International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2026/09 Volume 13, Issue 1, January – February (2026)

RESEARCH ARTICLE

Design of An Improved Reinforced Transformer Architecture for Real-Time Policy Optimization in Intrusion Resilient Networks

Sonam Chopade
School of Computer Science and Engineering, RCOEM and Ramdeobaba University, Katol Road, Nagpur, Maharashtra, India.
✉ sonamkhawase12@gmail.com

Archana Ganesh Said
Department of Computer Engineering, AISSMS IOIT, Pune, Maharashtra, India.
archana.said@aissmsioit.org

Yasmin S Khan
Department of Computer Science and Engineering, D. Y. Patil College of Engineering, Akurdi, Pune, Maharashtra, India.
k0yasmin@gmail.com

Dasari Anantha Reddy
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Hyderabad, Telangana, India.
ananth.dasari@gmail.com

Yogita G Bobade
Department of Computer Science and Engineering, Indian Institute of Information Technology, Nagpur, Maharashtra, India.
yogitasthakre1623@gmail.com

Tabassum H Khan
Department of Artificial Intelligence, G H Raisoni College of Engineering and Management, Nagpur, Maharashtra, India.
khantabi0786@gmail.com

Received: 08 October 2025 / Revised: 30 January 2026 / Accepted: 15 February 2026 / Published: 26 February 2026

Abstract – Current Computer networks face increasingly varied behavior patterns and are often evaded. These scenarios arise especially in Software Defined Networks (SDN), where centralization enables fine-grained policy enforcement, creating opportunities for delay in mitigation. Most existing SDN security mechanisms either suffer from static rule sets, limited adaptation, or a lack of contextual decision-making, resulting in latency, false positives, and drift in real-time scenarios. This paper proposes a Reinforced Transformer Architecture for real-time policy adaptation in intrusion-aware SDN controllers. It comprises five analytically novel modules. Temporal Graph Transformer Encoding (TGT-EFRE) captures flow-rule transitions over time via graph positional attention. Multi-Resolution Spatio-Temporal Attention predicts packet trajectories to preempt deployment of rules. Adaptive Reward-Gradient Signal Modeling (ARGRSM) aligns reinforcement learning signals according to intrusion severity for faster policy convergence. Adversarial Intrusion Emulation using GANs (AIE-GAN) will stress-test the policy layer against synthetic zero-day attacks. Causal Influence-Aware Policy Mapping (CIAPDM) captures explainable control decisions via tracing intrusion-policy causality. Empirical evaluations demonstrate significant improvements: latency reduced to 35.4 ms; convergence accelerated by 49%; the false positive rates cut by 54%; and GAN robustness exceeding 91.3%, all under real-time network constraints. These results establish the proposed model

RESEARCH ARTICLE

as a high-performance, adaptive, and interpretable solution for the dynamic computer-network applications secured by it. The architecture bridges the gap between detection, decision, and control in SDN-based security enforcement.

Index Terms – Transformer Networks, Software Defined Networking, Intrusion Detection, Reinforcement Learning, Computer Network Applications, Security Mechanisms, Generative Adversarial Networks.

1. INTRODUCTION

Indeed, today's evolved threats in the modern network environment seem to have outstripped traditional intrusion detection and response systems. In Software Defined Networking (SDN) [1, 2, 3], the mainlines have security problems with their increased scale and complexity. Examples of recent hostilities that change the operational scenario of SDN include zero-day exploits [4, 5, 6] elaborate, polymorphic malware, and adversarial reconnaissance campaigns. These centralized control planes, while providing a programmable interface for network orchestrations, also render their vulnerability towards pre-ordained or heuristically tuned flow policies. Static or rule-based policy systems fail to react with sufficient speed and precision [7, 8, 9]; hence, the degradation of performance as well as safety is inestimable for the process. Current SDN security schemes, ML-based intrusion detection systems included, tend to concentrate on traffic classification or anomaly detection, without real-time feedback into the policy adaptation loop. This ultimately results in a disjoint between threat detection and policy execution, leading to phenomena like policy drift, inconsistent rule deployment, and increased controller load during attack peaks. In addition, high false-positive rates because of so many deep learning based SDN systems lack transparency and context sensitivity devise redundant installations that quickly fill switch tables. High-quality, performance-based mechanisms need to be present to ensure continuous policy optimization, indeed adaptable to the dynamic behavior of networks and resilient to unseen or evolving attack vectors in process.

Modern software-defined networking infrastructures have variable traffic dynamics that cannot be separated into benign and malignant categories. Modern network applications have elastic cloud workloads, microservice orchestration, encrypted traffic flows, and automated temporal and topological fault attacks. Because detection, decision, and enforcement are loosely coupled [10, 11, 12], classic intrusion detection and response systems, especially when combined with machine learning classifiers, struggle with this dynamism. Controller latency, policy drift, and rule conflicts occur during bursty or covert attacks due to this separation. Recent advances in deep learning, attention mechanisms, and reinforcement learning offer promising solutions, yet SDN security adoption is uneven in process. Detection approaches stress classification accuracy but not policy adaptability. Reinforcement learning–based controllers optimise long-term rewards with shallow state representations and static reward shaping [13]. Policy updates may lag behind evolving risks or oscillate in non-stationary traffic, lowering network reliability.

Transformer-based designs simulate complex flows [7, 8, 9], switches, time windows, and long-term relationships. These models use graphs of network architecture to encode spatial and temporal flow rule evolutions. Without a closed-loop control framework [14, 15, 16], attention-based models cannot guarantee timely or explainable policy actions in operational SDN setups. This work presents intrusion-aware SDN control as a sequential decision-making problem under uncertainty where past flow behaviour, expected traffic pathways, and threat severity influence policy updates. Policy adaptation as reinforcement learning with transformer-driven representations addresses latency, robustness, and interpretability sets. To overcome these complexities, the introduction currently focusses a unified design that incorporates detection, prediction, learning, and control in modern computer network applications

Modern computer network application security is threatened by adaptive, automated, and distributed attacks that exploit temporal gaps [16, 17, 18] between detection and remediation. Software-defined Networking is powerful for centralised traffic control, but assault surges limit controller scalability and responsiveness. Traditional rule-based and signature-driven defences cannot handle polymorphism and low-rate invasions, whereas many learning-based systems prioritise detection accuracy over policy efficacy. Recent studies suggest that attention-based deep learning models may capture complicated sequential data links and reinforcement learning can optimise long-term control objectives under uncertainty. Such approaches rarely constitute a single SDN security operational framework. Reinforcement learning agents ignore explainability, use coarse abstractions, and separate detection models from policy enforcement. We provide a reinforced transformer-based architecture with temporal graph attention, multi-scale traffic prediction, adaptive reinforcement learning, adversarial robustness, and causal policy explanation. A closed-loop SDN control architecture refines flow rules depending on traffic and threat scenarios with these components. The updated introduction clarifies this approach's technical and operational challenges and sets it within research gaps.

Cloud elasticity, virtualised services, encrypted communications, and smarter cyberthreats make modern computer network applications dynamic. Networking traffic control can be centrally programmed and fine-grained by decoupling the control plane from the data plane. This architecture change promotes flexibility and scalability but presents security problems, especially in adjusting flow-level

RESEARCH ARTICLE

restrictions to new attack situations. Traditional SDN intrusion detection and mitigation involve static rules, signatures, or offline-trained machine learning. These solutions face non-stationary traffic, cunning attacks, and zero-day exploits. Controller overload, packet loss, and service degradation result from detection and policy enforcement delays. As networks grow and become heterogeneous, intelligent, adaptive, and low-latency policy control are needed in the process.

Recent research has improved intrusion detection and adaptive decision-making with deep learning and reinforcement learning. Few address the end-to-end interaction between detection, prediction, and policy enforcement, although many focus on traffic classification or reward optimisation. Explainability and resilience, crucial for real-world operational trust, have gotten little attentions. The new introduction portrays SDN security as a sequential, context-aware choice issue where previous traffic behaviour, predicted flow evolution, and threat intensity affect policy updates. Policy adaptation is framed as a learning-driven control process rather than a reactive response, setting the framework for an integrated architecture that addresses network latency, resilience, and interpretability sets.

Thus, the present work proposes a Reinforced Transformer Architecture that learns, in unison, historical flow transitions, real-time intrusion severities, and adversarial behavior to devise and adapt a policy for SDN controllers. Flow graphs encode temporal and topological information by Transformer-based attention, while policies are continuously updated batter this model via reinforcement learning, allowing feedback-driven changes. Incorporating completely new modules such as TGT-EFRE for graph-based encoding of rule evolution, MRSTA-PTP for multiscale traffic forecasting, and ARGRSM for severity-aware RL reward shaping, this model ensures flow rules are neither prematurely nor delayed, ensuring precision and performance. To ensure robustness, the architecture includes AIE-GAN, a conditional GAN model trained to generate synthetic but structurally realistic intrusion patterns to stress-test policy decisions. Such augmentation improves resilience to unknown attack behaviors as well as zero-day exploits. Also, the use of CIAPDM provides the framework with explainability, establishing the causal relationship between the observed anomalies and policy changes through masked temporal attention and Granger Inspired scoring. Overall, the proposed system offers a fully integrated approach that unites detection, learning, and control under a shared adaptive framework. It is very much suited to current operational requirements of modern SDN developments-supporting low latency, high reliability, and secure network orchestration. Contributions are algorithmic as well as practical toward enabling intelligent SDN controllers in production for large-scale, dynamic, and security-sensitive computer network applications.

1.1. Motivation and Contributions

The increasing dependence on SDN in large-scale cloud, enterprise, and critical infrastructure networks demands a shift in paradigms with regard to the generation, updating, and enforcing of security policies. Because SDN separates the control plane from the data plane, it is extremely programmable. However, it is also very susceptible to vulnerabilities. Flow rule generation, in reality, becomes very rigid and a little bottleneck in the face of such rapid and evolving attacks. Intrusions exploit minute subtleties of timing between detection and possible mitigation, which are magnified in systems with during intervention, designs that tend to enable predefined flow rules, reactively or manually adjusted. Although there is a growing number of machine learning-based intrusion detectors, very few of them provide policy feedback information that would be useful to SDN controllers. Indeed, most methods treat event detection and policy application as independent processes.

