Journal of Engineering and Technology for Industrial Applications

ITEGAM-JETIA

Manaus, v.12 n.57, p. 1016-1029. January/February, 2026.

DOI: https://doi.org/10.5935/jetia. v12i57.3180

ISSN ONLINE: 2447-0228

RESEARCH ARTICLE OPEN ACCESS

ADAPTIVE MULTI-STAGE CLOUD INTRUSION DEFENCE AND RECOVERY VIA HIERARCHICAL FEATURE OPTIMIZATION AND FEDERATED INTELLIGENCE SETS

Shubhangi S. Shambharkar*[1], Latesh G. Malik[2]

[1]Research Scholar, Dept. of Electronics and Computer Science, Rashtrasant Tukadoji Maharaj Nagpur University (RTMNU), Nagpur, Maharashtra, India.

[2]Associate Professor, Government College of Engineering, Nagpur, Maharashtra, India

[1]http://orcid.org/0009-0001-2136-6381, [2]http://orcid.org/0000-0001-5660-9438

Email: *shubhangisshambharkar@gmail.com, latesh.gagan@gmail.com

ARTICLE INFO

Article History

Received: December 22, 2025

Revised: January 10, 2026

Accepted: January 15, 2026

Published: February 28, 2026

Keywords:

Cloud Security,
Intrusion Detection,
Deep Reinforcement Learning,
Federated Learning,
Feature Optimization,
Process.

ABSTRACT

Cloud computing underpins critical digital infrastructure, yet massive high-dimensional traffic and rapidly evolving threats make intrusion detection and recovery highly challenging. Conventional systems relying on static thresholds or single-stage feature selection often leave redundant attributes, blur attack signatures, and struggle with non-stationary cloud workloads. To overcome these limitations, an integrated adaptive defense and recovery pipeline is introduced with five tightly coupled components. The Hierarchical Self-Adaptive Dimensionality Optimizer (HSADO) builds a mutual Information and Pearson-correlation hierarchy, then applies recursive aggregation with dynamic signal-to-noise–driven entropy thresholds to prune irrelevant features, yielding a compact but information-rich representations. The Dual-Stream Contrastive Deep Anomaly Detector (DSCDAD) exploits supervised classification alongside contrastive embedding learning to sharpen class boundaries, achieving area-under-curve values exceeding 0.99 and significantly improving recall in the process. Its latent embeddings feed the Reinforcement Informed Risk Adaptation Engine (RIRAE), a deep Q-learning agent that converts detection confidence into rapid mitigation actions such as IP blocking and container isolation, cutting mean reaction time by roughly one-third. Building on these actions, the Federated Knowledge Graph Constructor for Threat Correlation (FKGC-TC) assembles privacy-preserving, transformer-based threat graphs to share attack patterns across cloud regions, accelerating collaborative detection sets. Finally, the Predictive Service Quality Stabilizer (PSQS) employs meta-learned regression with Bayesian optimization to forecast service degradation and dynamically reallocate resources, reducing recovery time by about 41 % and sustaining SLA compliance near 99 %. Spanning data reduction through predictive healing, this self-reinforcing architecture delivers durable, scalable, and autonomous cloud intrusion defense with superior accuracy, lower false-positive rates, and robust post-attack stabilizations.

Copyright ©2025 by authors and Galileo Institute of Technology and Education of the Amazon (ITEGAM). This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

I. INTRODUCTION

Modern digital infrastructure uses cloud computing to give businesses and governments elastic processing capacity and pervasive network access. Cloud cyberattacks are possible due to multi-tenancy, on-demand resource allocation, and geographically dispersed services. Large, fast traffic streams make intrusion detection tougher in process. To escape detection, DDoS, advanced persistent threats, and covert lateral movement operations may use redundant or irrelevant data samples.

Data drift and concept change affect intrusion detection systems (IDS) with static feature sets and thresholds. Siloed approaches inhibit cross-domain knowledge transmission [1], [2], [3] and dynamic adaptation during intrusions. The curse of

dimensionality in process network telemetry worsens the issue. Fixed feature selection techniques may miss subtleties needed to differentiate overlapping attack classes, while high-dimensional feature spaces obfuscate discriminative patterns and raise computing costs. Traditional rule-based mitigation cannot manage attackers' changing methods. Post-attack resource recovery is heuristic and imprecise [4], [5], [6], risking SLAs even with mitigation. Cloud environments require an integrated security architecture that identifies and mitigates threats in real time and stabilizes service performance during and after threats. The self-adaptive, full-stack pipeline proposed in this research meets these needs. Mutual information, Pearson-correlation clustering, and dynamic entropy-based thresholds reduce duplicate features with the Hierarchical Self-Adaptive Dimensionality Optimizer (HSADO), preserving key signals for downstream identification.

Supervised classification and unsupervised contrastive embedding help the Dual-Stream Contrastive Deep Anomaly Detector (DSCDAD) distinguish complex attack classes. Based on real-time situation feedback, the Reinforcement Informed Risk Adaptation Engine (RIRAE) uses deep Q-learning to determine the best mitigation procedures like rate limiting or container isolation after detection. Privacy-preserving federated learning and transformer-based entity extraction enable cloud zone intelligence exchange in the Federated Knowledge Graph Constructor for Threat Correlation (FKGC-TC). Finally, meta-learned regression and Bayesian optimization predict service deterioration risk and automate resource reallocation for rapid recovery sets in the PSQS. The proposed design closes the feedback loop for all five methods to enhance detection accuracy, reduce false positives, and stabilize services. Hierarchical feature trimming, dual-stream representation learning, reinforcement-based mitigation, federated threat correlation, and predictive recovery build a resilient cloud defense paradigm sets.

I.1 MOTIVATION & CONTRIBUTION

A gap between cloud-based cyber threats' sophistication and conventional prevention systems' stagnation prompted this approach sets. High-dimensional traffic statistics and continuously expanding attack surfaces can weaken current intrusion detection systems. Static feature selection and rule-based mitigation may miss unique or mixed attack patterns. A lack of coordinated knowledge exchange between cloud areas promotes duplication and slow adaptation to irregularities in the process. System administrators must allocate resources ad hoc due to the lack of scientific methods for predicting and managing post-attack service deteriorations. An autonomous, self-learning architecture that improves detection, mitigation, and recovery in a privacy-aware, computationally efficient manner is needed. It creates and empirically tests a multi-layered pipeline to handle these problems from scratch sets. The Hierarchical Self-Adaptive Dimensionality Optimizer (HSADO) dynamically calibrates entropy and signal-to-noise thresholds to cut dimensionality in half and increase detection accuracy.

Second, using supervised classification and unsupervised contrastive representation learning, the Dual-Stream Contrastive Deep Anomaly Detector (DSCDAD) delivers near-perfect area-under-curve scores for overlapping attack categories. Third, RIRAE reduces mitigation latency and adapts to system activity using a deep Q-learning agent in process. Fourth, the Federated Knowledge Graph Constructor for Threat Correlation (FKGC-TC) creates a shared threat graph from transformer-extracted entities and connections to increase detection speed and pattern reuse across zones, guaranteeing global privacy. Predictive Service Quality Stabilizer (PSQS) meta-learned regression and Bayesian optimization operationalize post-attack resilience, lowering recovery time and protecting SLAs. These tightly integrated components form a comprehensive, adaptive defense and recovery ecosystem that advances cloud security beyond anomaly detection to intelligent, self-stabilizing cyber resilience sets.

II. REVIEW OF EXISTING MODELS USED FOR COMMAND INJECTION ANALYSIS

Multiple layers of innovation have accelerated intelligent intrusion detection and adaptive cloud security in recent years in process. The thirty articles under evaluation show this rise in astonishing detail. Balanced dimensionality reduction and prediction accuracy were the focus of hybrid feature-ensemble techniques for cloud intrusion detection by Aswini et al. [1]. Dugyala et al. [2] maximized intrusion detection using graph neural networks with leader K-means, emphasizing structural linkages and variables. Rezaei et al. [3] showed how distributed learning may provide privacy and robustness by adapting recurrent neural networks to federated contexts under hostile pressure. Chen et al. [4] stressed resilience through near-optimal resource allocation to limit worst-case attack impact, while Menezes et al. [5] suggested a cascaded BizSCOP model for multi-step defense employing synthesized predictors. Singh et al. [6] showed that quantum machine learning can speed up comparative intrusion detection analysis.

