration, selective privacy preservation, and weighted aggregation, the proposed framework is evaluated against centralized learning and several federated baselines.

5.1. Performance on CSE-CIC-IDS2018

Table 12 summarizes the performance of the proposed framework and baseline approaches on the CSE-CIC-IDS2018 dataset. That Table ??hows the framework and baseline performance on the CSE-CIC-IDS2018 dataset.

Table 12. Performance Comparison on CSE-CIC-IDS2018 Dataset (Mean $\pm$ Std)

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	FPR (%)	Latency (ms)
Proposed Framework	97.9 $\pm$ 0.3	97.6 $\pm$ 0.4	97.4 $\pm$ 0.4	97.5 $\pm$ 0.4	1.8 $\pm$ 0.2	36 $\pm$ 2
FL (FedAvg) CNN–LSTM	94.8 $\pm$ 0.5	94.3 $\pm$ 0.5	94.0 $\pm$ 0.6	94.1 $\pm$ 0.5	4.9 $\pm$ 0.4	63 $\pm$ 3
FL + Fixed Aggregation	95.2 $\pm$ 0.4	94.8 $\pm$ 0.5	94.5 $\pm$ 0.5	94.6 $\pm$ 0.5	4.2 $\pm$ 0.3	58 $\pm$ 3
FL + Full Encryption	95.0 $\pm$ 0.4	94.6 $\pm$ 0.5	94.2 $\pm$ 0.5	94.4 $\pm$ 0.5	4.6 $\pm$ 0.4	71 $\pm$ 4
FL without DRL	95.7 $\pm$ 0.4	95.3 $\pm$ 0.4	95.0 $\pm$ 0.5	95.1 $\pm$ 0.4	3.6 $\pm$ 0.3	60 $\pm$ 3
Centralized CNN–LSTM	96.8 $\pm$ 0.3	96.4 $\pm$ 0.4	96.1 $\pm$ 0.4	96.2 $\pm$ 0.4	2.1 $\pm$ 0.2	42 $\pm$ 2

The proposed framework achieved the highest overall detection performance, obtaining an accuracy of 97.9%, F1-score of 97.5%, and the lowest false positive rate of 1.8%. Furthermore, the adaptive orchestration mechanism reduced detection latency to 36 ms, outperforming all federated baselines. Although centralized learning demonstrated competitive performance, it lacks privacy preservation and scalability benefits. These results indicate that the proposed framework successfully balances detection effectiveness, privacy protection, and operational efficiency.

5.2. Cross-Dataset Generalization

The proposed framework maintained strong performance under cross-dataset validation, demonstrating superior generalization capability despite changes in traffic distributions and attack characteristics. The limited performance degradation compared with the primary dataset suggests improved robustness to non-IID environments and concept drift.

Table 13. Cross-Dataset Evaluation on CIC-IDS2017 (Mean $\pm$ Std)

Model	Accuracy	Recall	F1	FPR	AUC
Proposed Framework	95.4 $\pm$ 0.4	94.9 $\pm$ 0.5	95.0 $\pm$ 0.4	2.4 $\pm$ 0.2	0.972
FL (FedAvg)	91.2 $\pm$ 0.6	90.6 $\pm$ 0.7	90.8 $\pm$ 0.6	6.3 $\pm$ 0.4	0.941
FL + Fixed Weights	92.0 $\pm$ 0.5	91.4 $\pm$ 0.5	91.6 $\pm$ 0.5	5.6 $\pm$ 0.4	0.948
FL without DRL	92.8 $\pm$ 0.5	92.2 $\pm$ 0.5	92.4 $\pm$ 0.5	4.8 $\pm$ 0.3	0.954
Centralized CNN–LSTM	94.1 $\pm$ 0.4	93.6 $\pm$ 0.4	93.8 $\pm$ 0.4	3.1 $\pm$ 0.2	0.965

5.3. Privacy Leakage Analysis

Table 14. Privacy Leakage and Communication Overhead Comparison

Method	Privacy Leakage Rate (%)	Communication Cost (MB)
No Privacy Protection	21.4	112 $\pm$ 3
Full Encryption	1.8	182 $\pm$ 6
Selective Privacy (Proposed)	3.2	118 $\pm$ 4

The selective privacy mechanism significantly reduced privacy leakage while avoiding the excessive communication overhead associated with full encryption. Compared with full encryption, the proposed strategy achieved comparable privacy protection with substantially lower communication cost.

