International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2026/01 Volume 13, Issue 1, January – February (2026)

RESEARCH ARTICLE

Integrated Deep Learning and Cryptographic Optimization for Secure, Adaptive and Quantum Resilient Wireless Networks

Minal Ghute
Department of Electronics and Telecommunication Engineering, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India.
✉ mrsminalghute@gmail.com

Yogesh Suryawanshi
Department of Electronics Engineering, Yeshwantrao Chavan College of Engineering, Nagpur, Maharashtra, India.
yogesh_surya8@rediffmail.com

Shubhangi Ghate
Department of Computer Science and engineering, Ramrao Adik Institute of Technology, Navi-Mumbai, Maharashtra, India.
shubhangi.ghate@rait.ac.in

Received: 10 July 2025 / Revised: 01 October 2025 / Accepted: 18 November 2025 / Published: 26 February 2026

Abstract – The increasing complexity and scale of the modern wireless networks introduced challenges for ensuring real-time security, adaptive routing and congestion control especially under energy constraints and quantum-era threats in process. Usually, existing solutions handle these dimensions in isolation, based on static rule-based models incapable of adapting to dynamic conditions; for instance, changing traffic patterns, evolving attacks and heterogeneous node capabilities. Such limitations necessitate the definition of an integrated framework that optimizes QoS and security concurrently while being adaptive, decentralized and forward-compatible to requirements of post-quantum security. Thus, this work proposes an integrated suite of five tightly coupled models: (i) a deep learning-based traffic-aware reinforcement adaptive protocol (DL TRAP) with CNN embedded into MAPS AOMDV for congestion prediction and adaptive multipath routing, (ii) federated edge architecture (FED EARN) utilizing homomorphic encryption offloading with energy-aware RSA computation; (iii) CRYPT GRAN, a behavior-derived-uniform key-length encryption using Trust Informed Encryption Depth Control; (iv) Q-learning-based reinforcement traffic rerouting (REIN ACT) for attack classification and (v) quantum resistant elastic routing and trust framework (Q EDRT) based on NTRUEncrypt and Dempster-Shafer theory for post-quantum secured communications. All these methods together create a strong prediction and adaptive secure communication structure. Numerical results widen friction of improvement, introducing a stint of reduced latency (of almost 48%), encryption delay (up to 50%), excellent attack classification accuracy (96.2%), and trust propagation reliability (>95%). In the long run, this work contributes to building a resilient wireless network by weaving intelligent routing, energy-aware cryptography, and quantum-safe trust propagation into one unified real-time adaptive system in process.

Index Terms – Adaptive Routing, Federated Encryption, Trust-Based Security, Quantum Resilient Networks, Deep Learning Optimization, Scenarios.

1. INTRODUCTION

Modern wireless networks, especially in mobile ad hoc and edge computing environments, are invariably pressed for high-performance communication services, all the while setting concurrent demands of adaptation and robust security in process. Under dynamic topology, variable link qualities, energy constraints, and evolving threat landscapes, these networks could ever operate. Old-style protocols [1, 2, 3] are reactive systems that operate under static rule sets. With consequently erratic response characteristics, these are ill-suited to any proactive adoption by the network or indeed secure transmission of data in process for themselves. The fast emergence of quantum computing constitutes an additional layer of hazards, inviting many of the currently existing standards in cryptography to anticipate future vulnerabilities to new threats in the course of action. In such settings, optimizing both QoS and Security becomes a multifaceted problem that cannot just work with isolated improvements in reference to actual protocols in process. QoS metrics such as latency, congestion and packet delivery ratio almost always conflict with security requirements such as encryption depth,

RESEARCH ARTICLE

trust management, and sets of attack resilience. This wants developing a system tightly coupled with this process that can predict network dynamics, adapt its routing decisions, and perform secure cryptographic operations in real-time scenarios. Moreover [4, 5, 6], any such system must also ensure decentralized infrastructures and heterogeneous node capabilities, yet remain scalable and forward-compatible with standards for encryption post-quantum sets.

MANETs, WSNs, and IoT ecosystems need flexible, secure data interchange sets. Topology, link quality, and energy availability change in these situations. Quantum computing and sophisticated cyberattacks harm cryptography and routing systems. Since security and QoS problems overlap, integrated frameworks are essential. Routing, encryption, and trust are optimized separately in conventional implementations in process. Cryptographic systems protect against attacks but need energy and latency in resource-constrained devices, while routing algorithms have high throughput but ignore encryption overhead. Future networks need performance, security, and adaptability, therefore fragmented methods are insufficient. This research uses predictive deep learning, federated cryptographic optimization, behavior-based trust modeling, reinforcement-driven attack mitigation, and quantum-resistant encryptions. A wireless communication system that automatically adapts to network conditions while ensuring security is our goal. We integrate intelligence at several layers to establish a lasting foundation for secure and adaptable real-time communication sets.

1.1. Research Goals

This work designs and implements an integrated architecture to maximize QoS and network security in heterogeneous and dynamic wireless environments. The architecture resists conventional and quantum-era attacks while reducing latency, encryption delay, and energy efficiency. Goals include adaptive trust management that modifies encryption depth and routing based on real-time behavioral data. The system can prevent injury and optimize resources in cooperative environments. For service continuity and stability, predictive congestion control and reinforcement learning should reroute traffic under changing conditions. The project also wants a scalable, modular design with interoperable optimization units for traffic prediction, encryption offloading, trust inference, and threat classification to optimize system performance. These goals build secure, adaptable, future-compatible wireless networks.