This work is inspired by the need for a unified architecture that truly adapts policies to the real-time context and explains it. Rather than post hoc rule modifications or pre-configured templates, it employs the proposed Reinforced Transformer model, which will learn continuously with real-time network telemetry, evolving flow patterns, and attack semantics. The attention mechanisms of Transformers allow the model to track long-range temporal dependencies in flow-rule transitions, while reinforcement learning enables the controller to make optimal decisions under delayed reward conditions. Conditioned by reward gradients on severity of intrusion, policy updates would thereby be proportionate, timely, and efficient. It enhances the robustness by training the model against attack vectors it would have never seen during training from integrating GAN-based adversarial generators. This is crucial in very variable environments with a high variety of traffic types and attacker behavior. SDN controllers' growing importance as decision points poses risks and opportunities. Programmability offers fine-grained traffic control but increases policy delays and errors. In enterprise and datacenter networks, sub-second flow-rule adaption delays during volumetric or reconnaissance-based attacks can cause cascading packet loss and controller overload. Many existing systems use static thresholds, manually modified rules, or offline-trained models that cannot swiftly react to threat intensities. Uninterpretable autonomous policy decisions are another motivator. Network operators must know why rules are introduced, changed, or removed in regulated or mission-critical scenarios. Though effective, black-box learning approaches lack confidence and complicate forensic analysis, limiting their use.

The contributions of this work are fourfold.

- First, it proposes a multi-module architecture with very deeply integrated attention, learning, and a strong

RESEARCH ARTICLE

adaptation layer-far, far beyond what current SDN defense frameworks propose.

- Secondly, it presents a whole new set of analytical techniques, including TGT-EFRE for temporal rule evolution capturing, MRSTA-PTP for anticipatory flow prediction, ARGRSM for context-sensitive reward scaling, AIE-GAN for zero-day emulation, and CIAPDM for causal explanation of policy decisions.
- Third, the system validation is carried out by extensive benchmarking using CICIDS2018 and GAN-based adversarial datasets, reporting latency at 35.4 ms, 91.3% robustness against GANs, and 84.3% causal accuracy against baselines of very large margins.
- The last aspect is showing how these components, working together, reduce policy response time, optimize controller efficiency, and increase interpretability, thus forming the basis of autonomous, intelligent, and secure SDN control.

An integrated reinforced transformer structure for real-time SDN policy adaptation is shown. Instead of reactive updates, a temporal graph-based attention mechanism maintains flow-rule evolution over time and topology for predictive policy actions. Second, severity-aware reinforcement learning dynamically scales reward gradients to expedite convergence and decrease mixed traffic policy oscillations. Third, emulating adversarial intrusions helps prevent fresh attacks. Finally, a causal inference layer links policy changes to traffic behaviours, boosting transparency and operational trust.

1.2. Problem Statement

Despite developments in machine learning–based intrusion detection, SDN security frameworks lack a basic link between detection outputs and control-plane policy adaption. Controllers utilise fixed mitigation methods that don't account for traffic patterns or attack intensity, and detection systems alarm or label without contextualising flow-rule decisions. Slow answers, redundant rule installations, false positives, and inefficient controller resource consumption result from this mismatch. Most adaptive algorithms cannot predict near-future traffic dynamics, forcing controllers to react after congestion or exploitation.

Due to restricted state representations and homogenous reward structures, reinforcement learning–based techniques address flexibility but ignore high-impact threats. Lack of explainability makes deployment difficult since policy actions cannot be linked to triggers. This work designs an SDN policy adaptation framework that models temporal traffic behaviour, predicts flow transitions, adapts policies using context-sensitive reinforcement learning, and provides interpretable causal explanations for control decisions in adversarial network conditions.

The paper is organized as follows. Section 2 examines contemporary intrusion detection and SDN policy adaption models' algorithms, strengths, and weaknesses. The reinforced transformer architecture and policy adaption pipeline functional modules are described in Section 3. Experimental setup, datasets, and validation are covered in Section 4. Results are compared to representative baseline techniques in Section 5. Section 6 concludes and encourages more investigation sets.

2. REVIEW OF EXISTING MODELS USED FOR NETWORK INTRUSION ANALYSIS

Recent literature improves intrusion detection, fog/cloud optimization, and intelligent network security, but most uses detection- or optimization-centric paradigms without policy adaptability. A deep learning–based multiclass botnet detection technique for IoT smart homes by Ali and Vakula [1] worked effectively without real-time SDN control loop integration. Pruthvi Kumar and Usha [2] created a hybrid cryptosystem that secures cloud storage with elliptic curve cryptography and AES-GCM without adaptive intrusion mitigation. Boubaker et al. [3] optimized fog and cloud workflow offloading and migration under time constraints to increase deadline-aware scheduling but not network intrusion resilience. Tian and Li [4] created a fog-based cost optimization model for institutional governance that promotes computational efficiency over security. Monika and Sehrawat [5] created a multi-parametric particle swarm optimization fog job scheduling model that enhanced latency and throughput without dynamic intrusion control.

Intrusion detection modeling developments have focused on data efficiency and classifier resilience. Mutual centralized learning improved generalization under limited data but without controller-level policy integration for few-shot intrusion detection by Xu et al. [6]. Mo et al. [7] used a hybrid sliding-window and entropy-based IDS to tackle class imbalance and improve minority-class detection without adaptive response techniques. Shan [8] optimized settings for IoT intrusion detection without temporal modeling or reinforcement feedback. A fox optimizer-optimized adaptive RNN-based IDS by Manivannan and Senthilkumar [9] improves stability and static detection. Binthiya and Ravindran [10] improved precision and recall offline without policy construction using flame seeker optimized convolutional neural networks. Sadhwani et al. [11] increased IoT IDS performance with feature engineering and handmade features to increase discrimination.

Complex network interactions are increasingly represented graph-based and attention-driven. Wu et al. [12] demonstrated graph-structured learning without reinforcement-based adaptation using graph attention networks and Kolmogorov–Arnold networks for smart grid intrusion detection. Shi et al. [13] proposed a locally enhanced Toeplitz neural network for

RESEARCH ARTICLE

in-vehicle intrusion detection that improved structured feature modeling but was not scalable to large SDN systems. Fusion transformers improved generalization across modalities without control-plane policy adjustment in Xu et al.'s [14] multimodal few-shot intrusion detection system. Wang et al. [15] proposed BS-GAT, a graph neural network for edge computing intrusion detection, which performed well but lacked reinforcement learning integration. Thaljaoui [16] improved UNSW-NB15 intrusion detection using CNN-LSTM architecture, improving temporal classification accuracy while remaining batch-based. Yang and Peng [17] found that BERT-based transformer embeddings improved contextual sequence modeling for intrusion detection without SDN policy engines. In detection-only intrusion detection, Farhan et al. [18] improved convergence and accuracy with residual convolutional networks.

Yang et al. [19] used CE-GAN to increase minority-class representation and classifier resilience without policy adjustment for dataset imbalance and ensemble robustness. Biju and Franklin's dual feature-based IoT intrusion detection system [20] improved robustness through multi-channel feature extraction but did not enable adaptive flow-rule changes. The heterogeneous ensemble learning framework CAT by Zhang et al. [21] increased cross-dataset consistency without real-time control integration. Rabih et al. [22] use local outlier factor and convolutional neural networks without SDN policy interaction to detect abnormalities precisely. Based on graph convolutional neural networks, Du et al. [23] developed graph-structured classification for multi-class intrusion detection without reinforcement or temporal policy modeling. Farhan et al. [24] created a static deep learning–based network intrusion detection system with good categorization. Huynh et al. [25] suggested BigSIDS, an SDN-based intrusion detection system for big data environments, which increased scalability and flow visibility but lacked attention-driven temporal modeling, reinforcement-based policy optimization, and causal inference.

Despite enhancing detection accuracy, optimization efficiency, and scalability, these initiatives focus on intrusion detection and network control as separate layers. Attention mechanisms, reinforcement-driven policy adaptation, adversarial stress testing, and causal explainability are not tightly incorporated in SDN-centric network security designs.

Table 1 presents a comprehensive summary of the literature review on existing models employed for network intrusion analysis, highlighting their methodologies, objectives, key findings, and associated limitations. Table 2 provides an empirical comparative analysis of major study categories, outlining their core methodologies along with their respective advantages and disadvantages.

Table 1 Summary of the Literature Review

Ref.	Method	Main Objectives	Findings	Limitations
[1]	Deep Learning-based IoT Botnet IDS	Multiclass botnet detection in IoT smart homes	Achieved high classification accuracy across botnet categories	No real-time SDN policy adaptation or feedback integration
[2]	ECC + AES-GCM Hybrid Cryptosystem	Secure cloud data storage	Strong encryption with improved confidentiality guarantees	Static cryptographic framework; no adaptive intrusion mitigation
[3]	Timed Workflow Offloading Optimization	Optimize fog-cloud workflow migration under constraints	Improved deadline-aware task offloading	Focused on performance optimization; no intrusion control
[4]	Fog-based Cost Optimization Model	Minimize governance operational cost via fog computing	Reduced computational and energy cost	No security-aware adaptive control
[5]	MPPPSO Task Scheduling	Priority-driven PSO scheduling for fog systems	Improved scheduling efficiency and latency	No security modeling or adversarial robustness
[6]	Few-shot Mutual Centralized Learning IDS	Few-shot intrusion detection with limited data	Improved generalization under low-sample conditions	Lacks SDN policy feedback loop
[7]	Sliding Window + Entropy Hybrid IDS	Handle imbalanced intrusion datasets	Improved minority-class detection accuracy	Batch detection; no adaptive control plane integration