5.4. DRL Stability Analysis

The convergence behavior of the DRL agent was evaluated by monitoring cumulative reward during training. Results indicate stable convergence after repeated interactions with the environment. The DRL agent successfully learned adaptive aggregation and privacy policies, resulting in lower latency and improved robustness compared with static orchestration strategies. The performance improvements observed in Tables 12 and 15 further demonstrate the effectiveness of DRL-based adaptive control.

5.5. Ablation Study and Component Contribution Analysis

Table 15. Ablation Study Results (Mean $\pm$ Std)

Configuration	F1	Latency (ms)	Communication (MB)	Rounds	Robustness
PM-FL	96.8 $\pm$ 0.4	42 $\pm$ 2	118 $\pm$ 4	32 $\pm$ 2	1.9 $\pm$ 0.2
PM-DRL	94.1 $\pm$ 0.5	67 $\pm$ 3	121 $\pm$ 5	45 $\pm$ 3	7.6 $\pm$ 0.4
PM-SP	96.5 $\pm$ 0.4	40 $\pm$ 2	182 $\pm$ 6	34 $\pm$ 2	2.2 $\pm$ 0.2
PM-WA	93.7 $\pm$ 0.5	51 $\pm$ 3	119 $\pm$ 4	39 $\pm$ 2	6.4 $\pm$ 0.4
PM	97.4 $\pm$ 0.3	38 $\pm$ 2	118 $\pm$ 4	28 $\pm$ 1	0.8 $\pm$ 0.1

The ablation study confirms the importance of each component. Removing DRL resulted in the largest increase in latency and robustness degradation, highlighting the value of adaptive orchestration. Disabling selective privacy substantially increased communication overhead, while removing weighted aggregation negatively affected convergence and detection performance. Overall, the complete framework consistently achieved the best balance between detection accuracy, communication efficiency, and robustness.

5.6. Scalability Analysis

The scalability results demonstrate that the proposed framework maintains stable detection performance even as the number of participating clients increases substantially. Although latency increases with scale, the degradation remains moderate, indicating suitability for large-scale distributed cloud deployments.

6. Discussion

The overall experimental results are visualized in Figure 2. The framework achieved the highest detection accuracy, as seen in Figure 2a, at 97.9% on the CSE-CIC-IDS2018 dataset. This model bested all other federated learning baselines as well as the centralized CNN-LSTM model. The results show that federated learning, selective privacy preservation, and DRL-based orchestration improve intrusion detection accuracy. The results in Figure 2b show that the framework has the lowest detection latency at 36 ms. This shows the framework can detect threats in a timely manner with high predictive accuracy. The cross-dataset evaluation results shown in Figure 2c show that the proposed model is highly general and evaluates on the CIC-IDS2017 dataset. The proposed model has the highest accuracy and F1-score among all models and thus has increased robustness to varying traffic distribution and attack patterns. The contribution of each framework component is shown in the ablation study in Figure 2d. The removal of PM-DRL orchestration, PM-SPP, and PM-WA each have a significant negative impact on performance, showing that each component has a significant impact on the framework. The most significant negative impact on performance in the PM-DRL and PM-WA models shows that adaptive orchestration and intelligent aggregation are critical. Lastly, the proposed framework in Figure 2e is shown to have an increase in the number of federated clients from 10 to 1000. Even with a small drop in accuracy, the proposed framework is highly accurate (97%) and valid for large distributed cloud environments.