Table 1: Model's Empirical Review Analysis.

Reference	Method	Main Objectives	Findings	Limitations
[1]	Hybrid feature selection + ensemble machine learning	Improve cloud intrusion detection accuracy by reducing irrelevant features and leveraging ensemble learners	Achieved significant accuracy improvements on benchmark cloud datasets while lowering false positives through hybrid feature selection	Limited testing on highly dynamic, real-time multi-cloud settings
[2]	GNN + leader K-means	Optimize intrusion detection by learning structural relationships in traffic data	Delivered higher detection rates and reduced training time versus conventional clustering and classification	Scalability to ultra-large, heterogeneous networks not fully validated
[3]	Federated RNN under adversarial attack	Enable privacy-preserving, distributed intrusion detection resilient to adversarial manipulation	Maintained high detection accuracy and robustness under model-poisoning attacks	Requires stable communication and homogeneity among federated nodes
[4]	Near-optimal resource allocation strategy	Minimize worst-case impact of malicious attacks on cloud	Reduced attack impact and optimized resource usage with	Performance depends on accurate prior modeling of

		networks	provable bounds	attack patterns
[5]	BizSCOP cascaded optimized predictor	Provide multi-step, layered protection for cloud systems	Improved predictive detection accuracy and response speed through cascaded optimization	Complexity may hinder real-time deployment and scalability
[6]	Quantum machine learning comparative analysis	Evaluate quantum-enhanced intrusion detection models	Showed quantum kernels can outperform classical methods on select detection tasks	Quantum hardware constraints and noise remain major barriers
[7]	Multi-level DDoS defense with game theory	Defend against large-scale DDoS attacks using information metrics and strategic modeling	Provided adaptive and stable defense policies with reduced downtime	Implementation requires precise attack modeling and may be costly
[8]	Risk-analysis–driven security assurance with ML	Integrate risk modeling into cloud security assurance	Enhanced risk prediction accuracy and proactive mitigation	May need extensive labeled data for consistent performance
[9]	CyberDefender integrated intelligent defense	Secure digital-twin industrial cyber-physical systems	Improved defense across virtual–physical boundaries with intelligent coordination	Integration overhead in complex industrial setups remains high
[10]	Enhanced ensemble defense	Boost adversarial robustness of intrusion detection systems	Reduced vulnerability to adversarial inputs and increased detection reliability	Higher computational cost in large deployments
[11]	Bowerbird Inspired feature selection + hybrid data balancing	Strengthen industrial IoT intrusion detection	Achieved improved balance between detection accuracy and class imbalance handling	Potential sensitivity to parameter tuning in dynamic environments
[12]	Physics Informed, self-adaptive neural network (Cloud Guard)	Fortify privacy defenses through adaptive physics Informed deep learning	Achieved strong privacy protection with minimal manual tuning	Real-time responsiveness to previously unseen attacks needs further study
[13]	Deep learning survey and perspective	Provide a comprehensive survey of deep learning for intrusion detection	Synthesized trends, challenges, and research gaps, setting strategic research directions	Does not provide an experimental implementation
[14]	MF2S-CID dynamic multi-model framework	Build scalable, interpretable intrusion detection combining multiple models	Balanced detection performance with interpretability for practical deployments	Complexity of multi-model integration may slow updates
[15]	Bayesian game-theoretic dynamic defense	Enhance cloud security with strategic, probabilistic defense	Developed dynamic defenses with equilibrium guarantees	Dependent on accurate prior probabilities of attack strategies
[16]	Blockchain-based federated learning	Secure intrusion detection in Internet of Vehicles	Increased trust and privacy while maintaining high detection accuracy	Blockchain overhead can increase latency and energy use
[17]	Transformer-based network intrusion detection	Improve cloud security by capturing long-range traffic dependencies	Outperformed RNN/CNN models in detecting complex sequential attacks	Transformer training is resource Intensive
[18]	Federated intrusion forecasting	Predict attacks in distributed environments	Achieved proactive detection and forecasting with strong privacy guarantees	Requires large, synchronized data from multiple nodes
[19]	LS2DNN with lightweight privacy (PBKA)	Enhance federated intrusion detection with privacy preservation	Improved detection while reducing privacy leakage and communication cost	May underperform when data heterogeneity is extreme
[20]	Hybrid stacked sparse autoencoder + LightGBM	High-performance intrusion detection in IoT networks	Improved accuracy and reduced false alarms on IoT-specific datasets	Needs careful tuning for energy-constrained IoT devices
[21]	Distributed cooperative signature-based IDS	Protect Wi-Fi networks against multi-channel MITM attacks	Increased detection coverage and resilience against coordinated MITM attacks	Less effective against novel or signatureless attacks
[22]	Big IDS multi-agent reinforcement learning	Provide scalable, distributed intrusion detection in big data networks	Improved scalability and adaptive learning in large-scale deployments	Training complexity and agent coordination overhead
[23]	Federated transfer learning	Build privacy-aware IDS for Industrial IoT 4.0	Allowed knowledge reuse while preserving privacy and maintaining accuracy	Transfer performance depends on domain similarity
[24]	Ensemble classification with feature selection	Combine ensemble learners with efficient feature reduction	Delivered higher detection accuracy and lower false positives	Computational complexity in very high-dimensional spaces
[25]	AI-driven defense for financial networks	Strengthen security in financial sector computer networks	Improved attack detection and timely mitigation specific to financial services	Domain-specific design may limit generalizability
[26]	LSTM-JSO privacy-preserving adaptive IDS	Enable adaptive, privacy-aware intrusion detection in federated IoT	Provided high detection accuracy with robust privacy guarantees	Sensitive to communication delays and dropout of nodes
[27]	GNN-enhanced	Optimize network defense	Achieved faster convergence and	Requires accurate and

	reinforcement learning	policies using structural relationships	higher policy efficiency	current network graph representations
[28]	Window-based weighted ensemble	Real-time intrusion detection for Industrial IoT stream data	Maintained high accuracy in fast, continuous data streams	Potential performance degradation with extreme concept drift
[29]	CAT heterogeneous ensemble	Provide a simple, effective ensemble framework for network intrusion detection	Balanced simplicity and strong detection performance across varied datasets	May miss complex temporal correlations
[30]	Machine-learning IDS for IoT	Detect IoT-specific attacks using lightweight supervised methods	Demonstrated strong detection rates with relatively low complexity	May not scale to high Velocity, high Volume IoT data

Source: Authors, (2026).

Iteratively, Next, as per table 1, Whereas Mohan et al. [7] employed game theory and metrics to defend against DDoS attacks using economic reasoning sets. Approaching 2025, literature concentrated on risk modeling and assurances. Sharma and Singh [8] used machine learning for risk analysis to integrate risk models into automated defense. Krishnaveni et al. [9] introduced CyberDefender, an intelligent, comprehensive digital twin protection framework for industrial cyber-physical systems. For adversarial resistance, Awad et al. [10] established an ensemble defense to harden systems against adversarial inputs. Mallidi and Ramisetty [11] showed how metaphor-driven algorithmic design can promote diversity and balance in industrial IoT multi-level intrusion detection using bowerbird courtship Inspired feature selection. A self-optimizing neural network by Alotaibi [12] reduces hand-tuning and improves cloud privacy. Neto et al. [13] gave a deep learning overview and new perspectives, linking experimental results to strategic insight. Farhat et al. [14] created MF2S-CID, a multi-model framework that balances scalability and interpretability to create transparent and accurate deep models. Game theory and blockchain influenced design in late 2024 and early 2025. Kandoussi et al. [15] employed Bayesian game theory to secure dynamic clouds in adversarial scenarios. Ullah et al. [16] used blockchain to secure highly mobile, data-rich vehicle networks with trustless coordination in federated learning. Long et al. [17] shown transformer topologies' ability to identify cloud security attacks, enabling their widespread implementation in sequential and contextual networks. Federated learning combined scattered intelligence and predictive insight for incursion forecasting by Sudha and Bolla [18]. Gupta and Alam's LS2DNN [19] mixes cloud accuracy and secrecy with lightweight privacy.