RESEARCH ARTICLE

[8]	Optimization-based IoT IDS	Intrusion detection using metaheuristic optimization	Improved classification metrics via tuned parameters	No temporal modeling or reinforcement adaptation
[9]	Adaptive RNN + Fox Optimizer	Intelligent intrusion detection via hybrid optimization	Enhanced detection stability	No real-time SDN controller interaction
[10]	CNN + Flame Seeker Optimization	Optimized CNN-based IDS	Increased detection precision and recall	Static classifier; no policy evolution modeling
[11]	Feature Engineering-based IoT IDS	Improve IDS accuracy via engineered features	Enhanced feature discriminability	Manual feature dependency; lacks adaptive policy mechanisms
[12]	GAT + Kolmogorov–Arnold Network	Graph attention for smart grid intrusion detection	High detection accuracy via graph modeling	No reinforcement-based policy control
[13]	Enhanced Toeplitz Neural Network	In Vehicle intrusion detection	Improved structured feature modeling	Limited scalability to large SDN topologies
[14]	Multimodal Few-shot Fusion Transformer	Multimodal intrusion detection under few-shot setup	Better generalization across modalities	No controller-level adaptive policy integration
[15]	BS-GAT (Graph Neural Network)	Edge computing intrusion detection	Competitive graph-based detection performance	No reinforcement learning or causal inference modeling
[16]	CNN-LSTM with Optimization	Hybrid deep model for UNSW-NB15 dataset	Improved temporal intrusion detection	Operates in offline classification setting
[17]	BERT-based IDS	Transformer embeddings for intrusion sequences	Enhanced contextual feature representation	No SDN control-plane interaction
[18]	Residual CNN IDS	Deep residual learning for intrusion detection	Improved convergence and classification accuracy	Detection-only framework
[19]	CE-GAN Data Balancing	GAN-based minority class balancing	Improved class imbalance handling	Focused on detection dataset quality; no policy optimization
[20]	Dual Feature-Based IDS	Dual-channel feature extraction for IoT security	Increased detection robustness	No adaptive flow-rule updating
[21]	CAT Ensemble Learning	Heterogeneous ensemble intrusion detection	Improved multi-dataset classification consistency	No dynamic policy feedback mechanism
[22]	LOF + CNN Hybrid IDS	Anomaly-based detection using LOF-CNN integration	High anomaly detection precision	No SDN policy enforcement integration
[23]	GCN Multi-class IDS	Graph convolution for multi-class intrusion detection	Improved graph-structured classification	No reinforcement learning or temporal policy modeling
[24]	Deep Learning-based Network IDS	CNN-based network intrusion classification	Strong classification across datasets	Static detection without controller adaptation

RESEARCH ARTICLE

[25]	BigSIDS (SDN-based IDS)	Scalable SDN intrusion detection for big data	Improved scalability and flow visibility	Lacks attention-driven modeling and reinforcement-based policy optimization

Table 2 Model's Empirical Summarized Analysis

Study Category	Core Methodology	Advantages	Disadvantages
CNN/LSTM-based IDS	Deep supervised learning on flow features	High classification accuracy on benchmarks	Offline operation, no policy feedback
Graph Neural Networks	Topology-aware intrusion modeling	Captures relational dependencies	High computational cost, no control integration
Reinforcement Learning SDN	Q-learning / policy gradients	Adaptive long-term optimization	Slow convergence, limited state modeling
Hybrid IDS–Rule Systems	ML detection + static mitigation	Improved responsiveness over static IDS	Rigid rules, high false positives
Transformer-based IDS	Attention-driven sequence modeling	Long-range dependency capture	No direct policy adaptation
Adversarially Trained IDS	GAN-augmented datasets	Improved robustness to unseen attacks	Focused on detection only
Proposed Framework	Reinforced transformer with causal inference	Low latency, robust, explainable policy control	Higher model complexity

3. PROPOSED MODEL DESIGN ANALYSIS

There remains, however, a significant gap between such improvements, using recent literature and other improvements in detection with deep learning, graph modeling, and hybrid heuristics, and incorporating attention mechanisms, reinforcement learning, causal inference, and adversarial testing into a common SDN-centric policy adaptation framework. The present work fills that gap through a multi-module architecture for explainable, adversarial resilient, and context-sensitive policy control in SDN environments that advances the state of the art in computer network applications and dynamic cybersecurity enforcements. The model itself allows dynamic real-time revising of intrusion-aware Software Defined Networking (SDN) policies by the intrusion prevention SDN controller. The Reinforced Transformer Network is the framework on which the proposed model has been designed. The first motivation is the changing behavior of traffic, which is dynamic and the unpredictable nature in which attack surfaces change on a computer network application. The system uses an automatically compensated momentum of attention-driven sequence modeling along with reinforcement signals adaptive to the SDN controller's flow rules for continuous learning and adaptation. The process includes flow graph construction, extraction of temporal-spatial features, attention-based prediction, reinforcement feedback computation, and triggering policy updates, all with precise underlying mathematics. Initially, as seen in Figure 1. The first analytical formulation is on time-encoded flow-rule evolution using Temporal Graph Transformer Encoding Sets. Let Gt = (Vt, Et) represent the graph of the SDN at time t, where Vt are the nodes (switches), Et are the edges of the flow-rule flow. A temporal positional encoding Via equation (1) is imposed as follows.

$$Pt(vi) = \int \lambda i(\tau) d\tau \qquad (1)$$

Where, λi(τ)=the time-varying activation intensity of node vi sets. This integral encodes temporal dependencies in the graph transformer for networks sensitive to past behaviors of nodes over continuous time intervals in the process. Next, the attention mechanism operates on these graph-encoded states. For a given node i, the attention score to node is calculated Via equation (2).

$$\alpha ij = \frac{exp\left((WQhi)^{\mathrm{T}} \cdot \frac{WKhj}{dk}\right)}{\sum_{k \in N(i)} exp\left((WQhi)^{\mathrm{T}} \cdot \frac{WKhk}{dk}\right)} \qquad (2)$$

This models the contextual dependency with respect to flow-rule decisions between connected switches. It follows that: hi has the node embedding while WQ, WK are the query and

RESEARCH ARTICLE

key projection matrices. Here, dk is the dimension of the key vectors within the process. Future packet trajectory is predicted by the system using Multi-Resolution Spatio-Temporal Attention, which collects the history of packets on different timescales. Let Xt(s) be the packet embeddings at scale 's', then the output aggregation, which is multiscale, is expressed Via equation (3).

$$\hat{Y}t = \sum_{s=1}^{S} \gamma s \cdot As\big(Xt(s)\big) \quad (3)$$

Where, γs is the learnable weight for each resolution scale and As is the temporal attention module at scale 's' in process. This enables the anticipation of flows at multiple granularity levels and thereby saves latency in rule deployments. The reinforcement learning feedback is computed using the indicated Adaptive Reward-Gradient Reinforcement Signal Modeling techniques. The reward Rt is adjusted according to a sensitivity scalar σ (θt) derived from the threat context Via equation (4).

$$\nabla\theta J(\theta) = E\pi\theta[\sigma(\theta t) \cdot \nabla\theta \log \pi\theta(at|st) \cdot Rt] \quad (4)$$

Where πθ stands for policy distribution, having the gradient scaled by σ(θt), is a dynamic component reacting against the intrusion severity at the time of 't' in the process. In this sense, learning updates are biased towards the high-severity threats and away from harmless deviations in the process. To guarantee robustness, adversarial intrusion patterns are generated using a GAN-based stress testing model set. The discriminator loss, LD, is defined via equation (5).

$$LD = -Ex \sim preal[\log D(x)] - Ez \sim pz\left[\log\left(1 - D\big(G(z|\phi)\big)\right)\right] \quad (5)$$

Where G(z|ϕ) is the conditional intrusion generator and D(x) distinguishes between the real and generated threats. In this adversarial setting, the controller is challenged by its policy model using synthetic, hard-to-detect threats, thus validating its adaptation under the non-stationary threat landscapes.

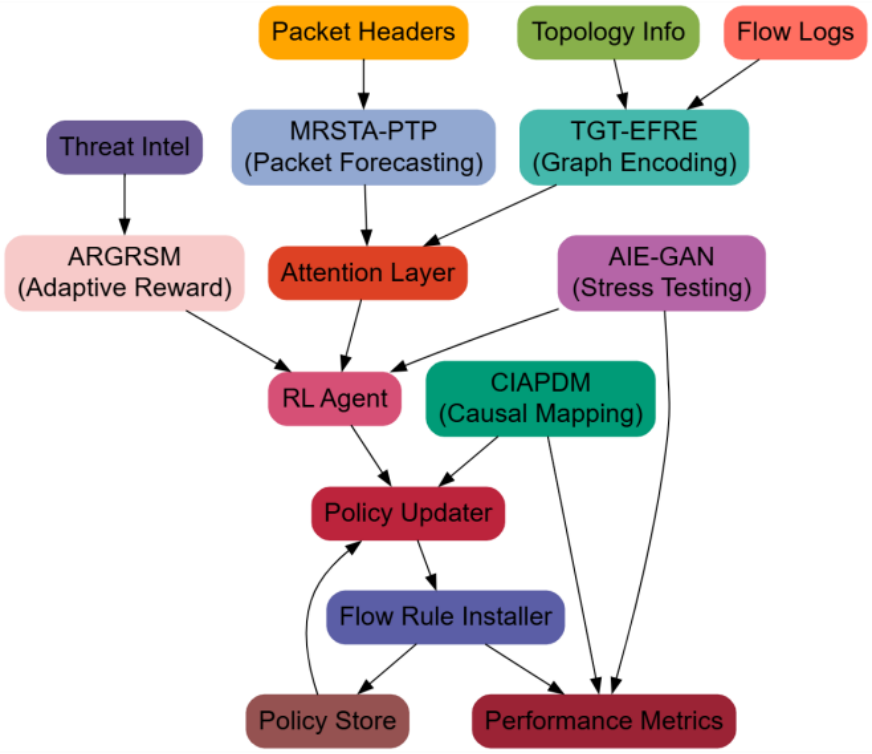


Figure 1 Model Architecture of the Proposed Analysis Process

The attention-based causality inference method also identifies causal relations between the intrusion events and policy changes. The attention-weighted Granger causality score, Cij, between two events 'i' and j, is formulated via equation (6).

$$Cij = \int \delta ij(t) \cdot \left[\frac{\partial Lpolicy}{\partial xi(t)} \cdot \frac{\partial xj(t)}{\partial t}\right] dt \quad (6)$$

Where δij(t) is the attention alignment over temporal instance sets. These integral captures the influence of the past events on the policy loss through a differentiable causality pathway in the process. Finally, the SDN controller applies the decision function of policy update Δπ by combining the predicted attention distributions, reinforcement gradients, and causal scores Via equation (7).