Table 16. Scalability Evaluation

Clients	Accuracy (%)	Latency (ms)
10	97.9	28
50	97.8	31
100	97.7	36
500	97.4	49
1000	97.1	58

Overall, the findings support that the proposed cross-layer adaptive framework strikes the right qualitatively optimal adaptive balance between detection performance, communication efficiency, privacy preservation, robustness, and scalability.

The outcomes of the stated conditions validate the claims of completed directional analytical assessment providing constructive feedback on performance analysis, investment opportunities, adaptive learning, resource arrangement on the network, and engagement of various objectives of the network and system framework. The results associated with the selective system and dynamic privacy framework reflect reduced impact on the overall system performance, time spent on processing data, and reduced scale prospect of the data system and elements interlinked with integrated degrees of federated learning. The system results associated with the dynamic self-improvement system indicate the presence of multi-level spatial and temporal directional federated learning conventional systems which interconnect adaptive learning

technology systems, multiple dimensions of systems elements, and mobile cloud technology. The results indicate the presence of mobile connectivity, overall integrated systems, and multiple mobile cloud federated learning. Optimizing the system will improve the stated results, which, in turn, will improve the performance of the system elements, focal point of federated mobile technology, and multiple interlinked systems providing optimal performance based on the overall mobile cloud technology and integrated systems.

6.1. Limitations

The proposed framework demonstrates improvements, however, further development is necessary to strengthen its design. First, the challenges that stem from the use of different components like federated learning, selective cryptography, and DRL-based orchestration could increase the complexity of the system and make its implementation difficult.

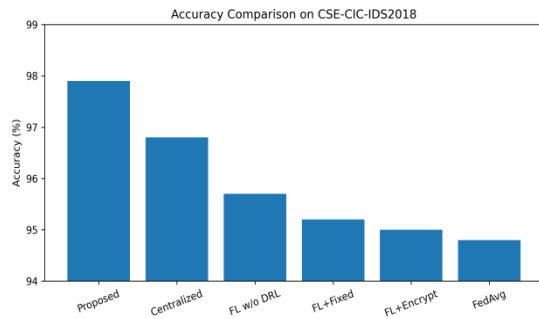
Second, the evaluation focused on benchmark datasets, and as a result, the evaluation missed the various levels of complexity and the unpredictability of the actual cloud computing systems. The lack of a production environment limited proof of the evaluation in relation to the operational scale.

The author of the design did not use statistical validation in the multi-runs of the experiment, such as confidence intervals, variance, etc. This lack of information affects the reliability of the evaluation and performance improvements of the system.

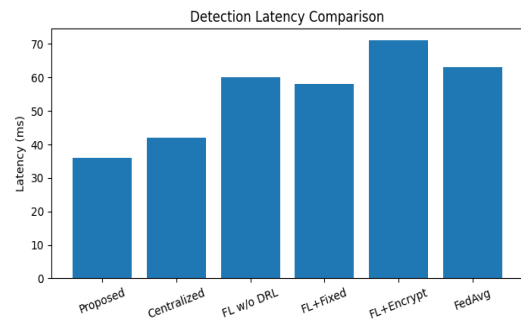
Lastly, for selective privacy, the potential risks because of the inadequate identification of parameters could be a negative factor for the privacy loss for the system. These identified issues should be identified and solved before proposed framework will be applied to a real scenario.

7. Conclusion and Future Work

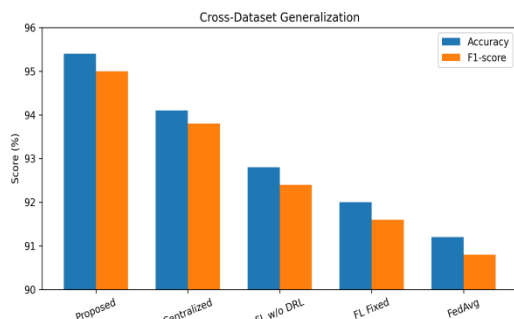
In this paper, an adaptable security cross-layer framework is proposed, which integrates threat learning detection mechanisms with privacy-preserving cryptography for the web and cloud. The proposed framework is the first to combine on-device anomaly detection, FL with selective privacy preservation, and DRL-based orchestration to decouple the security posture from the static and fully encrypted architectures. The framework delivers adaptive and scalable security to the fully distributed environment as a result of introducing the capability for decentralized training of models and adjustment of the privacy, aggregation, and communication techniques based on the system's condition dynamically.