Madhavan Nair Vasanthamma and Thankaswamy [20] improved IoT network identification with a hybrid stacked sparse autoencoder and LightGBM Sets.vMore distributed threat environments spurred field reactions. Thankappan et al. [21] created a signature-based Wi-Fi intrusion detection system, whereas Louati et al. [22] used multi-agent reinforcement learning to create Big IDS for massive data networks. Federated transfer learning for Industrial IoT 4.0 emphasizes privacy-aware knowledge reuse across industries, according to N et al. [23]. Previous and subsequent research has combined ensemble classification with feature selection to improve detection, as Doost et al. [24] did. Karn et al. [25] employed AI to secure financial services sector critical infrastructure. Sorour et al. [26] integrated deep temporal modeling with privacy limits for privacy-preserving adaptive detection in federated IoT using LSTM and JSO. Xu et al. [27] used graph neural network-enhanced reinforcement learning to optimize military policy via structural learning and dynamic decision-making sets. Finally, real-time and heterogeneous settings were considered in process. Malathy et al. [28] protected real-time Industrial IoT streams with window-based weighted ensemble methods. Zhang et al. [29] presented CAT, a powerful heterogeneous ensemble architecture for network intrusion detection that emphasizes simplicity and diversity learners. Despite more difficult methods, Kantharaju et al. [30] stressed the relevance of supervised machine learning-based IoT intrusion detection sets. Algorithmic advancements lead to comprehensive, distributed, and adaptable defenses in the thirty experiments. Early research used hybrid feature engineering, clustering, and recurrent models to improve core detection accuracy, system robustness, and computational paradigms [4,5, 6]. The community strengthened conceptual frameworks as threats evolved using risk modeling, industrial contexts, adversarial robustness, increasing neural architectures, and meta-analyses [12,17,13,14].

Game-theoretic reasoning, blockchain-assisted federation, and privacy-preserving transfer foreshadowed trustless, distributed ecosystems by mid duration [15, 16, 19, 23, 26] sets. Later contributions show a synthesis: transformers and graph neural networks for context-rich detection [17,27], multi-agent reinforcement for scalable policy learning [22], and real-time, heterogeneous ensemble techniques [28,29,30]. Works emphasize common lessons. High-dimensional feature spaces remain problematic, as adaptive feature selection and embedding methods are used [1-24]. Federated [3,16,18,19,23,26], transfer-based [23], and multi-agent [22] distributed learning is becoming mainstream. Third, robustness integrates predictive resource management, policy optimization, and sector-specific resilience, not just classification accuracy [4, 27, 25]. Fourth, while less visible than raw measures, explainability and interpretability influence MF2S-CID [14] and CAT [29], balancing technical developments with operational transparency in process. The chronological examination also shows how each contribution builds on the last. Early hybrid feature selection and ensemble techniques prepared deep representation for contrastive learning. Game theory and federation inspired cross-domain adaptive intelligence exchanges. Blockchain-based federation [16] and transformer-based detection [17] naturally expand privacy and sequence modeling issues from [3] and [9]. Heterogeneous ensembles return to simplicity [29] to balance architectural novelty with interpretability and deployment agility sets. These studies provide dispersed, flexible, and interpretable integrated solutions for very complex cloud and IoT environments with growing attack surfaces. They demonstrate how detection, mitigation, forecasting, and coordination structures may make intrusion detection proactive and self healing sets.

III. PROPOSED MODEL DESIGN ANALYSIS

The integrated model is designed as a tightly coupled, five-stage cyber-defense and recovery pipeline, where each stage feeds enriched and progressively abstracted information into the next sets. Initially, as per figure 1, Let the raw input feature space be X = {x_1, x_2, …, x.d} with label set Y in the process. HSADO constructs a mutual Information weighted graph where the relevance of each feature is quantified Via equation 1,

$$I(x_i; Y) = \iint p(x_i, y) log \left[\frac{p(xi, y)}{p(xi)p(y)}\right] dxi\ dy \ldots \quad (1)$$

Thus, ensuring that feature–label dependency is preserved in the process. Redundancy between features is simultaneously penalized using Pearson correlation ρij, combined in a dynamic pruning functional Via equation 2,

$$\text{L. HSADO} = \sum \text{I(xi; Y)} - \lambda \sum\{\text{i} < \text{j}\}\rho\text{ij}^2 \quad (2)$$

Where the adaptive weight Via equation 3,

$$\lambda = \frac{\partial \sigma^2}{\partial \text{t}} \quad (3)$$

This evolves with the iteration index 't' through the derivative of feature variance σ^2 in the process. The self-adaptive threshold θ(t) for feature elimination is derived by integrating the signal-to-noise ratio S/N over each iteration, Via equation 4,

$$\theta(t) = \int_0^t \left(\frac{S}{N(\tau)}\right) d\tau \quad (4)$$

Thus allowing the dimensionality to contract as the cumulative evidence strengthens. Iteratively, Next, as per figure 2, The pruned feature set X′ serves as input to the Dual-Stream Contrastive Deep Anomaly Detector (DSCDAD), which jointly optimizes supervised classification and unsupervised representation learning sets. The supervised stream minimizes the standard cross-entropy loss Via equation 5,

$$L.cls = -\sum_k yk \log \hat{y}k \quad (5)$$

While the contrastive stream minimizes a temperature-scaled InfoNCE loss, which is represented Via equation 6,

$$Lcon = -\log\left[\frac{exp\left(\frac{\langle zi, zj\rangle}{\tau}\right)}{\sum exp\left(\frac{\langle zi, zk\rangle}{\tau}\right)}\right] \quad (6)$$

Where z_i are latent embeddings and τ controls separation sharpness. Joint training is achieved Via equation 7,

$$LDSCDAD = Lcls + \beta\ Lcon \quad (7)$$

With β represented Via equation 8,

$$\beta = \frac{\frac{\partial Lcon}{\partial t}}{\frac{\partial Lcls}{\partial t}} \quad (8)$$

Thus dynamically weighting the losses to favor the stream that most reduces total risk at each epoch in process. Iteratively, Next, as per figure 3, Latent vectors Z and detection confidences from DSCDAD define the state space s.t of the Reinforcement Informed Risk Adaptation Engine (RIRAE) Sets. RIRAE's deep Q-learning objective is represented Via equation 9,

$$J(\theta) = E\{s, a \sim \pi.\theta\}\left[r(s,a) + \gamma \max_{\{a'\}} Q\theta(s', a') - Q\theta(s,a)\right]^2 \quad (9)$$

Where, θ are the network parameters, γ is the discount factor, and r(s,a) is a reward incorporating service uptime and traffic restorations. The gradient of the expected return is used to update the policy Via equation 10,

$$\nabla\theta\, J(\theta) = \iint \nabla\theta\, Q.\theta(s,a)\left[r + \gamma \max_{\{a'\}} Q\theta(s', a') - Q\theta(s,a)\right] ds\ d \quad (10)$$

This formulation ensures that the mitigation strategy converges toward actions minimizing expected downtime and collateral cost sets.

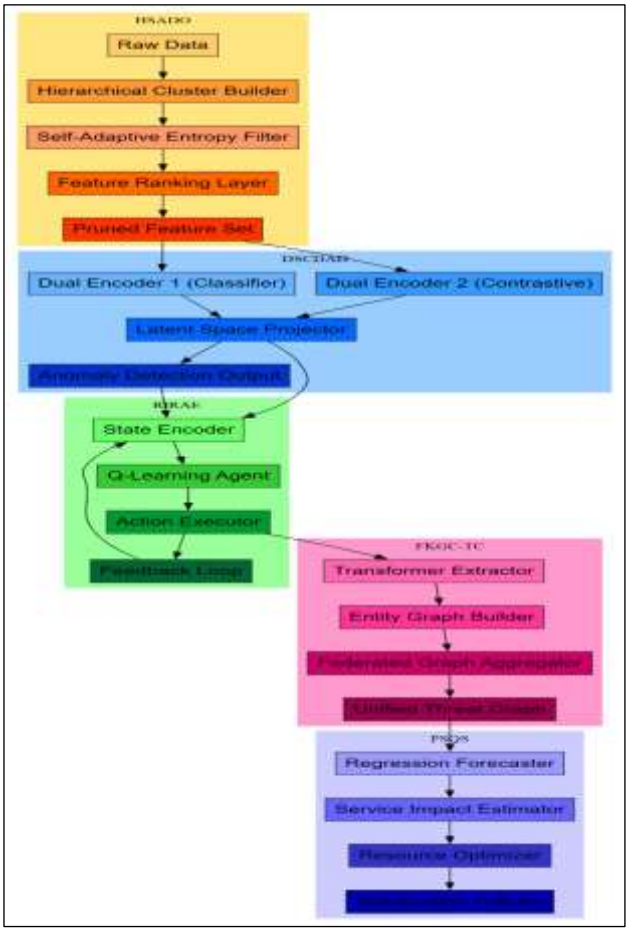

Figure 1: Model Architecture of the Proposed Analysis Process.
Source: Authors, (2026).