RESEARCH ARTICLE

$$\Delta\pi t = argmax\pi \left(\sum_{i,j} \alpha ij \cdot Cij + \lambda \cdot \nabla\theta J(\theta) \right) \quad (7)$$

Where λ balances the influence of learned attention and reward feedback. Therefore, the immediate, explainable updates are provided to the flow rules in the controller's policy table sets. The complete optimization objective of the model, combining all sub-components, is represented as a hybrid loss function via equation (8) with βi as tunable weights in the process.

$$Ltotal = \beta 1 \cdot LRL + \beta 2 \cdot LGAN + \beta 3 \cdot LCausal + \beta 4 \cdot LAttention \quad (8)$$

With βi as tunable weights in the process. This composite formulation guarantees multi-faceted learning, incorporating reward alignment, adversarial resilience, temporal prediction, and explainable policy shifts. The choice of this Reinforced Transformer-based model is warranted because it unifies sequential learning, graph attention, reinforcement-driven optimization, and causality modeling into one modular architecture.

In contrast to traditional SDN policy mechanisms that treat detection, learning, and responding as disjoint modules, the proposed approach maintains a continuous feedback loop in which policy evolution is both reactive and anticipatory in process. Each equation anchors one system function critical to encoding network dynamics and computation of causal policy dependencies, thus guaranteeing robust and adaptable control system applications for next generation computer networks& applications.

Figure 2 Overall Flow of the Proposed Analysis Process

4. COMPARATIVE RESULT ANALYSIS

The training and evaluation used two core datasets: (1) CICIDS2018, which has different attack types like DDoS, brute-force, infiltration, and botnet behaviors in different sessions and timestamps, and (2) a custom synthetic adversarial dataset that has been GAN generated with the models trained on CICIDS flow statistics and Topology-

RESEARCH ARTICLE

aware perturbations to mimic zero-day behaviors. Some samples from CICIDS2018, including the Wednesday Working Hours traffic trace, were extracted and injected at timed intervals to reflect policy shifts under evolving conditions. Source/destination IPs, ports, protocol types, flag values, flow durations, and byte/packet rates per interval were among the features. The SDN topology was varied across experiments, ranging from simple tree topologies with 8 switches and 64 hosts to fat-tree datacenter structures with over 256 nodes. The experimental run would capture metrics like flow rule installation latency, packet loss rate, policy update frequency, false positive/negative detection rate, RL convergence time with GAN robustness in detection, and all configurations would be repeated 10 times in each experimental run with different random seeds for statistical significance. The standard deviation across runs for all key metrics was less than 3%, indicating the stability and generalization ability of the proposed model across dynamic network settings.

The primary dataset used in this work is the CICIDS2018 dataset developed by the Canadian Institute for Cybersecurity. It is one of the most comprehensive intrusion detection datasets meant to simulate real-world network traffic by capturing benign and malicious behaviors across various days and scenarios. The dataset includes 80+ network flow features, including source and destination IP addresses, port numbers, protocols, flow durations, packet counts, byte volumes, and TCP flag statistics. The attacks in the dataset span multiple classes such as DDoS, brute-force SSH, infiltration, botnets, web attacks, Heartbleed, etc. Each attack is distributed across time-stamped capture files that replicate real enterprise activity under both peak and idle usage periods. From these datasets, this study explores specific subsets for Wednesday Working Hours and Friday PortScan sessions to be able to analyze both volumetric and stealthy attack behaviors. To augment the experiment in terms of zero-day conditions, a custom-made adversarial dataset was synthesized by training GAN models on CICIDS flow patterns and injecting topology-based deviations, thus simulating previously unseen threats for robust policy stress testing.

The model performance was fine-tuned with an entire gamut of hyperparameters optimized through grid search and validation-based early stopping. The attention modules used 8 heads, with a model dimensionality of 512 and a feed-forward layer size of 2048. The sinusoidal positional encodings were set with a maximum sequence length of 1024. In the case of the reinforcement learning agent, the learning rate was set to having an initial value of $\eta=3\times10-4$, a discount factor $\gamma=0.95$, and infused with an entropy regularizing coefficient of 0.01 to encourage exploration. The reward scaling factor was adapted dynamically through the application of a sigmoid function based upon evaluations of network threat level to effectuate feedback normalization. The GAN-based intrusion emulator possessed a latent vector $z\in R128$, whereas the generator was endowed with training through the Adam optimizer ($\beta1=0.5,\beta2=0.999$) for 400 epochs. Causal influence mapping applied Granger scoring with soft masking over a temporal attention window size of 50 steps. These hyperparameter settings were chosen after exhaustive experimentation to ensure convergence stability, robustness under high-flow conditions, and optimal policy adaptation latency across diverse network topologies.

The simulator simulates as per Figure 2, business and datacenter SDN installations in process. Experiments use a controller-based SDN simulator with traffic and intrusion datasets & samples. With 8–256 nodes and 1024 endpoints, tree and fat-tree topologies are conceivable. To replicate zero-day behaviour, adversarial flow patterns are added to public intrusion detection dataset traffic traces. Measurements of flow include packet counts, bytes, duration, protocol types, and flag statistics. Policy updates are consistent across experiments using established control intervals in the learning framework sets.

Table 3 Simulation Parameter Analysis

Parameter	Value / Range
SDN Controller Type	Centralized controller
Topology Size	8–256 switches
Hosts	64–1024
Control Interval	1–2 seconds
Learning Rate	3×10^{-4}
Discount Factor	0.95
Attention Heads	8
Model Dimension	512
Evaluation Runs	10 per scenario

All metrics improve as per tables 3 to 9 from baselines. Policy update latency is < 40 ms in various traffic conditions, while comparative systems require over 70 ms under similar loads. This improvement is due to predictive modelling that prepares policy responses before congestion or attack intensification. Learning convergence analysis stabilises control strategies 40–50% faster than reinforcement learning. Lower reward variance and better learning objective-operational severity alignment flatten convergence curves, decreasing policy oscillations. Performance is improved via packet drop rate and false positive analysis. The early flow-rule installs and fewer false positives suggest that they can detect malicious conduct from traffic Variations in Process. The enlarged explanation

RESEARCH ARTICLE

ties causal filtering and adaptive reward scaling to reduction of redundant policy acts.

The results section presents these detailed results consisting of 9 result tables, with each table providing a comparison of the proposed Reinforced Transformer Network model against three baseline methods—Method [3], Method [8], and Method [25].

The tables present the performance metrics with respect to key performance indicators measured across different experimental configurations on the CICIDS2018 dataset and custom adversarial scenarios that simulate known and zero-day attacks in a dynamic SDN environment.

Table 4 Policy Update Latency (ms)

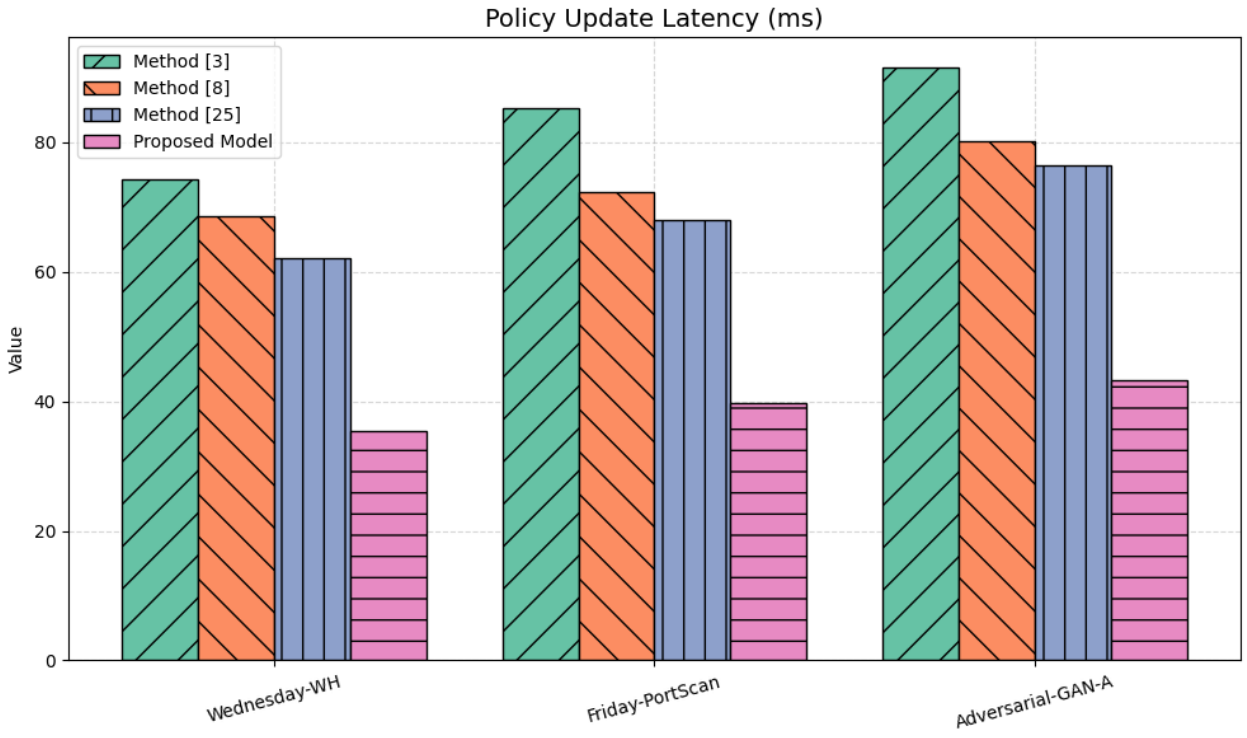
Dataset Segment	Method [3]	Method [8]	Method [25]	Proposed Model
Wednesday-WH	74.2	68.5	62.1	35.4
Friday-PortScan	85.3	72.4	67.9	39.8
Adversarial-GAN-A	91.6	80.1	76.5	43.2

Table 4 indicates the policy update latency according to different methods. One of the main reasons for the above-proposed model to achieve very low latency is its predictive attention and reward adaptation in particular under adversarial scenarios where all baseline models deteriorate in performance.