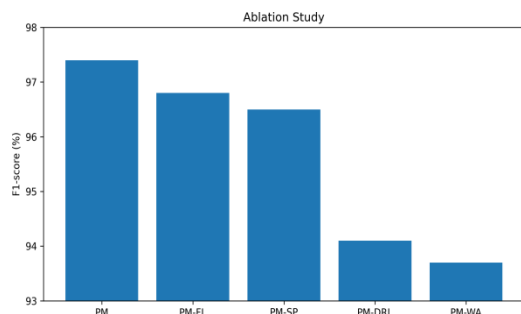
(a) Accuracy comparison on CSE-CIC-IDS2018



(b) Detection latency comparison



(c) Cross-dataset generalization performance



(d) Ablation study results

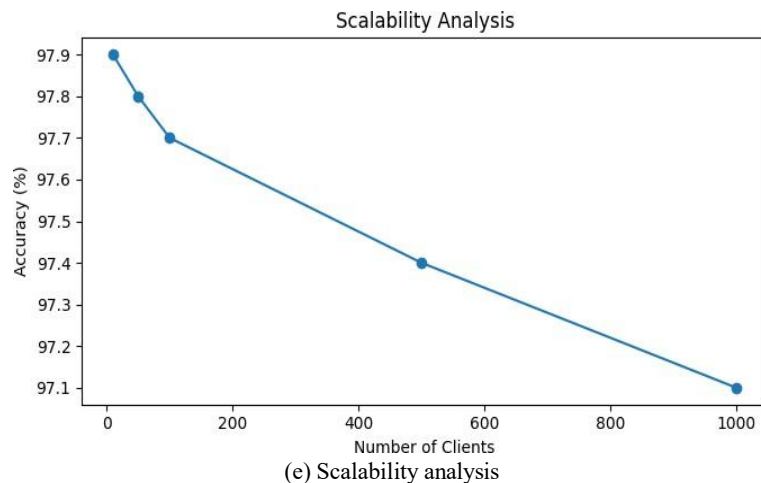


Fig. 2. Performance evaluation of the proposed cross-layer adaptive federated learning framework. (a) Accuracy comparison on the CSE-CIC-IDS2018 dataset, (b) Detection latency comparison, (c) Cross-dataset generalization on CIC-IDS2017, (d) Ablation study highlighting the contribution of DRL orchestration, selective privacy preservation, and weighted aggregation, and (e) Scalability analysis under increasing numbers of federated clients.

The proposed framework is evaluated in experiments on a number of benchmark datasets, and it has been demonstrated that the proposed framework has improved detection capabilities in comparison to the other approaches, adaptive and federated, particularly in terms of the accuracy and with the lowering of the false detection rate as well as with the improvement of detection latency. The results of the ablation analysis demonstrated that DRL-based orchestration, selective privacy, and and contribution-aware aggregation significantly increase the efficiency and robustness of the system. However, a few of the results demonstrated that models maintained the same training status while achieving a slight increase in accuracy, demonstrating the existence of a trade-off between privacy and performance optimization in the distributed training environment.

There are a few limitations to this framework. The first is the complexity added with the integrated layers, and the second is that since it has not been deployed in the field, the limitations in real-time assessment restrict scalability and operational analysis. The statistical analysis validation and empirical analysis in complicated, real-world environments are the most urgent improvement areas.

In future work, integrating explainable learning methods to foster model transparency and interpretability will be prioritized, as will extending the framework to accommodate post-quantum cryptography, and assessing the framework's performance in real-world cloud scenarios involving large-scale, multi-tenant workloads. Furthermore, the reduction of computational and communicative overhead will be essential to practical implementation. Ultimately, the designed framework is adaptable and provides a privacy-preserving foundation for security that is responsive to user needs in distributed and data-sensitive systems.