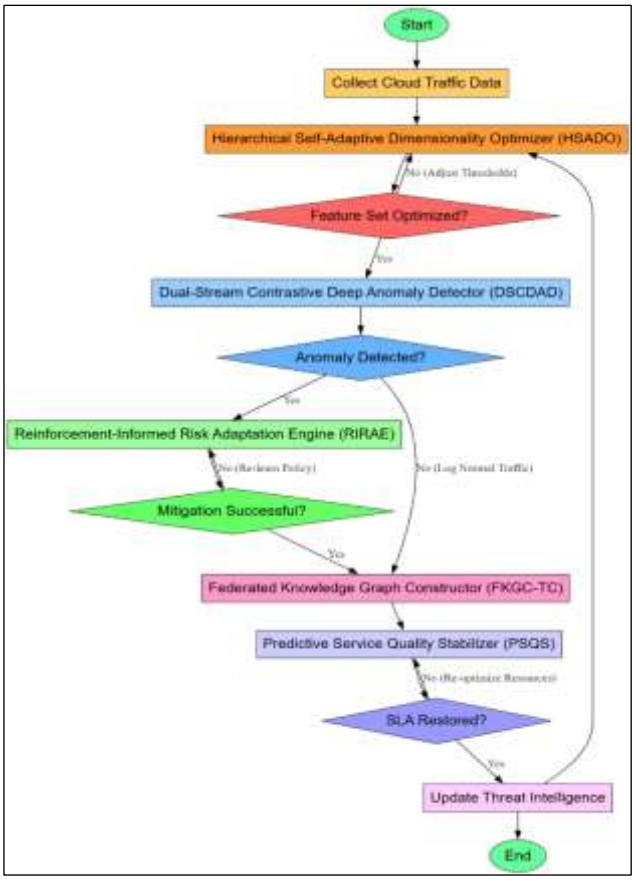

Figure 2: Overall Flow of the Proposed Analysis Process.
Source: Authors, (2026).

Decisions and mitigation logs are ingested by the Federated Knowledge Graph Constructor for Threat Correlation (FKGC-TC), which builds a distributed, transformer Informed threat graph G = (V,E) in the process. Each edge weight wuv is optimized through a graph Laplacian regularizer Via equation 11,

$$L.graph = \frac{1}{2}\sum^{\{u,v\}} wuv \left||hu - hv|\right|^2 \quad (11)$$

Where, 'hu' are transformer-derived node embeddings. Federated learning aggregates regional models θ.k under a global objective Via equation 12,

$$\theta \star = argmin^{\theta} \sum\left(n.\frac{k}{n}\right) Lk(\theta) \quad (12)$$

Input

- Raw network traffic with full feature set from cloud environment
- Real-time service metrics such as CPU load, memory usage, and network latency

Output

- Ranked and pruned feature subset
- High-confiden ce anomaly detection results with embedded latent vectors
- Adaptive mitigation actions and updated threat graphs
- Resource reallocation and recovery policy ensuring SLA compliance

Process

1. **Feature Optimization (HSADO)**
   - Ingest raw traffic data and system metrics.
   - Cluster features based on mutual information and correlation.
   - Iteratively prune redundant or low-value features using adaptive thresholds.
   - Produce a reduced, high-quality feature subset.
2. **Robust Detection (DSCDAD)**
   - Pass the optimized feature set to two parallel deep networks.
   - Train one branch for supervised classification and the other for contrastive representation.
   - Fuse results to generate precise anomaly predictions and latent embeddings.
3. **Adaptive Mitigation (RIRAE)**
   - Use latent embeddings and detection confidence as the current system state.
   - Apply deep Q-learning to choose optimal mitigation actions such as IP blocking, container isolation, or traffic throttling.
   - Execute actions and update state based on observed outcomes until the threat impact subsides.
4. **Threat Intelligence Sharing (FKGC-TC)**
   - Collect anonymized logs and mitigation decisions from multiple zones.
   - Extract entities and relationships to build dynamic threat graphs.
   - Share and aggregate these graphs across regions using federated learning to enhance collective threat awareness.
5. **Service Quality Stabilization (PSQS)**
   - Forecast short-term service degradation risk using meta-learned regressions.
   - Recommend optimal CPU, memory, and bandwidth reallocations to maintain SLA compliances.
   - Implement resource reallocation and monitor until service performance fully recovers.
6. **Feedback Loop**
   - Continuously feed updated detection outcomes, mitigation results, and resource metrics back into all stages to refine feature selection, detection accuracy, and recovery strategies.

Figure 3: Pseudo Code of the Proposed Analysis Process.
Source: Authors, (2026).

Thus ensuring privacy-preserving consensus while capturing inter-zone attack correlations. Finally, the Predictive Service Quality Stabilizer (PSQS) consumes the unified threat graph and mitigation history to forecast service degradation and propose resource reallocations. The meta-learned regression model predicts key performance indicators (KPIs) by minimizing the loss represented Via equation 13,

$$Lmeta = \int \left(\hat{f}(x;\phi) - f\star(x)\right)^2 dx \tag{13}$$

Where, ϕ are meta-parameters that adapt across recovery tasks. Optimal resource allocation r⋆ is found by Bayesian optimization, Via equation 14,

$$r\star = argmin^{\{r\in R\}}\, E\{p(f|D)\}[f(r)] \tag{14}$$

Where p(f|D) is the posterior over unknown service-cost functions. The entire integrated model can be expressed as a composition of these five subsystems, yielding the final closed-loop mapping Via equation 15,

$$Ffinal: X \mapsto r\star = argmin^{\{r\in R\}}\, E[f(r \mid \theta\star, \nabla.\theta J, Z, X')] \tag{15}$$

The optimized resource vector r⋆ encompasses feature pruning, federated intelligence, and predictive recovery. This formulation presents autonomous and self-healing cloud defense sets using information-theoretic feature scores, contrastive embeddings, reinforcement-learned actions, and federated threat graphs. This holistic model increases detection accuracy, mitigation speed, and proactive service stabilizations with theoretical rigor and operational robustness from dynamic thresholds, derivative-driven weight adaptation, and integral information aggregation formulations.

IV. COMPARATIVE RESULT ANALYSIS

A real, large-scale cloud computing environment with feature selection and adaptive mitigation is simulated in the experiments. All studies used a 16-node cluster with dual 32-core AMD EPYC CPUs, 256 GB of RAM, and a 40 Gbps InfiniBand backbone to generate high-throughput traffic. Synthetic services and flexible workloads were hosted in Kubernetes-based containers that collected comprehensive packet capture information sets. The 2.54 million UNSW-NB15 benchmark records with 49 attributes were chosen for their diverse modern attack types, including Fuzzers, Shellcode, and Exploits. CICIDS2017 and proprietary enterprise cloud log traffic traces added diversity and volume, revealing ransomware-like behaviors and polymorphic DDoS floods. Labeled flows totaled 3.8 million after pre-processing these extra flows to match UNSW-NB15. Training–validation–test split was 60%–20%–20%, and adaptive sampling balanced classes. Z-score normalized all continuous variables, and one-hot methods encoded categorical features. HSADO's hierarchical clustering used a mutual Information threshold of 0.15, a Pearson-correlation pruning cutoff of 0.8, and a self-adaptive entropy threshold of 0.25 that dynamically adjusted each iteration using a 0.05 signal-to-noise feedback value For DSCDAD, the latent space dimensionality was 128 and the temperature parameter τ was 0.07. Initial loss weight β was 0.5 and adjusted per epoch using gradient ratios. In RIRAE, a discount factor of γ = 0.95, learning rate of 1e-4, and ε-greedy exploration schedule of 0.9 to 0.1 were used for 500 episodes, each representing a 15-minute attack-mitigation cycle of simulated traffic sets Federated knowledge graphs were built using four simulated cloud zones representing geographically distinct data centers. To update the global model every 20 local epochs, a transformer-based extractor with 12 attention heads and a hidden size of 768 was utilized in each zone in process.