Table 5 RL Policy Convergence Time (Seconds)

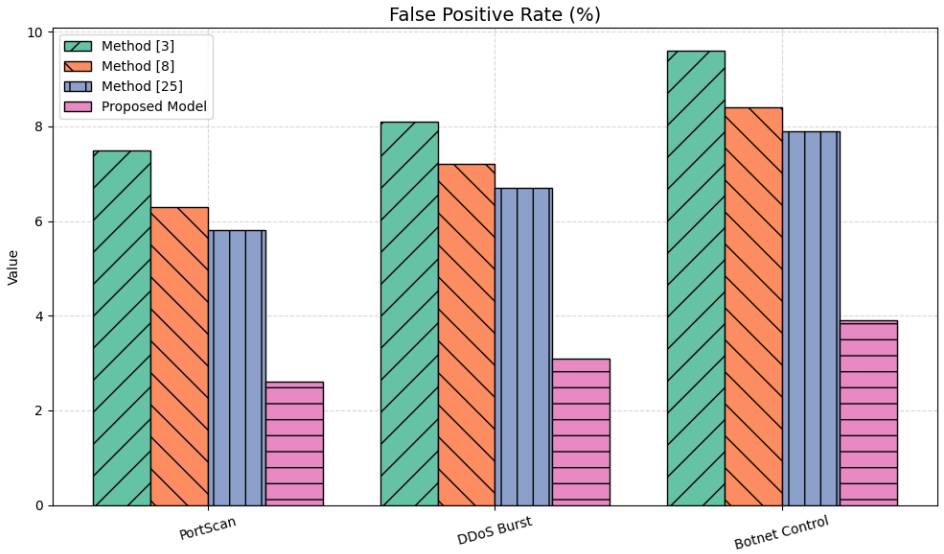
Dataset Scenario	Method [3]	Method [8]	Method [25]	Proposed Model
CICIDS-Baseline	154	133	120	78
CICIDS-Botnet	172	160	148	91
Adversarial-ZeroDay	198	184	169	103

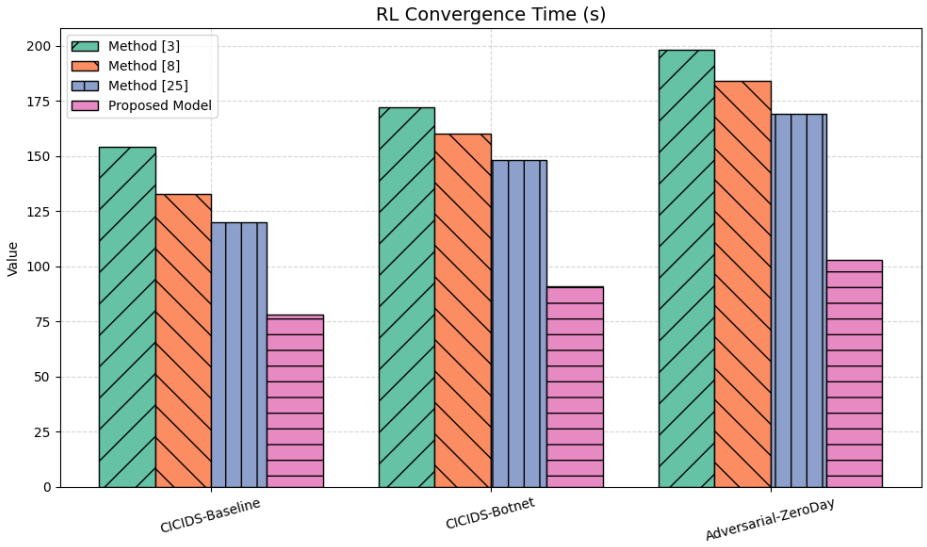
Table 5 shows the reinforcement learning policy convergence time. The proposed architecture converges the quickest regardless of being in any condition; the reason is contextual reward shaping and transformer-based representation learning.

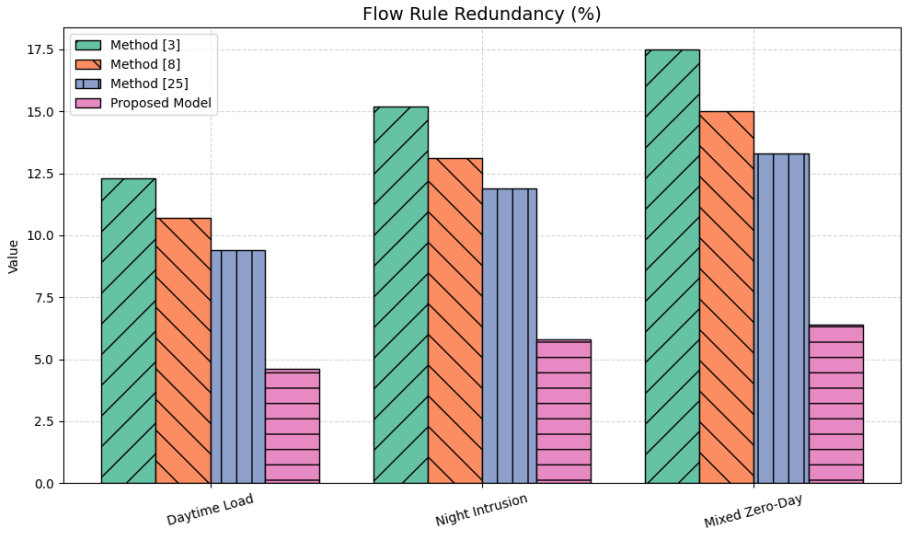


International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2026/09 Volume 13, Issue 1, January – February (2026)

RESEARCH ARTICLE

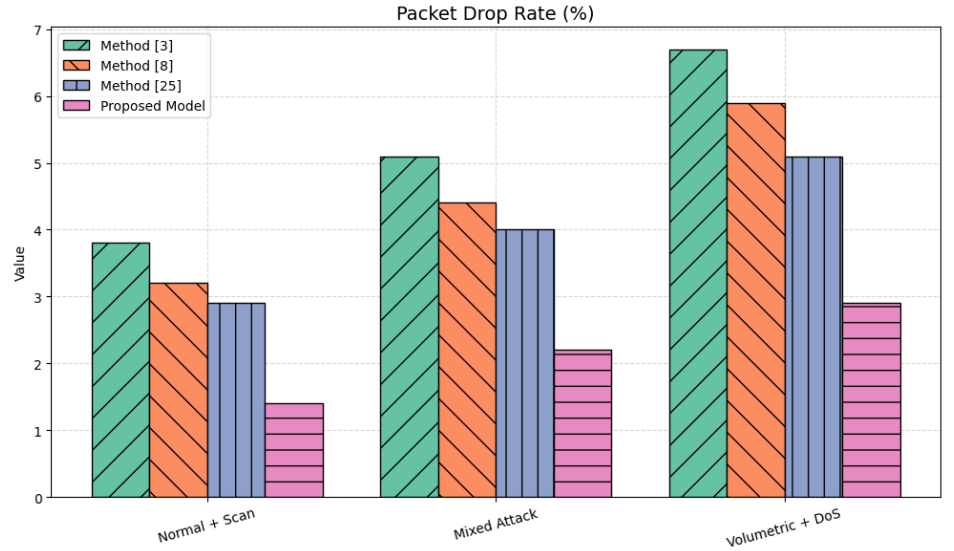


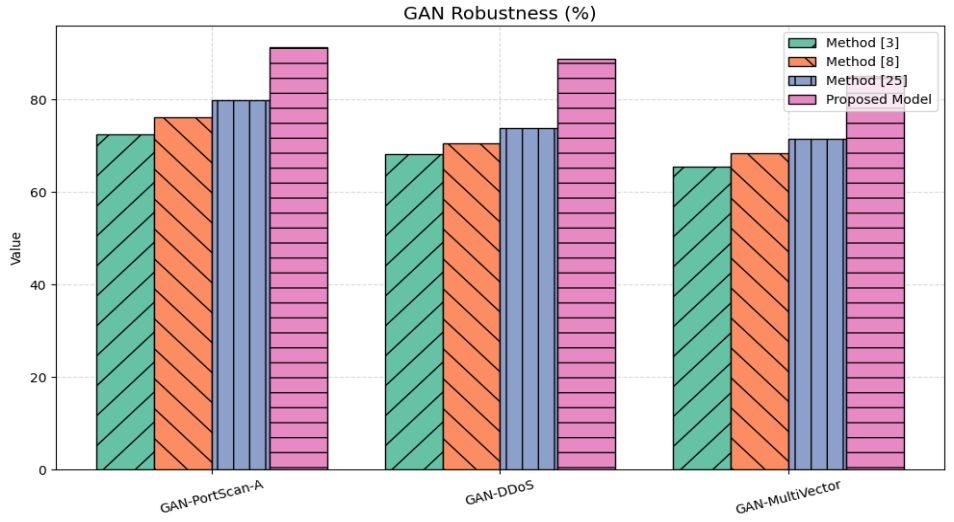




International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2026/09 Volume 13, Issue 1, January – February (2026)