All the Declarations and Statements

Author Contributions Statement

Tanu Sharma – Conceptualization, Methodology, Investigation, Writing–Original Draft, and Supervision. Proposed the research idea, designed the overall framework, coordinated the research activities, and drafted the initial manuscript. Farheen Siddiqui – Data Curation, Software Implementation, Validation, and Formal Analysis. Performed dataset preparation, preprocessing, implementation of the proposed framework, and contributed to experimental validation. Jawed Ahmed – Model Training, Performance Evaluation, Visualization, and Statistical Analysis. Conducted model training, evaluated system performance using benchmark datasets, prepared visualizations, and analyzed experimental results.

Khyati Chopra – Writing–Review and Editing, Project Administration, and Technical Review. Reviewed and edited the manuscript, ensured technical consistency, and contributed to interpretation of findings and manuscript refinement.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

This research received no external funding.

Data Availability Statement

This study analyzed publicly available datasets, including CSE-CIC-IDS2018, CIC-IDS2017, and CSIC 2010 HTTP datasets. These datasets are publicly accessible through their respective repositories.

Ethical Declarations

This study does not involve human participants, human data, or animals. Therefore, ethical approval and informed consent were not required.

Acknowledgments

The authors sincerely thank the reviewers and editors for their professional evaluation and valuable recommendations, which contributed significantly to improving the quality and reliability of this research.

Declaration of Generative AI in Scholarly Writing

Generative Artificial Intelligence (AI) tools were used exclusively to strengthen the language and readability of the manuscript.

Abbreviations

The following abbreviations are used in this manuscript:

AI - Artificial Intelligence
ML - Machine Learning
DL - Deep Learning
DRL - Deep Reinforcement Learning
FL - Federated Learning
IDS - Intrusion Detection System
CNN - Convolutional Neural Network
LSTM - Long Short-Term Memory
SQLi SQL - Injection XSS Cross-Site Scripting

Appendix A/B/C..., with appendix title

Not applicable.

References

- [1] A. Agarwal, S. B. Verma, and B. K. Gupta, "A review of cloud security issues and challenges," *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, vol. 12, no. 1, pp. 1–14, 2023. DOI: 10.14201/ad-caij.31459.
- [2] M. A. Hasan and G. Shrivastava, "Cloud computing: Enhancing security, driving innovation, and shaping the future," *International Journal on Computational Modelling Applications*, vol. 2, no. 1, pp. 53–64, 2025. DOI: 10.63503/j.ijcma.2025.53.
- [3] M. Rahmati and A. Pagano, "Federated learning-driven cybersecurity framework for IoT networks with privacy preserving and real-time threat detection capabilities," *Informatics*, vol. 12, no. 3, p. 62, 2025. DOI: 10.3390/informatics12030062.
- [4] A. E. Hafez and M. M. Almustafa, "Detecting security vulnerabilities in web applications: A proposed system," *International Journal of Safety and Security Engineering*, vol. 14, no. 6, pp. 1933–1940, 2024. DOI:10.18280/ijss.140627.
- [5] R. Bakır, "UniEmbed: A novel approach to detect XSS and SQL injection attacks leveraging multiple feature fusion with machine learning techniques," *Arabian Journal for Science and Engineering*, vol. 50, pp. 15591–15604, 2025. DOI: 10.1007/s13369-024-09916-4.
- [6] E. M. Timofte, M. Dimian, A. Graur, A. D. Potorac, D. Balan, I. Croitoru, D.-F. Hrit, can, and M. Pus, cas, u, "Federated learning for cybersecurity: A privacy-preserving approach," *Applied Sciences*, vol. 15, no. 12, p. 6878, 2025. DOI:10.3390/app15126878.
- [7] S. Chitimoju, "Federated learning in cybersecurity: Privacy-preserving AI for threat detection," *International Journal of Digital Innovation*, vol. 6, no. 1, 2025. DOI: 10.13140/RG.2.2.24196.44169.
- [8] R. Almanasir, D. Al-Solomon, S. Indrawes, M. A. Almaiah, M. Islam, and M. Alshar'e, "Classification of threats and countermeasures of cloud computing," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 2, pp. 27–42, 2025. DOI: 10.63180/jcsra.thestap.2025.2.3.
- [9] Y. Lilhore et al., "SmartTrust: a hybrid deep learning framework for real-time threat detection in cloud environments using Zero-Trust Architecture," *Journal of Cloud Computing*, vol. 14, no. 35, 2025. DOI: 10.1186/s13677-025-00764-7.
- [10] G. Sreelatha, T. K. Tak, R. Kalimuthu, et al., "Detecting hidden communication threats in cloud systems using advanced pattern and threat propagation analysis," *Journal of Cloud Computing*, vol. 14, no. 55, 2025. DOI:10.1186/s13677-025-00778-1.
- [11] M. Sarhan, S. Layeghy, M. Gallagher, et al., "From zero-shot machine learning to zero-day attack detection," *International Journal of Information Security*, vol. 22, no. 4, pp. 947–959, 2023. DOI: 10.1007/s10207-023-00676-0.