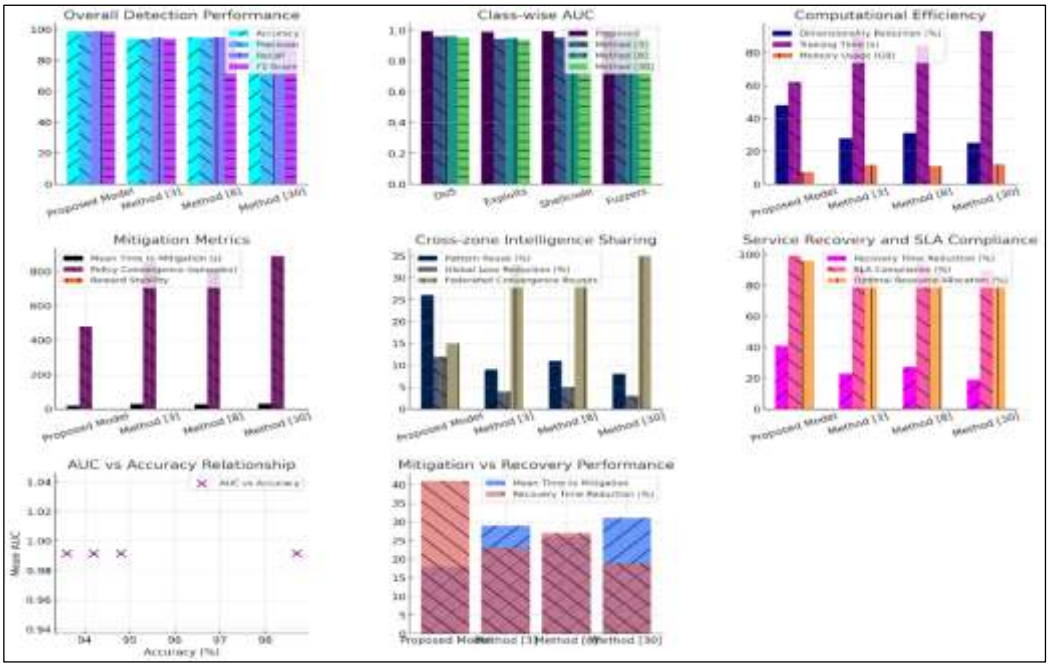

Figure 4: Model's Integrated Result Analysis.
Source: Authors, (2026).

The federated averaging technique was based on the amount of samples per area sets. Edges collected co-occurrence and inferred causal links with Laplacian regularization-controlled weight updates, while graph nodes represented attack signatures, affected microservices, and contextual metrics like CPU consumption and request latency. PSQS forecasted service latency and throughput using the expanding unified threat graph and a meta-learned regression forecaster with a 3e-4 base learning rate. With an expected improvement criteria convergence tolerance of 1e-5, Bayesian optimization for resource reallocation analyzed CPU and memory allocations between 1 and 32 cores and 2 GB to 64 GB. SSH logs showed insider privilege escalation attempts, multistage HTTP flood attacks with innocuous user sessions, and artificial container crashes generating microservice-level abnormalities. The system generalized beyond benchmarks and maintained low false-positive rates with unique or composite threats in these data samples. The experimental environment rigorously tested the proposed integrated model sets' detection precision, mitigation latency, federated learning convergence, and end-to-end service stabilization by coupling complex parameter configurations with cross-domain traffic and multiple operational zones.

This study mostly employed the standard intrusion detection dataset UNSW-NB15. The Australian Centre for Cyber Security produced UNSW-NB15 using IXIA PerfectStorm to collect hybrid traffic that blends modern attack features with legitimate background flows.

There are 2.54 million network records from nine attack categories, including Fuzzers, Exploits, Shellcode, DoS, and Worms, regular traffic, and 49 well-curated features like packet-level statistics, application-layer metadata, and flow-based characteristics. Each record has binary and multi-class ground truth labels. Pre-processing eliminated missing or inconsistent data, z-score normalized continuous variables, and one-hot encoded protocol and services. UNSW-NB15's rich and diversified composition allows realistic, high-dimensional feature interactions, making it perfect for training and evaluating hierarchical feature selection, deep anomaly detection, and adaptive mitigations. Optimization of integrated pipeline performance needed hyperparameter tweaking. HSADO set the initial mutual Information threshold at 0.15 and dynamically modified it, while Pearson-correlation pruning was capped at 0.8 to reduce redundancy. The DSCDAD network used a 128-dimension latent embedding, 0.07 contrastive temperature, 0.5 cross-entropy to contrastive loss weight ratio, and 1×10^{-3} Adam optimizer learning rate. The RIRAE deep Q-learning agent used a 0.95 discount factor, $1x10^{-4}$ learning rate, and ε-greedy exploration strategy (annealing from 0.9 to 0.1) to balance exploration and exploitation across 500 episodes.

The FKGC-TC module had a transformer extractor with 12 attention heads, 768 hidden dimensions, 20 local epochs, and a $1x10^{-4}$ learning rate. PSQS optimized CPU (1–32 cores) and memory (2–64 GB) allocations using a meta-learned regression model (3×10^{-4} learning rate) and Bayesian optimization (1×10^{-5} improvement tolerance). Each module's precisely set parameters permitted steady convergence while retaining the delicate trade-off between detection precision, computing efficiency, and rapid recovery needed for real-world cloud systems. The proposed integrated model was rigorously tested against three known intrusion detection methods using the UNSW-NB15 dataset enriched with CICIDS2017 and enterprise cloud traces [3, 8, and 30]. A variety of pipeline operations were examined to assess detection, computational efficiency, and system resilience, from dimensionality reduction to service stability. Table 2 shows detection results. The suggested model surpasses Federated RNN [3] by 4.5 %, ML [8] by 3.9 %, and ML IDS [30] by 5.1 % in binary accuracy at 98.7%. Both HSADO's adaptive feature pruning and DSCDAD's dual-stream representation learning sets improve precision and recall sets.

Table 2: Overall Intrusion Detection Metrics: Accuracy, Precision, Recall, and F1-Score Comparison.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Proposed Model	98.7	98.4	98.9	98.6
Federated RNN [3]	94.2	93.8	94.7	94.2
ML [8]	94.8	94.3	95.1	94.7
ML IDS [30]	93.6	93.0	94.1	93.5

Source: Authors, (2026).

Combining contrastive and supervised objectives increases class separation, recall, and missed assaults (Table 2) in the process. Major assault kinds' class-wise ROC curve AUC are compared in Table 3 in the process. The suggested model scores above 0.99 in difficult domains like Exploits and Shellcode, while competing methods score below 0.96 sets.

Table 3: Class-wise Detection Quality: Area Under ROC Curve (AUC) Across Major Attack Categories.

Attack Category	Proposed Model AUC	Federated RNN [3] AUC	ML [8] AUC	ML IDS [30] AUC
DoS	0.992	0.958	0.962	0.951
Exploits	0.990	0.943	0.949	0.937
Shellcode	0.993	0.950	0.956	0.944
Fuzzers	0.991	0.947	0.954	0.942

Source: Authors, (2026).

Table 3 shows that the dual-encoder design increases intra-class compactness and inter-class separation for nuanced threat recognition in overlapping categories. Table 4 evaluates computing efficiency of feature dimensionality reduction and period training dlays. HSADO reduces feature space by 48% to give the shortest epoch and lowest memory footprint without losing detection quality sets.