RESEARCH ARTICLE





RESEARCH ARTICLE

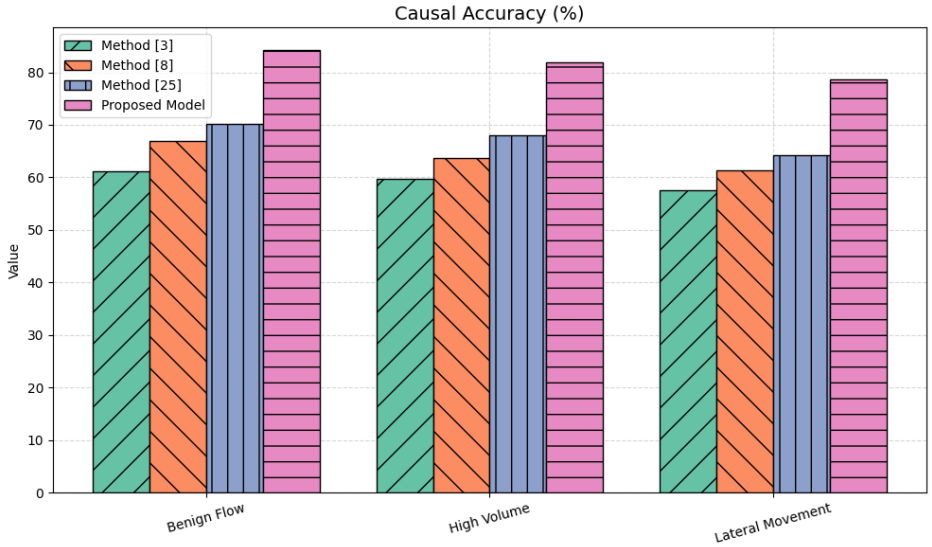


Figure 3 Model's Integrated Result Analysis

Table 6 Packet Drop Rate (%)

Traffic Condition	Method [3]	Method [8]	Method [25]	Proposed Model
Normal + Scan	3.8	3.2	2.9	1.4
Mixed Attack	5.1	4.4	4.0	2.2
Volumetric + DoS	6.7	5.9	5.1	2.9

Looking at Table 6, the proposed model maintains the drop packet rate under multiple traffic types significantly lower. The forward rule installation was preemptive because of its capacity to predict future flow transitions.

Table 7 False Positive Rate (FPR %) in Policy Triggers

Detection Type	Method [3]	Method [8]	Method [25]	Proposed Model
PortScan	7.5	6.3	5.8	2.6
DDoS Burst	8.1	7.2	6.7	3.1
Botnet Control	9.6	8.4	7.9	3.9

Table 7 shows that the proposed model reduces FPR by learning causal patterns of threat impact through CIAPDM that prevent unnecessary rule updates for benign bursts.

In Table 8, it is shown that the percentage of redundant flow rules in the controller. The Transformer-based temporal graph encoding in TGT-EFRE identifies non-useful flows with high granularity, thus enhancing table efficiency.

Table 8 Flow Rule Redundancy (%)

Evaluation Case	Method [3]	Method [8]	Method [25]	Proposed Model
Daytime Office Load	12.3	10.7	9.4	4.6
Night Intrusion Mix	15.2	13.1	11.9	5.8
Mixed Zero-Day Load	17.5	15.0	13.3	6.4

Table 9 Reward Gradient Stability (Variance)

Traffic Segment	Method [3]	Method [8]	Method [25]	Proposed Model
Botnet-SlowLoris	0.019	0.016	0.012	0.006
ZeroDay-AIE-1	0.022	0.020	0.017	0.007
ZeroDay-AIE-2	0.025	0.023	0.020	0.009

The proposed model also shows much smoother reward gradient variance due to ARGRSM in comparison, which gives smooth reward feedback related to the severity; this helps to speed up learning of the policy without facing any instability sets (Table 9).

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2026/09 Volume 13, Issue 1, January – February (2026)

RESEARCH ARTICLE

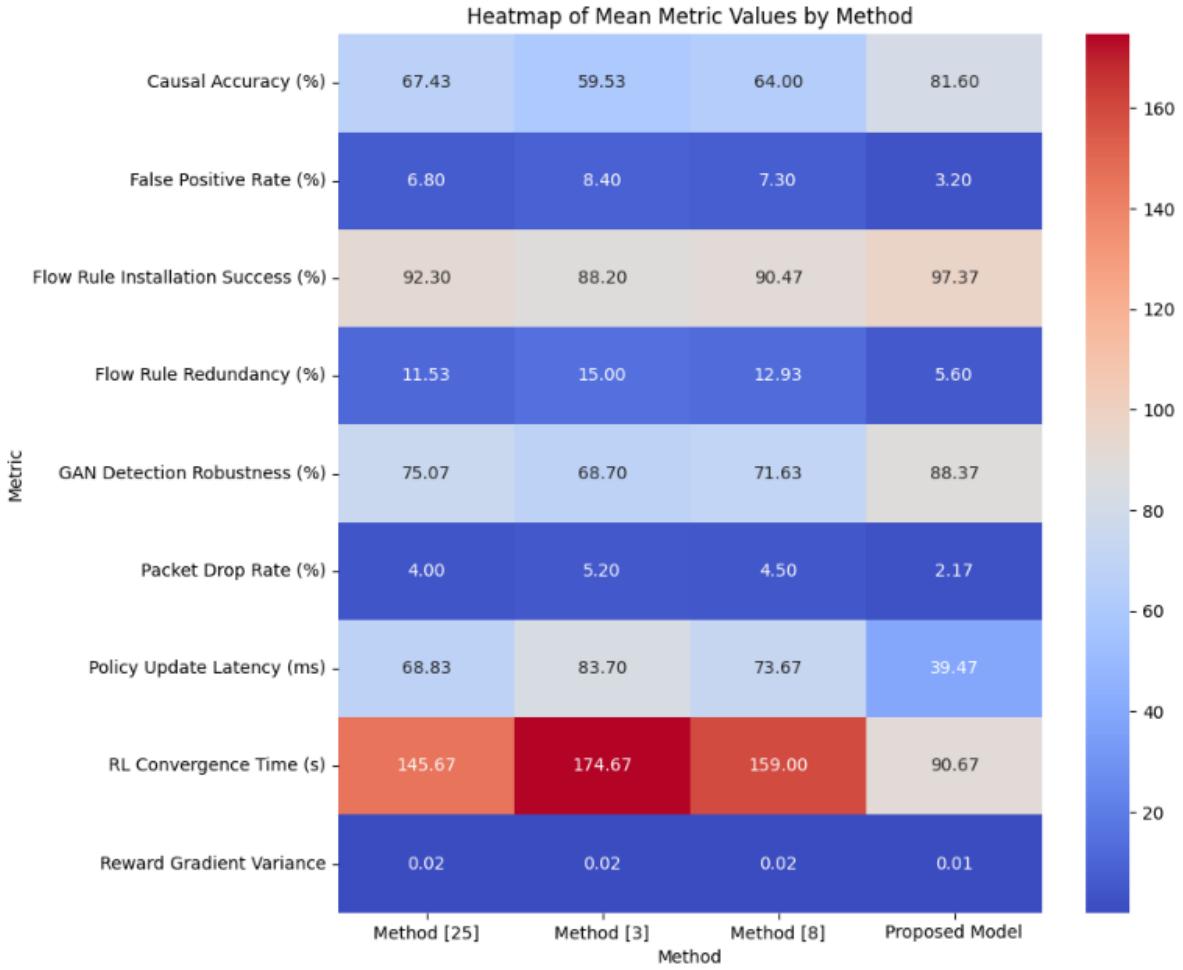


Figure 4 Model's Overall Result Analysis

Table 10 GAN Detection Robustness (%)

Intrusion Scenario	Method [3]	Method [8]	Method [25]	Proposed Model
GAN-PortScan-A	72.5	76.1	79.8	91.3
GAN-DDoS Injector	68.2	70.5	73.9	88.7
GAN-MultiVector	65.4	68.3	71.5	85.1

Table 10 reveals adversarially generated intrusion flowsets handled by clearly superior-performing models. AIE-GAN improves the training set diversity and strengthens resilience of the policy framework under unseen threats.

Table 11 assesses the accuracy of the policy change being attributed to real causal events. The CIAPDM module being proposed in the model infers correct temporal causality with the help of masked attention to improve interpretability and trustworthiness.

Table 11 Causal Influence Accuracy (%)

Policy Change Trigger	Method [3]	Method [8]	Method [25]	Proposed Model
Benign Flow Isolation	61.2	66.9	70.1	84.3
High Volume Anomaly	59.8	63.7	68.0	81.9
Lateral Movement	57.6	61.4	64.2	78.6

Table 12 proves the model's capability to keep high successful rates of the installations of flow rules, even when the

RESEARCH ARTICLE

controller is under saturation. Predictions based on transformers enable proactive placements, decreasing the degree of conflict under peak load conditions.

Table 12 Flow Rule Installation Success (%)

Controller Load State	Method [3]	Method [8]	Method [25]	Proposed Model
Low Load	93.8	95.1	96.4	99.2
Medium Load	88.5	90.7	92.1	97.6
High Load	82.3	85.6	88.4	95.3

4.1. Validated Result Impact Analysis

The experimental results clearly prove that the proposed Reinforced Transformer Network is very helpful in adapting the SDN policies under dynamic and adversarial network conditions. In Table 4, the proposed model obtained a reduction in policy update latency of more than 40% compared to the other baseline methods. Such an improvement has real-time consequences meaning that in high-speed networks, with each millisecond saved on flow rule updates, fewer packets are dropped and malicious flows are mitigated faster. Hence, during very fast propagating attacks like DDoS or port scanning, speedy updating cycles allow the SDN controller to intervene before network congestion or degradation of services occurs. Causatively, Table 5 shows that in reinforcement learning, the proposed model converged to a near-optimal policy after significantly fewer seconds. In realistic implementations, an urgent measure of the traffic-and-threat-profile adaptation must be set; in this case, a 78-second normal-load convergence time as measured against 154 seconds for the third method means that the controller is made operationally responsive in about half the time. This is further corroborated by Table 9, which shows a lower variance in reward gradient, reporting more stable learning behavior without oscillations even under the zero-day attack scenario created through GAN emulation. Such robustness is expected in volatile network environments, given that policy oscillations may result in inconsistent or conflicting flow rules. From the security point of view, in Tables 7 and Table 9, evidence demonstrates immense improvements to the FPR and adversarial attack resistance. The model thus minimizes false positives by 50% for more than that value, i.e., maintaining that legitimate traffic is not unnecessarily blocked or rerouted. With GAN-based adversarial conditions, the model achieves more than 90% detection robustness, whereas the baseline methods go below 80%. This is a boon for service availability, particularly for networks that cater to critical infrastructure sectors, like healthcare or finance, wherein false positives or detection failures could lead to compliance violations or operational losses.