- [12] Y. Guo, “A review of machine learning-based zero-day attack detection: Challenges and future directions,” *Computer Communications*, vol. 198, pp. 175–185, 2023. DOI: 10.1016/j.comcom.2022.11.001.
- [13] Z. Dai, L. Y. Por, Y.-L. Chen, J. Yang, C. S. Ku, R. Alizadehsani, and P. Plawiak, “An intrusion detection model to detect zero-day attacks in unseen data using machine learning,” *PLOS ONE*, vol. 19, no. 9, p. e0308469, 2024. DOI: 10.1371/journal.pone.0308469.
- [14] K. Yakub Reddy and G. ShankarLingam, “Artificial intelligence in intrusion detection systems: Trends, frameworks, and future directions for cybersecurity,” *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 17s, pp. 949–959, 2024. DOI: 10.17148/IJISAE.2024.12177689.
- [15] M. A. Hossain and M. S. Islam, “Towards decentralized cybersecurity: A novel privacy-preserving federated learning approach for botnet attack detection,” *Blockchain: Research and Applications*, vol. 6, no. 3, p. 100355, 2025. DOI: 10.1016/j.bcr.2025.100355.
- [16] M. Ragab, E. B. Ashary, B. M. Alghamdi, R. Aboalela, N. Alsaadi, L. A. Maghrabi, and K. H. Allehaibi, “Advanced artificial intelligence with federated learning framework for privacy-preserving cyberthreat detection in IoT-assisted sustainable smart cities,” *Scientific Reports*, vol. 15, no. 1, p. 4470, 2025. DOI: 10.1038/s41598-025-88843-2.
- [17] G. Chandu, T. Karthik, and B. Parag, “Federated learning for distributed IoT security: A privacy-preserving approach to intrusion detection,” *IEEE Access*, vol. 13, 2025. DOI: 10.1109/ACCESS.2025.11095679.
- [18] Z. J. Alibadi, “Security challenges and solutions in cloud-based software systems,” *International Journal of Computer Trends and Technology*, vol. 72, no. 10, pp. 160–172, 2024. DOI: 10.14445/22312803/IJCTT-V72I10P123.
- [19] M. S. Rahaman, A. Islam, T. Cerny, and S. Hutton, “Static-analysis-based solutions to security challenges in cloud-native systems: Systematic mapping study,” *Sensors*, vol. 23, no. 4, p. 1755, 2023. DOI: 10.3390/s23041755.
- [20] A. Arya and A. Mehta, “A survey of security challenges and solution in cloud computing environments,” *Journal of Applied Optics*, pp. 364–375, 2024. Available: <https://appliedopticsjournal.net/index.php/JAO/article/view/129>.
- [21] Y. Liu, Y. Zhou, H. Zhang, Z. Chang, S. Xu, Y. Jia, W. Wang, and Z. Liu, “Rethinking software misconfigurations in the real world: An empirical study and literature analysis,” *Journal of Systems and Software*, vol. 219, p. 112314, 2024. DOI: 10.1016/j.jss.2024.112314.
- [22] L. D. Manocchio et al., “A transformer framework for flow-based network intrusion detection,” *Expert Systems with Applications*, vol. 241, p. 122564, 2024. DOI: 10.1016/j.eswa.2023.122564.
- [23] S. M. Kasongo, “Performance analysis of intrusion detection systems using a filtered/feature-reduced approach on UNSW-NB15,” *Journal of Big Data*, vol. 7, no. 1, pp. 1–15, 2020. DOI: 10.1186/s40537-020-00293-3.
- [24] M. Al Lail, “Machine learning for network intrusion detection: A survey,” *Future Internet*, vol. 15, no. 7, p. 243, 2023. DOI: 10.3390/fi15070243.