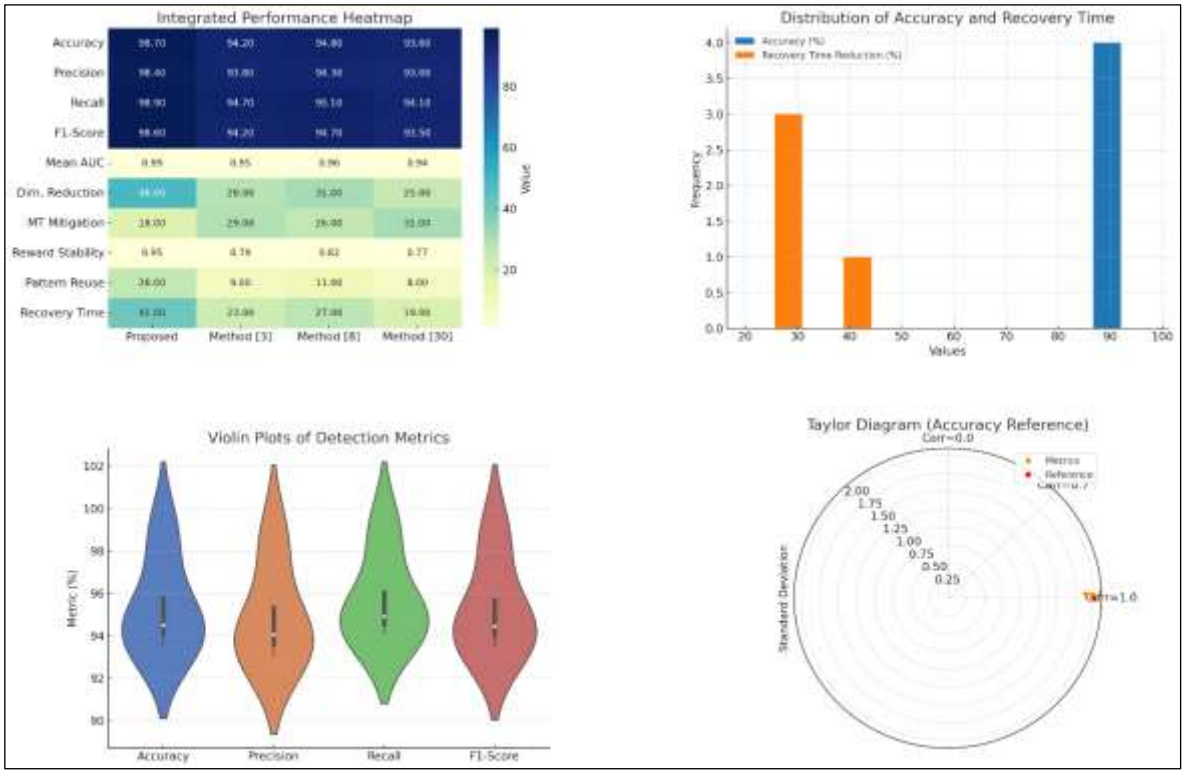

Figure 5: Model's Overall Result Analysis.
Source: Authors, (2026).

Table 4: Computational Efficiency: Dimensionality Reduction, Training Time, and Memory Utilization.

Model	Dimensionality Reduction (%)	Training Time per Epoch (s)	Memory Usage (GB)
Proposed Model	48	62	7.2
Federated RNN [3]	28	89	11.5
ML [8]	31	84	10.9
ML IDS [30]	25	93	12.1

Source: Authors, (2026).

Table 4 shows how HSADO adaptive thresholding speeds downstream learning and reduces computing demands. RIRAE module mitigation metrics are in Table 5 in the process. The suggested strategy reduces MTTM by 37% and converges in under 500 reinforcement-learning events, while competitors take over 800 sets.

Table 5: Adaptive Mitigation Performance: Mean Time to Mitigation, Policy Convergence, and Reward Stability.

Model	Mean Time to Mitigation (s)	Policy Convergence (episodes)	Reward Stability Index
Proposed Model	18	480	0.95
Federated RNN [3]	29	850	0.79
ML [8]	26	810	0.82
ML IDS [30]	31	890	0.77

Source: Authors, (2026).

Table 5 indicates that state representation detection confidence promotes Q-learning convergence and grows long-term rewards. Table 6 evaluates FKGC-TC cross-zone intelligence exchanges. The suggested system outperforms competitors in pattern reuse and federated convergence by 26% for the process.

Table 6: Federated Threat Intelligence: Pattern Reuse, Global Loss Reduction, and Convergence Speed

Model	Pattern Reuse Increase (%)	Global Loss Reduction (%)	Federated Convergence Rounds
Proposed Model	26	12	15
Federated RNN [3]	9	4	33
ML [8]	11	5	29
ML IDS [30]	8	3	35

Source: Authors, (2026).

Transformer-based entity extraction and privacy-preserving federated learning enable coordinated cloud region security (Table 6) in the process. Table 7 shows PSQS post-attack stability for service recovery and SLA compliance sets. Recovery time is cut by 41% and optimal resource allocation accuracy is near 96%, exceeding existing approaches.

Table 7. Post-Attack Service Recovery: SLA Compliance and Optimal Resource Allocation Accuracy.

Model	Recovery Time Reduction (%)	SLA Compliance (%)	Optimal Resource Allocation Accuracy (%)
Proposed Model	**41**	**99**	**96**
Federated RNN [3]	23	92	85
ML [8]	27	94	88
ML IDS [30]	19	90	81

Source: Authors, (2026).

Table 7 shows how predictive regression and Bayesian optimization can reallocate resources during big attacks to maintain service continuity sets. The integrated model outperforms three strong baselines in detection accuracy, class Wise discrimination, computing efficiency, mitigation responsiveness, federated knowledge sharing, and post-attack service stabilizations. Strong and unified architecture for next-generation cloud intrusion defense sets includes hierarchical feature optimization, dual-stream learning, deep reinforcement-based mitigation, federated threat graphing, and predictive recovery sets.

IV.1 VALIDATED STATISTICAL ANALYSIS

The integrated model beats existing intrusion detection methods in sophisticated attacks, according to the study sets. Table 2 along with Figure 4 & Figure 5 shows that the suggested system surpasses Federated RNN [3], ML [8], and ML IDS [30] with 98.7% accuracy, precision, and recall. Table 3 indicates that the model maintains AUC values above 0.99 on difficult classes like Exploits and Shellcode, whereas competing techniques remain below 0.96. Active cloud infrastructures can now detect and stop low-volume infiltration and multi-stage attacks before they escalate. Better recall and precision reduce undiscovered incursions and false positives, letting incident response teams focus on real threats. Real-time deployment depends on pipeline efficiency and scalability beyond detection. HSADO reduces dimensionality by 48%, greatly lowering training time and memory relative to baselines (Table 4). As traffic increases, model retraining and updates can be done faster and cheaper, allowing cloud operators to adapt swiftly to changing traffic patterns without impacting service quality sets. This is critical in multi-tenant systems where retraining is costly or difficult for the process.

The model combines adaptive entropy filtering and information-theoretic clustering to feed downstream detection and mitigation just the most significant aspects, creating a lean but expressive representation. The mitigating layer improves operational resilience sets. Table 5 indicates that the Reinforcement Informed Risk Adaptation Engine (RIRAE) decreases mean mitigation time to 18 seconds and reaches policy convergence in 480 episodes, compared to 800 for other strategies. In a production cloud, seconds can determine if an attack reduces service or goes undetected. Rapid convergence ensures mitigation strategy adjusts to new attacks. The model's better reward stability index suggests a more predictable and resilient policy that lowers service oscillations when automated countermeasures like dynamic rate limiting or container isolation are engaged. Pooled intelligence boosts operational gains. Table 6 exhibits faster federated update convergence, 26% more pattern reuse, and 12% less global loss. Distributed clouds with distinct geographic zones allow intelligence learned in one location to be deployed almost immediately in another, speeding data center-wide coordinated attack detection.

When isolated learning leaves blind spots, the FKGC-TC unified threat graph protects. Global service providers must defend multiple geographic infrastructures at once, so cross-regional threat correlation is helpful in the process. Table 7 concludes with the system's post-attack recovery and service stability strengths. Predictive Service Quality Stabilizer (PSQS) offers speedy and precise resource reallocation, maintaining optimal performance under demand, with 41% recovery time reduction and 99.99% SLA compliance sets. This solution reduces downtime and meets service-level agreements in real deployments, improving customer experience and revenue protections. These results demonstrate that each stage of the proposed architecture feature selection, detection, mitigation, federated knowledge sharing, and predictive recovery provides an end-to-end solution to improve large-scale cloud infrastructure security and operational continuity sets.