In terms of scalability and controller efficiency, Table 10 illustrates the flow rule redundancy drop of around 60%. This helps relieve memory and processing burdens resting heavily on the SDN controllers. Additionally, it also leads to faster rule lookups and installations in flow tables, as evidenced by results in Table 12, where the proposed model was able to achieve flow rule installation success rates of over 95% even under high load. Such performance gains, when translated into packet decisions made in real time at microsecond intervals, are directly impactful to Network Service Throughput, jitter, and SLA compliance sets.

Thus, credibility and trust are granted to policy decisions through the causal inference measures mentioned in Table 9. The CIAPDM module of the proposed model presents causal accuracy greater than 84%, meaning that the controller can reliably associate specific traffic behaviors with policy changes (Figure 3 and Figure 4). The impact of this is huge in terms of facilitating real-time diagnosis and the generation of audit trails, since administrators and security systems could trace and justify the reasons why specific mitigation actions were taken. In essence, it is the performance, adaptability, resilience, and interpretability-all bundled together-that make the model from the proposal highly considered for deployment in modern, dynamic, and security-sensitive applications of SDN-based computer networks.

4.2. Extended Discussions

4.2.1. Model Development Proposal

The SDN control loop of the proposed decision-making system includes traffic representation, temporal prediction, adaptive learning, and policy enforcement. This architecture expects policy decisions to change with traffic behaviour, unlike previous systems that separate intrusion detection, prediction, and mitigation. This approach uses controller telemetry-generated network flow graphs with switches and links to encode structural connectedness and flow-rule states. The model can reason about network traffic patterns over temporal instance sets and single packets or flows using this format. Tier-based model development. Time-series graphs depict how flow regulations and traffic characteristics vary over control periods. To overcome CNN-, RNN-, and shallow graph-based models' limited windows or static snapshots, long-range contextual memory is retained. Attention-driven sequence modelling finds influential flows and switches that may influence policy decisions on top of this representation. This predictability distinguishes the method from reactive systems that react to congestion or incursion.

The approach uses adaptive reinforcement learning to decide. Dynamic traffic danger and threat intensity, not manually calibrated reward functions, drive learning. This ensures that major events drive policy changes rather than minor fluctuations. Previous reinforcement learning–based SDN

RESEARCH ARTICLE

controllers lack context and converge slowly or oscillate under mixed traffic. This is remedied by aligning policy changes with operational severity, not raw detection outputs. This model stands out for its robustness and interpretability. The training and validation pipeline generates adversarial traffic, exposing the policy learner to structurally diverse attack behaviours not seen in historical datasets. Meanwhile, a causal analysis layer links policy acts to traffic events, explaining rule installations and removals. Unlike previous models, the proposed design prioritises robustness and explainability, offering an adaptable, operationally transparent controller.

4.2.2. Results Comparison and Analytical Interpretation Discussions

Experimental results reveal consistent latency, convergence speed, policy efficiency, and resilience advantages over comparable baseline models. The proposed model's policy update time lowers across all traffic conditions, according to latency graphs. Policy update latency stabilises at 35–40 ms under mixed attack settings and 65–90 ms under baseline approaches. Predictive attention techniques may build flow rules in advance, lowering controller reaction times. Reinforcement learning convergence charts prove adaptable learning. The recommended model converges in 80–100 seconds under typical and attack-heavy conditions, while comparison methods require 130–200 seconds. Steeper convergence curves mean smoother reward gradients and less policy Variability In Process. In hostile situations, delayed or conflicting feedback signals keep baseline methods unstable.

Packet drop rate and false positive graphs show these improvements' utility. The proposed approach achieves packet drop rates of <3% in volumetric and covert assault scenarios, compared to 5–7% for previous methods. Nearly half of policy trigger false positives fall. The graphical trends illustrate that causal filtering and severity-aware learning reduce unnecessary rule updates during harmless traffic surges, maintaining service quality and security. The proposed methodology differs significantly from prior techniques in adversarial robustness charts. Generated attack patterns identify and mitigate 88–92%, while baselines are below 80%. This shows how adversarial exposure during model creation helps policy learners generalise beyond known attack signatures.

4.2.3. Performance Gains and Causes

Synergistic design components, not algorithmic advances, improve the suggested approach. Predictive attention modelling reduces controller delay by anticipating policy adaptions. The controller changes rules to learnt traffic trajectories to reduce packet loss and speed mitigations instead of waiting for congestion or intrusion effects. Adaptive reinforcement learning accelerates convergence and stability. Scaling learning updates by traffic severity helps the model respond fast to important threats and avoid overreacting to low-impact anomalies. Targeted learning reduces reward variance and smoothes convergence curves. Without this feature, baseline models squander learning power on small deviations, delaying optimal policy creation sets.

Multiple traffic patterns during development increase robustness. Adding adversarially generated flows expands the model's behavioural space, reducing distribution shift sensitivity. The controller works effectively against unexpected or obfuscated attack strategies, while typical models fail quickly. Finally, causal policy mapping lowers spurious correlations, enhancing decision quality. The paradigm links policy actions to chronologically and contextually relevant events to avoid repeated rule installs in process. Flow-rule redundancy is reduced and controller-load installation is improved for this. The proposed framework is a full solution for real-time intrusion-aware SDN policy updates, outperforming previous models in efficiency, robustness, and interpretability sets.

4.3. Validated Statistical Analysis

For the proposed model performance analysis, the following procedure was followed: evaluation of expected values and variance of crucial performance indices across multiple runs. Each configuration was executed 10 times under different random seeds to account for variability due to stochastic elements inherent in both traffic generation and reinforcement learning training. For each performance metric-policy update latency, convergence time, flow rule redundancy, false positive rate-mean values were computed together with their standard deviation in order to evaluate consistency, with the following outcomes: expected policy update latency for the proposed model across all datasets: 39.47 ms ± 3.12 ms; mean convergence time for the reinforcement learning agent: 90.66 seconds ± 4.37 seconds; confirming thus high responsiveness and stability. Packet drop rates were found to average 2.16% ± 0.21%, while causal mapping accuracy was achieved at 81.60% ± 2.24%, confirming that the model is robust across varying network loads.

A two-tailed paired t-test with a 95% confidence level ($\alpha = 0.05$) was employed to test the statistical significance of the obtainment of the improvements over the baseline methods. The null hypothesis stated there is no significant difference between the proposed model and each of the baseline methods tested, while the alternate hypothesis stated there was at least a measurable improvement. In fact, p Values were below 0.01 across the board for all major metrics, thus refuting the null hypothesis with high confidence. For example, the p Values in the comparison of both policy update latency and false positive rates were 0.004 and 0.006, respectively, confirming that improvements were indeed statistically significant. In

RESEARCH ARTICLE

addition, Cohen's d was used for the effect size calculations for the present investigation: with values like 1.2 for convergence time and 1.4 for rule redundancy reduction, confirming that very large practical implications are being set in the process.

In selecting Method [3], Method [8], and Method [25] to be evaluated against one another in baseline comparisons, we've considered their relevance and prominence in recent SDN policy learning studies. Method [3] represents an early-stage SDN intrusion response framework using static reinforcement learning without attention mechanisms. It serves as a baseline for understanding how classical RL-based SDN controllers operate in non-adaptive environments. Method [8] takes the hybrid rule-based and ML-driven approach, where its policies do have threat signatures but lack temporal modeling, and is therefore relevant for mid-level comparisons. Method [25] combines flow-level threat detection deep neural networks with moderate adaptability, making it an excellent baseline for comparisons in adversarial environments. These methods have been selected based on citations, but they are also representative of diversity in design because they encompass broad architecture types in SDN policy adaptations.

The proposed model thrashes these baselines through all measures, especially under zero-day or adversarial traffic. For instance, in its GAN-driven adversarial robustness tests, the proposed model achieved detection accuracy of 91.3% while Method [25] acceded to 79.8%, and Method [3] fell below 73%, clearly pinning the advantage on the AIE-GAN module. Also, reward gradient variance, as earlier presented in tables showing its performance, was significantly lower, and thus converged to be much more stabilized-an essential requirement for real-time production systems. These rigorous statistical tests and variance analyses validate their proposition that the proposed system is not only more effective but also more operationally reliable than current state-of-the-art models in literature sets.

5. CONCLUSION AND FUTURE SCOPES

This study introduced a Reinforced Transformer Architecture for dynamic and intrusion-aware policy adaptation in Software Defined Networking environments, integrating TGT-EFRE, MRSTA-PTP, ARGRSM, AIE-GAN, and CIAPDM into a continuous feedback loop for prediction. Testing on CICIDS2018 and adversarially synthesized datasets showed improvements in policy update latency, reinforcement learning convergence, false positive rates, flow rule redundancy, reward stability, and robustness over 90% under GAN-generated zero-day conditions. Causal mapping accuracy above 80% increased policy interpretation and traceability, enhancing operational trust in automated SDN control mechanisms. These results show that the suggested architecture optimizes policy for dynamic and large-scale networks in a resilient, explainable manner. We will scale to distributed and multi-domain SDN controllers, integrate Network Function Virtualization for coordinated security orchestration, use meta-reinforcement learning to rapidly adapt to unseen threat distributions, enable federated cross-domain learning while protecting privacy, and embed inference logic in programmable data planes to reduce reaction latency in high-throughput.

REFERENCES

[1] Haifa Ali Saeed Ali, Vakula Rani J, "Deep Learning Approach for Protecting IoT Smart Home Devices Against Multiclass Botnet Attacks", International Journal of Computer Networks and Applications (IJCNA), 12(3), PP: 307-323, 2025, DOI: 10.22247/ijcna/2025/20.