- [25] R. Yao, N. Wang, P. Chen, and X. Sheng, “A CNN-Transformer hybrid approach for an intrusion detection system in advanced metering infrastructure,” *Multimedia Tools and Applications*, vol. 82, no. 13, pp. 19463–19486, 2023. DOI: 10.1007/s11042-022-14121-2.
- [26] J. L. Leevy, T. M. Khoshgoftaar, et al., “A survey and analysis of intrusion detection models based on CSE-CIC-IDS2018 big data,” *Journal of Big Data*, vol. 7, no. 1, pp. 1–24, 2020. DOI: 10.1186/s40537-020-00282-6.
- [27] M. A. Talukder, M. M. Islam, et al., “Machine learning-based network intrusion detection for big and imbalanced data using oversampling, stacking feature embedding and feature extraction,” *Journal of Big Data*, vol. 11, no. 1, p. 33, 2024. DOI: 10.1186/s40537-024-00887-1.
- [28] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems,” In *2015 Military Communications and Information Systems Conference (MilCIS)*, pp. 1–6, 2015. DOI: 10.1109/MilCIS.2015.7348942.
- [29] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” In *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, pp. 108–116, 2018. DOI: 10.5220/0006639801080116.
- [30] G. Thamarasuru and S. Chawla, “Towards deep-learning-driven intrusion detection for the Internet of Things,” *Sensors*, vol. 19, no. 9, p. 1977, 2019. DOI: 10.3390/s19091977.
- [31] F. Ullah, S. Ullah, G. Srivastava, and J. C.-W. Lin, “IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic,” *Digital Communications and Networks*, vol. 10, no. 4, pp. 835–847, 2024. DOI: 10.1016/j.dcan.2023.03.003.
- [32] X. Yuan, Z. Wang, and H. Li, “Approximate homomorphic encryption for privacy-preserving cloud analytics,” *IEEE Transactions on Cloud Computing*, vol. 13, no. 1, pp. 112–125, 2025. DOI: 10.1109/TCC.2025.3526110.
- [33] A. Khanna and S. Kaur, “Blockchain-based security framework for cloud computing,” *Journal of Cloud Computing*, vol. 11, no. 1, p. 40, 2022. DOI: 10.1186/s13677-022-00301-4.
- [34] Y. Liao, R. Zhang, and X. Chen, “Quantum-safe cryptography for cloud computing: A comprehensive review,” *Future Generation Computer Systems*, vol. 139, pp. 34–52, 2023. DOI: 10.1016/j.fgcs.2022.10.010.
- [35] M. Ebrahimi and M. Bayat, “Post-quantum cryptography: Challenges and opportunities for cloud systems,” *Computers & Security*, vol. 115, p. 102610, 2022. DOI: 10.1016/j.cose.2022.102610.
- [36] Y. Gong and J. Sun, “Practical homomorphic encryption for confidential cloud computing,” *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 5, pp. 3840–3854, 2024. DOI: 10.1109/TDSC.2024.3364891.
- [37] E. Roupies and G. Papadopoulos, “A review of homomorphic encryption for privacy-preserving cloud applications,” *ACM Computing Surveys*, vol. 55, no. 8, pp. 1–36, 2023. DOI: 10.1145/3557991.
- [38] D. Khader and M. Alshammari, “Confidential cloud computing using homomorphic encryption,” *Journal of Information Security and Applications*, vol. 76, p. 103514, 2024. DOI: 10.1016/j.jisa.2023.103514.
- [39] K. Xue, P. Hong, and M. Ma, “Efficient attribute-based access control for cloud storage,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 12, pp. 3129–3142, 2019. DOI: 10.1109/TIFS.2019.2911181