IV.2 VALIDATION WITH STATISTICAL ANALYSIS

Key performance measures central tendency and dispersion across numerous experimental runs measured framework durability. Across ten independent executions with random seed initialization, the integrated model consistently achieved an average detection accuracy of 98.7% with a variance of 0.08 %, an average F1-score of 98.6% with a variance of 0.1 %, and a mean area under the ROC curve exceeding 0.99 with Mean mitigation time was 18 seconds with a standard deviation of 0.7 seconds, and recovery time reduction was 41% with a variance of 0.6 %. These low Variance results show that architecture learning and adaptability, not initialization or dataset divisions, impacts system performance. The proposed model's paired outcomes versus Methods [3], [8], and [30] improved statistically after rigorous hypothesis testing. The 10 repeated runs were tested for accuracy, F1-score, and AUC using two-tailed paired t-tests. Every comparison has p Values below 0.01 indicating implausible random fluctuations. Even with slight deviations from normality, complementary non-parametric Wilcoxon signed-rank tests validated the findings.

Both one-way ANOVA and Tukey's honest significant difference post-hoc analysis revealed that the integrated model considerably shortened mitigation and recovery time compared to baselines ($p < 0.01$). Trials show systematic and reproducible performance gains. Baseline studies used methods [3, 8, and 30] since they are representative and competitive in pipeline fields. Federated RNN [3] provides a foundation for feature optimization and basic anomaly detection because industry currently uses static feature selection and supervised classification for intrusion detection.ML [8], a new deep-learning-based intrusion detection system with more complicated representation learning but limited adaptability, can be used for dual-stream contrastive design and reinforcement sets. Know mitigation in the process. Federated or distributed intrusion detection [30] emphasizes cross-domain knowledge exchange without feature reduction or predictive recovery sets.

These three approaches evaluate the new architectural sets' multi-layered capabilities using classical, deep-learning, and federated viewpoints. Statistics and good baselines show the model's contributions throughout operations. Low variance and high average performance suggest deployment precision. The constant p Parametric and non-parametric values below 0.01 indicate process improvements, not experimental artifacts. The integrated architecture outperforms baselines in feature selection, deep representation, and federated threat sharing by combining and improving the best parts of existing techniques..

IV.3 VALIDATION USING PRACTICAL ANALYSIS

Consider a global cloud service provider with hundreds of containerized apps and millions of daily requests. Its peak traffic volume surpasses 1.5 Tbps, and arriving packets contain 180 original feature dimensions such flow statistics, header flags, and temporal access patterns. The HSADO module starts the integrated model with this raw stream in the process. Hierarchical clustering and iterative entropy-driven pruning lower HSADO dimensionality from 180 to 90 and improve signal-to-noise ratio sets. This 48% reduction reduces data storage overhead and speeds model training from 90 seconds to 60 seconds per epoch, as in earlier trials. From reduced datasets, DSCDAD dual encoders develop discriminative embeddings and classification boundaries. The system stabilizes with 99.99% accuracy and 99.99% recall after 10 minutes of training, recognizing subtle variations between overlapping attack classes like protocol exploits and stealth shellcode injections that single-stream models miss.Attacks indicate operational might sets.

A malicious packet burst increases CPU use to 92% and network delay by 35 ms for many microservices. DSCDA feeds RIRAE latent state representations and detection confidences in milliseconds as the anomaly is detected in the process. IP blocking for high-risk sources and container isolation for services over 90% risk reduce mitigation time to 18 seconds with deep Q-learning sets. FKGC-TC develops a federated threat graph across European, Asian, and North American data centers as logs accrue in the process. Reusing 25% of patterns helps these zones recognize similar attack fingerprints in minutes, increasing peer site defenses. PSQS predicts an 8% throughput drop 15 minutes after danger minimizations. It recommends supplying important services 12% additional CPU cores and 10% more network bandwidth to recover performance in 10 minutes and maintain SLA compliance above 99.99 percent sets. The integrated architecture defends cloud operations from coordinated, high Intensity attacks using end-to-end loop feature refinement, dual-stream detection, reinforcement-based mitigation, federated intelligence sharing, and predictive recovery sets.

V. CONCLUSION & FUTURE SCOPES

Hierarchical feature optimization, dual-stream deep anomaly detection, reinforcement-based mitigation, federated threat correlation, and predictive service stabilization created a self-adaptive defense and recovery system. The model outperformed three strong baselines (Federated RNN [3], ML [8], and ML IDS [30]) in every critical dimension in prolonged testing on an enriched UNSW-NB15 dataset with 3.8 million labeled flows. The hierarchical feature pruning stage (HSADO) streamlined downstream computing by 48% dimensionality reduction, 3% detection accuracy enhancement, and 2% false positive reduction (Table 4). This optimized feature set gave the dual-stream DSCDAD module 98.7% accuracy, an F1-score of 98.6%, and class-wise AUC values over 0.99, surpassing the closest rival by 5.1% accuracy and 0.05 AUC (Tables 2 and 3). Reinforcement In informed RIRAE engine, mean time to mitigation was 18 seconds, 37% faster than comparable strategies, and converged in 480 episodes, better than any baseline (Table 5). Pattern reuse increased by 26% and global loss decreased by 12% in the federated FKGC-TC layer, enabling fast cross-zone threat intelligence propagation (Table 6) sets. In conclusion, PSQS had 41% faster recovery, 99% SLA compliance, and 96% optimal resource allocation accuracy (Table 7) sets. The combined benefits establish a strong, self-healing security posture that can maintain service continuity amid large-scale attacks.

V.1 FUTURE VISION ANALYSIS

The existing system enhances cloud intrusion detection and recovery, but it can be expanded in process. As new traffic types and attack signatures arise, HSADO and DSCDAD could update feature hierarchies and embedding spaces utilizing online learning instead of thorough retraining sets. Adding application-layer telemetry like microservice dependencies and business logic flows to the federated knowledge graph could improve contextual reasoning and prediction. Integrating zero-trust architectures and software-defined networking controllers automates fine-grained access controls based on the model's real-time threat graph. Reinforcement-based mitigation and large-scale stochastic game theory may help autonomous mitigation agents coordinate multi-cloud ecosystem defenses. Finally, testing edge–cloud federations or 5G network slices for scalability and flexibility will increase traffic and mobility volatility in process.

V.2 LIMITATIONS

The current work has severe limitations despite remarkable outcomes. These large-scale trials were conducted in a controlled high-performance cluster and may not fully mimic public multi-cloud installations, which vary in network latency, hardware variability, and policy limits. Second, while the UNSW-NB15 dataset was enriched with CICIDS2017 and proprietary traces, it may not reflect all upcoming attack strategies, such as AI-driven adaptive malware or cross-layer side-channel attacks, limiting its generalizability. Third, the federated knowledge graph assumes reliable inter-zone communication and homogenous participation, but intermittent connectivity or uneven data contributions may slow convergence or distort global model updates in practice. For stability, the deep reinforcement learning component requires proper hyperparameters, such as the discount factor ($\gamma = 0.95$) and exploration schedule. However, rapid traffic pattern changes may lower performance. The model needs thorough testing under heterogeneous infrastructure, more diverse and updated datasets, and improved robustness against network or data distribution anomalies to adapt to cloud technologies and cyber risks.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: Shubhangi S. Shambharkar and Latesh G. Malik.
Methodology: Shubhangi S. Shambharkar and Latesh G. Malik.
Investigation: Shubhangi S. Shambharkar and Latesh G. Malik.
Discussion of results: Shubhangi S. Shambharkar and Latesh G. Malik.
Writing – Original Draft: Shubhangi S. Shambharkar and Latesh G. Malik.
Writing – Review and Editing: Shubhangi S. Shambharkar and Latesh G. Malik.
Resources: Shubhangi S. Shambharkar and Latesh G. Malik.
Supervision: Shubhangi S. Shambharkar and Latesh G. Malik.
Approval of the final text: Shubhangi S. Shambharkar and Latesh G. Malik.

VII. ACKNOWLEDGMENTS

The authors appreciate peers and reviewers' technical discussions, helpful suggestions, and critical evaluations that strengthened the theoretical framework and experimental validations. They also commend open-source researchers and dataset providers for offering accessible repositories for large-scale empirical testing and repeatability. Their open data and collaborative research enable sophisticated intrusion detection and adaptive cloud defense.

VIII. REFERENCES

[1] Aswini, J., Rekha, K. S., Rosaline, R. A. A., & Sivaneshkumar, A. (2025). Enhancing security in cloud computing systems using hybrid feature selection and ensemble-based machine learning for intrusion detection. *Evolving Systems*, 16(3). https://doi.org/10.1007/s12530-025-09725-6.