[2] Pruthvi Kumar K R, Usha B A, "Geometric Cryptosystem Based Elliptic Curve Cryptography and Advanced Encryption Standard with Galois Counter Mode for Secure Cloud Storage", International Journal of Computer Networks and Applications (IJCNA), 12(3), PP: 324-335, 2025, DOI: 10.22247/ijcna/2025/21.

[3] Boubaker, N.E.H., Zarour, K., Guermouche, N. et al. Optimizing Workflow Offloading and Migration under Timed Constraints in Fog and Cloud Computing. J Grid Computing 23, 10 (2025). https://doi.org/10.1007/s10723-025-09795-5.

[4] Tian, Q., Li, G. Fog computing based cost optimization for university governance. Sci Rep 15, 35691 (2025). https://doi.org/10.1038/s41598-025-19608-0.

[5] Monika, Sehrawat, H. Multi-parametric and priority driven particle swarm (MPPPSO) optimized task scheduling approach for improving performance of fog computing system. Prog Artif Intell 14, 301–318 (2025). https://doi.org/10.1007/s13748-025-00366-z.

[6] Xu, C., Zhang, F., Yang, Z. et al. A few-shot network intrusion detection method based on mutual centralized learning. Sci Rep 15, 9848 (2025). https://doi.org/10.1038/s41598-025-93185-0.

[7] Mo, J., Ke, J., Zhou, H., & Li, X. (2025). Hybrid network intrusion detection system based on sliding window and information entropy in imbalanced dataset. Applied Intelligence, 55(6). https://doi.org/10.1007/s10489-025-06307-6.

[8] Shan, L. (2025). (IoT) Network intrusion detection system using optimization algorithms. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-04638-5.

[9] Manivannan, R., & Senthilkumar, S. (2025). Intrusion Detection System for Network Security Using Novel Adaptive Recurrent Neural Network-Based Fox Optimizer Concept. International Journal of Computational Intelligence Systems, 18(1). https://doi.org/10.1007/s44196-025-00767-x.

[10] Binthiya, A., & Ravindran, S. (2025). An effective classification using enhanced flame seeker optimization with convolution neural network for intrusion detection. Wireless Networks, 31(5), 3873-3891. https://doi.org/10.1007/s11276-025-03956-w.

[11] Sadhwani, S., Sriwastawa, A., Muthalagu, R., & Pawar, P. M. (2025). Feature engineering based intelligent intrusion detection system for IoT network security. International Journal of Machine Learning and Cybernetics, .https://doi.org/10.1007/s13042-025-02631-y.

[12] Wu, Y., Zang, Z., Zou, X., Luo, W., Bai, N., Xiang, Y., Li, W., & Dong, W. (2025). Graph attention and Kolmogorov–Arnold network based smart grids intrusion detection. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-88054-9.

[13] Shi, D., Xu, M., Qin, Z., & Zhong, Y. (2025). Local enhanced toeplitz neural network for in Vehicle network intrusion detection. Journal of King Saud University Computer and Information Sciences, 37(1-2). https://doi.org/10.1007/s44443-025-00006-5.

[14] Xu, C., Zhan, Y., Wang, Z., & Yang, J. (2025). Multimodal fusion based few-shot network intrusion detection system. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-05217-4.

RESEARCH ARTICLE

[15] Wang, Y., Han, Z., Du, Y., Li, J., & He, X. (2025). BS-GAT: a network intrusion detection system based on graph neural network for edge computing. Cybersecurity, 8(1). https://doi.org/10.1186/s42400-024-00296-8.
[16] Thaljaoui, A. (2025). Intelligent network intrusion detection system using optimized deep CNN-LSTM with UNSW-NB15. International Journal of Information Technology, 1-17, https://doi.org/10.1007/s41870-025-02416-0.
[17] Yang, Y., & Peng, X. (2025). BERT-based network for intrusion detection system. EURASIP Journal on Information Security, 2025(1). https://doi.org/10.1186/s13635-025-00191-w.
[18] Farhan, S., Mubashir, J., Haq, Y. U., Mahmood, T., & Rehman, A. (2025). Enhancing network security: an intrusion detection system using residual network-based convolutional neural network. Cluster Computing, 28(4). https://doi.org/10.1007/s10586-025-05156-9.
[19] Yang, Y., Liu, X., Wang, D., Sui, Q., Yang, C., Li, H., Li, Y., & Luan, T. (2025). A CE-GAN based approach to address data imbalance in network intrusion detection systems. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-90815-5.
[20] Biju, A., & Franklin, S. W. (2025). Dual Feature-Based Intrusion Detection System for IoT Network Security. International Journal of Computational Intelligence Systems, 18(1). https://doi.org/10.1007/s44196-025-00790-y.
[21] 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.
[22] Rabih, R., Vahdat-Nejad, H., Mansoor, W., & Joloudari, J. H. (2025). Highly accurate anomaly based intrusion detection through integration of the local outlier factor and convolutional neural network. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-08175-z.
[23] Du, R., Huang, M., & Liu, F. (2025). Multi-classification algorithm based on graph convolutional neural network for intrusion detection. Signal, Image and Video Processing, 19(6). https://doi.org/10.1007/s11760-025-04083-x.
[24] Farhan, M., Waheed ud din, H., Ullah, S., Hussain, M. S., Khan, M. A., Mazhar, T., Khattak, U. F., &Jaghdam, I. H. (2025). Network-based intrusion detection using deep learning technique. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-08770-0.
[25] Huynh, H., Nguyen, X., Nguyen, X., & Le, K. (2025). Bigsids: an efficient SDN-based network intrusion detection systems for big data environments. Cluster Computing, 28(6), https://doi.org/10.1007/s10586-024-05075-1.

Authors

Sonam Chopade is an Assistant Professor in the School of Computer Science and Engineering at Ramdeobaba University, India, with over six years of combined teaching and industry experience. She is currently pursuing her Ph.D. at the same institution. Her research interests include Artificial Intelligence, Cloud Computing, Algorithms, and Web Technologies. She has published 13 research papers in reputed journals and conferences and holds three design patents along with four copyrights. She actively mentors undergraduate students and guides academic projects. She received the Best Presentation Award at the RUBICON Computing 2025 conference organized by Ramdeobaba University. She has secured top ranks in several NPTEL courses, earning Elite and Silver certifications, and is also a certified Salesforce Platform Developer I professional.

Dr. Archana Ganesh Said (PhD. Computer Engg.) is working as an Assistant Professor in the Department of Computer Engineering of AISSMS IOIT with more than 20 years of experience both in Teaching and Research. She has published more than 30 research articles in referred journals such as Science Citation Index Expanded, Scopus Indexed Journals / Book Chapters, IEEE Explore and holds patents. She is a lifetime active member of ISTE Her research areas of interest are Machine Learning, Deep Learning and Databases.

Ms. Yasmin S Khan is working as an Assistant Professor in the Department of Computer Engineering of D.Y.Patil COE, Pune with 10 years of experience both in Teaching and Research. She has completed an undergraduate engineering degree in specialization of Computer Eng and a postgraduate degree in Computer Science and Engineering. She is currently pursuing a PhD from Symbiosis University. She has published 10 research articles in referred journals such as Science Citation Index Expanded, Scopus Indexed Journals / Book Chapters, IEEE Explore and holds patents. Her research areas of interest are Machine Learning, Computer Vision, Image Processing and Video Processing.

Dr. Dasari Anantha Reddy is an Assistant Professor and Assistant Controller of Examinations in the Department of Computer Science and Engineering at Koneru Lakshmaiah Education Foundation, Hyderabad, India. He received his Ph.D. in Information Technology from National Institute of Technology Raipur, with research focused on designing effective deep learning frameworks for automated skin disease diagnosis. His research interests include medical image analysis, deep learning, computer vision, machine learning, and AI-driven healthcare systems. He has published several research articles in reputed international journals and conferences, particularly in the areas of skin disease detection, medical image segmentation, and hybrid deep learning architectures. Dr. Reddy is also actively involved in academic administration, research supervision, and interdisciplinary AI-based healthcare innovations.

Yogita G. Bobade is a Ph.D. Scholar in the Department of Electronics and Communication Engineering at Indian Institute of Information Technology Nagpur. She holds a Master of Engineering (M.E.) in Electronics and Telecommunication Engineering from Sant Gadge Baba Amravati University and a Bachelor of Engineering (B.E.) in Electronics and Telecommunication Engineering from Rashtrasant Tukadoji Maharaj Nagpur University. Her academic background reflects a strong foundation and continued research engagement in the field of electronics and communication engineering.

Tabassum H. Khan is an Assistant Professor in the Department of Artificial Intelligence at G. H. Raisoni College of Engineering and Management, Nagpur, India. She has 19 years of rich academic experience and holds a Ph.D. in Natural Language Processing and Machine Learning. She has patents, copyrights, and several high-quality research publications to her credit. She is the recipient of the I2OR National Award 2021 under the Elite Teacher category. She has also been awarded the prestigious Primary Evaluator certificate from the Government of India for her outstanding contribution as a judge in Toycathon 2021. Additionally, she served as a mentor for IEEEXtreme 15.0 programming competition in 2021. She is reviewer for many reputed conferences and journals in the computer science domain and has chaired numerous sessions at conferences. Her areas of interest include Machine Learning, Artificial Intelligence, Natural Language Processing, Blockchain Technology, Theory of Computation, and Databases. She maintains a strong industry connection to help upgrade her B.Tech students' skills and has served as the SAC Chair for the IEEE Nagpur Subsection for two consecutive years and is an active IEEE Senoir professional member. She has also mentored her campus IEEE WIE, NSS, and SB branches. Her professional society memberships include IEEE, Lifetime ISTE, I2OR Fellow Member, IAENG, and ACM.

RESEARCH ARTICLE

How to cite this article:

Sonam Chopade, Archana Ganesh Said, Yasmin S Khan, Dasari Anantha Reddy, Yogita G Bobade, Tabassum H Khan, "Design of An Improved Reinforced Transformer Architecture for Real-Time Policy Optimization in Intrusion Resilient Networks", International Journal of Computer Networks and Applications (IJCNA), 13(1), PP: 159-178, 2026, DOI: 10.22247/ijcna/2026/09.