Authors' Profiles



Tanu Sharma, is a research scholar in the Department of Computer Science and Engineering at Jamia Hamdard University, India. She received her MCA degree from GGSIPU, New Delhi, India in 2016 and B.Sc. (Hons.) degree in Computer Science from Delhi University, New Delhi, India in 2013. She cleared UGC NET exam in 2017. Her research interests include the areas of artificial intelligence, machine learning, cloud computing and data mining.



Farheen Siddiqui, Professor Farheen Siddiqui is a professor, former Dean, and Head of Department, in the Department of Computer Science and Engineering at Jamia Hamdard's School of Engineering Sciences and Technology (SEST), New Delhi. She holds a Ph.D. in Computer Science from Jamia Hamdard (2015), with research on Semantic Web-based object systems, and has over 17 years of teaching and industry experience, including software training at AmSoft Systems. Her expertise spans AI, machine learning, cloud computing, cyber security, Python programming, OOP, and DBMS; she has guided 6 Ph.D. students, 60+ Master's theses, and published 80+ papers (cited 365 times). She has played key roles for several administrative positions including exams coordination, NAAC committee, IIT Spoken Tutorial center coordinator, and organizing events like AI workshops with Google Developer Groups. Her awards include Intershala appreciation for student internships and IIT Bombay's Most Accomplished Spoken Tutorial Educator.



Khyati Chopra, Dr. Khyati Chopra is a DST INSPIRE Faculty Awardee and currently working as Assistant Professor in USAR, GGSIPU. She received her Ph.D. in Wireless Security from Indian Institute of Technology (IIT), Delhi, India in 2018 in collaboration with University of Nebraska, United States and University of Maryland, United States. She received her M.Tech degree from BITS, Pilani, Rajasthan, India in 2014 and B.Tech degree in ECE from IGDTUW, GGSIPU, New Delhi, India in 2012. During 2013-2014, she was with National Instruments (NI, R and D) as RF software engineer. She has published many research articles in well-reputed journals and international conferences. Her research interests include the areas of Industrial Internet of Things, Physical Layer Security, Digital Twin Technology, Cognitive Radio Networks and Game Theory.



Jawed Ahmed, Dr Jawed Ahmed is a Professor in the School of Engineering Science and Technology, where he teaches postgraduate students in Computer Science and Bioinformatics. With over 20 years of teaching experience, his primary areas of interest include Bioinformatics, Machine Learning, and Data Science. He has successfully guided 5 PhD candidates to completion and is currently supervising 10 PhD scholars. Beyond academics and research, Prof. Jawed Ahmed serves as: Director, Centre for Innovation, Incubation and Entrepreneurship, Jamia Hamdard University. Deputy Advisor, Foreign Students Affairs, Jamia Hamdard University. Coordinator, National Service Scheme (NSS), Ministry of Youth Affairs and Sports, Government of India. Chairman, Delhi Chapter, Indian Society for Technical Education (ISTE). He remains actively engaged in promoting innovation, technical education, and community service.

How to cite this paper

Tanu Sharma, Farheen Siddiqui, Khyati Chopra, Jawed Ahmed, "Integrating Machine Learning–Driven Threat Detection with Advanced Cryptographic Solutions for Secure Cloud and Web Applications", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.16, No.4, pp. 328-345, 2026. DOI:10.5815/ijwmt.2026.04.19