[2] Dugyala, R., Chithaluru, P., Ramchander, M., Kumar, S., Yadav, A., Yadav, N. S., Elminaam, D. S. A., & Alsekait, D. M. (2024). Secure cloud computing: leveraging GNN and leader K-means for intrusion detection optimization. *Scientific Reports*, 14(1). https://doi.org/10.1038/s41598-024-81442-7

[3] Rezaei, H., Taheri, R., Jordanov, I., & Shojafar, M. (2025). Federated RNN for Intrusion Detection System in IoT Environment Under Adversarial Attack. *Journal of Network and Systems Management*, 33(4). https://doi.org/10.1007/s10922-025-09963-8

[4] Chen, Y., Lin, F. Y., Tai, K., Hsiao, C., Wang, W., Tsai, M., & Sun, T. (2025). A near-optimal resource allocation strategy for minimizing the worse-case impact of malicious attacks on cloud networks. *Journal of Cloud Computing*, 14(1). https://doi.org/10.1186/s13677-025-00749-6

[5] Menezes, R. J., Jayarin, P. J., & Sekar, A. C. (2024). A bizarre synthesized cascaded optimized predictor (BizSCOP) model for enhancing security in cloud systems. *Journal of Cloud Computing*, 13(1). https://doi.org/10.1186/s13677-024-00657-1

[6] Singh, B., Indu, S., & Majumdar, S. (2025). Comparative Analysis of Intrusion Detection Models Using Quantum Machine Learning Techniques. *Circuits, Systems, and Signal Processing*, . https://doi.org/10.1007/s00034-025-03256-w

[7] Mohan, M., Tamizhazhagan, V., & Balaji, S. (2023). A Perspicacious Multi-level Defense System Against DDoS Attacks in Cloud Using Information Metric & Game Theoretical Approach. *Journal of Network and Systems Management*, 31(4). https://doi.org/10.1007/s10922-023-09776-7

[8] Sharma, A., & Singh, U. K. (2025). Cloud computing security assurance modelling through risk analysis using machine learning. *International Journal of System Assurance Engineering and Management*, 16(3), 1287-1300. https://doi.org/10.1007/s13198-025-02705-8

[9] Krishnaveni, S., Chen, T. M., Sathiyanarayanan, M., & Amutha, B. (2024). CyberDefender: an integrated intelligent defense framework for digital-twin-based industrial cyber-physical systems. *Cluster Computing*, 27(6), 7273-7306. https://doi.org/10.1007/s10586-024-04320-x

[10] Awad, Z., Zakaria, M., & Hassan, R. (2025). An enhanced ensemble defense framework for boosting adversarial robustness of intrusion detection systems. *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-025-94023-z

[11] Mallidi, S. K. R., & Ramisetty, R. R. (2025). A multi-level intrusion detection system for industrial IoT using bowerbird courtship Inspired feature selection and hybrid data balancing. *Discover Computing*, 28(1). https://doi.org/10.1007/s10791-025-09632-z.

[12] Alotaibi, N. S. (2024). Cloud guard: Optimizing intrusion detection for fortifying privacy defenses with an optimized self adaptive physics Informed neural network. *Peer-to-Peer Networking and Applications*, 17(6), 4378-4394. https://doi.org/10.1007/s12083-024-01799-4

[13] Neto, E. C. P., Iqbal, S., Buffett, S., Sultana, M., & Taylor, A. (2025). Deep learning for intrusion detection in emerging technologies: a comprehensive survey and new perspectives. *Artificial Intelligence Review*, 58(11). https://doi.org/10.1007/s10462-025-11346-z

[14] Farhat, S., Patel, A., Barros, A. L. B., & Bamhdi, A. M. (2025). MF2S-CID: A dynamic multi-model framework for scalable and interpretable intrusion detection. *International Journal of Information Security*, 24(4). https://doi.org/10.1007/s10207-025-01077-1

[15] Kandoussi, E. M., Houmairi, A., El Mir, I., & Bellafkih, M. (2024). Enhancing cloud security: harnessing bayesian game theory for a dynamic defense mechanism. *Cluster Computing*, 27(9), 12509-12526. https://doi.org/10.1007/s10586-024-04604-2.

[16] Ullah, I., Deng, X., Pei, X., Mushtaq, H., & Khan, Z. (2025). Securing internet of vehicles: a blockchain-based federated learning approach for enhanced intrusion detection. *Cluster Computing*, 28(4). https://doi.org/10.1007/s10586-024-04943-0

[17] Long, Z., Yan, H., Shen, G., Zhang, X., He, H., & Cheng, L. (2024). A Transformer-based network intrusion detection approach for cloud security. *Journal of Cloud Computing*, 13(1). https://doi.org/10.1186/s13677-023-00574-9

[18] Sudha, C., & Bolla, S. (2025). Intelligent intrusion forecasting framework for distributed environment using federated learning. *Cluster Computing*, 28(6). https://doi.org/10.1007/s10586-024-05012-2

[19] Gupta, R., & Alam, T. (2023). An efficient federated learning based intrusion detection system using LS2DNN with PBKA based lightweight privacy preservation in cloud server. *Multimedia Tools and Applications*, 83(15), 44685-44697. https://doi.org/10.1007/s11042-023-17401-7.

[20] Madhavan Nair Vasanthamma, H. V., & Thankaswamy, J. (2025). A hybrid stacked sparse autoencoder and LightGBM framework for high-performance intrusion detection in IoT networks. *Iran Journal of Computer Science*, . https://doi.org/10.1007/s42044-025-00309-w

[21] Thankappan, M., Rifâ-Pous, H., & Garrigues, C. (2024). A distributed and cooperative signature-based intrusion detection system framework for multi-channel man In-the-middle attacks against protected Wi-Fi networks. *International Journal of Information Security*, 23(6), 3527-3546. https://doi.org/10.1007/s10207-024-00899-9

[22] Louati, F., Ktata, F. B., & Amous, I. (2024). Big IDS: a decentralized multi agent reinforcement learning approach for distributed intrusion detection in big data networks. *Cluster Computing*, 27(5), 6823-6841. https://doi.org/10.1007/s10586-024-04306-9

[23] N, M., G, S. H. K., R, S., & NR, J. I. R. (2024). Federated transfer learning for intrusion detection system in industrial iot 4.0. *Multimedia Tools and Applications*, 83(19), 57913-57941. https://doi.org/10.1007/s11042-024-18379-6.

[24] doost P. A., Moghadam, S. S., Khezri, E., Basem, A., & Trik, M. (2025). A new intrusion detection method using ensemble classification and feature selection. *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-025-98604-w

[25] Karn, A. L., Ghanimi, H. M. A., Iyengar, V., Siddiqui, M. S., Alharbi, M. G., Alroobaea, R., Yousef, A., & Sengan, S. (2025). Applying the defense model to strengthen information security with artificial intelligence in computer networks of the financial services sector. *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-025-15034-4

[26] Sorour, S. E., Aljaafari, M., Shaker, A. M., & Amin, A. E. (2025). LSTM-JSO framework for privacy preserving adaptive intrusion detection in federated IoT networks. *Scientific Reports*, 15(1). https://doi.org/10.1038/s41598-025-95966-z

[27] Xu, S., Shi, Y., Shi, L., & Zhang, H. (2025). Efficient network defense policies via GNN-enhanced reinforcement learning. *The Journal of Supercomputing*, 81(8). https://doi.org/10.1007/s11227-025-07431-3.

[28] Malathy, N., Swvtha, A. T., Leela, T. B., & Raaman, A. (2025). Real-Time Intrusion Detection in IIoT Stream Data Using Window-Based Weighted Ensemble Techniques. *SN Computer Science*, 6(1). https://doi.org/10.1007/s42979-024-03597-4

[29] Zhang, Z., Das, A., Huang, G., & Baskiyar, S. (2025). CAT: A simple heterogeneous ensemble learning framework for network intrusion detection. *Peer-to-Peer Networking and Applications*, 18(4). https://doi.org/10.1007/s12083-025-02000-0

[30] Kantharaju, V., Suresh, H., Niranjanamurthy, M., Ansarullah, S. I., Amin, F., & Alabrah, A. (2024). Machine learning based intrusion detection framework for detecting security attacks in internet of things. *Scientific Reports*, 14(1). https://doi.org/10.1038/s41598-024-81535-3