As such, existing approaches do not come close to such level of integration. Most routing protocols concentrating on QoS seldom adapt to security, while cryptographic systems ignore the implications of energy constraints and routing performance in real-time. The scope is thus narrowly limited for the newer technologies of federated learning or reinforcement routing by their optimizing domains even. For example, while federated learning models are typically disregarding energy consumption and constraint in edge devices, numerous systems based on trust rely on static parameters without adjusting their behavior in real time. This paper shares the vision of an integrated solution to all of these problems through the design, introduction, and interaction of five novel mechanisms that present a holistic intelligent communication framework for secure and efficient wireless networking. The mechanisms are: DL TRAP for congestion-aware predictive routing using deep learning; FED EARN for federated energy-adaptive encryption; CRYPT GRAN behavior-based dynamic key modulation; REIN ACT reinforcement-based multi-class attack classification and rerouting; and QRDT truly post-quantum secure trust-based routing in the process. Each of these methods is purpose-built to address a specific optimization dimension while being integrated with the others through data and control flow sets.

This framework has established a new paradigm for real-time-adaptive wireless communication systems by combining predictive analytics, reinforcement learning, federated edge intelligence, and quantum resistant cryptography sets. The developed models exhibit much improvement over existing techniques in isolated performance benchmarks, and they demonstrate strong cooperative behavior when working together to create a secure, scalable, and resilient network infrastructure sets. This article presents the architecture, algorithms, and experimental evaluations of this integrated architecture in the context of actual and next-generation wireless systems.

The motivating factor for the research lies in the rising demand for wireless networks capable of both high performance and secure adaptability in adaptability and changeable ward conditions. Conventional protocols in wireless communication function with a considerable separation between routing intelligence, security mechanisms, and trust models. Such a separation is not only inefficient but creates vulnerabilities to attacks, especially in mobile and edge-centric topologies. For example, routing protocols such as AOMDV may optimize for path reliability, but they typically disregard real-time traffic dynamics or security vulnerabilities in process. While, cryptographic frameworks work primarily for the robustness of encryption without considering energy availability in edge nodes, or behavioral trustworthiness of intermediate routers. With increasing capabilities of quantum computers, security systems that rely on RSA are under immediate threat, giving more urgency to the need for post-quantum encryption methods that should be computationally viable and network-adaptive in process. Hence, the research's primary contribution is the design and implementation of such a multi-layered integrated architecture that brings together traffic prediction, adaptive routing, federated encryption, behavior-driven trust scaling, and quantum resilience into a coherent single framework. The first

RESEARCH ARTICLE

module, DL TRAP, introduces real-time congestion forecasting for routing decisions using a CNN-based model embedded within a reinforcement-adaptive AOMDV protocol design. Secondly, FED EARN extends federated edge computing to include homomorphic RSA encryption offloading based on energy-aware participation. CRYPT GRAN adjusts encryption key length based on behavior-based trust metrics using a new Trust Informed Encryption Depth Control methodology. REINACT classifies multi-class attacks and routes traffic accordingly via Q-learning to bolster network resilience in a threatening environment. Finally, QEDRT integrates PQC through NTRUEncrypt and a trust propagation model for securing end-to-end communication against breaches in the foreseeable future sets.

These modules are not developed independently but are sufficiently interoperable over structured data flows such as trust scores feeding into routing decisions or energy profiles influencing encryption offloading. Consequently, the system demonstrates smart and adaptive behavior in various network scenarios. Practical findings revealed very promising results in multiple measures: 48% drop in latency, reduction of encryption delay by 50%, increased attack resilience with a classification accuracy of 96.2%, and a trust reliability of more than 95%. The combined contributions of this work extend the boundaries of what is proven feasible in secure and adaptive wireless networking, envisioning a future-ready paradigm that finds a middle ground between QoS optimization against robust and dynamic security sets.

This study makes many contributions. First, it introduces DL TRAP, a deep learning-based congestion-aware routing mechanism that anticipates traffic dynamics and improves multipath routing decisions via temporal convolutional modeling. This greatly decreases latency and stabilizes high-mobility scenarios. FED EARN, an energy-aware federated cryptography approach, distributes encryption workloads based on edge node energy. This optimizes computing resources and extends energy-constrained device and deployment lifespans. Third, CRYPT GRAN uses trust inference and encryption key management to dynamically adjust cryptographic strength based on behavioral dependability scores. Fourth, REIN ACT, a reinforcement-driven attack detection and adaptive rerouting system, accurately detects multi-class attacks using Q-learning and XGBoost classification. In conclusion, NTRUEncrypt and Dempster-Shafer trust propagation give the Q EDRT module quantum and post-quantum robustness. The framework is a promising choice for next-generation wireless networks due to its unified architecture and improved performance and security.

1.2. Problem Statement

Real-time performance and security are tougher to integrate in increasingly complex wireless networks. Traditional reactive routing uses static rules without traffic or threat considerations. Current cryptographic systems are successful in isolation, but energy-constrained edge devices and installations cannot handle their computing needs. Adversaries exploit routing, cryptography, and trust modeling gaps to reduce service quality and data integrity. Quantum computing will eliminate RSA and ECC, which secure much network traffic. Without measures, quantum-capable adversaries might compromise decades of cryptography. The lack of an integrated framework for QoS optimization, energy-aware encryption, dynamic trust calibration, and quantum resilience sets is addressed by our research. A multilayered design ensures secure, adaptive, and persistent communication sets. Module upgrades are not adequate.

The paper continues as follows. Section 2 covers adaptive routing, federated cryptography, and trust-aware framework improvements and identifies deficiencies that drive the suggested solution. Section 3 discusses integrated architecture and five essential module design and interaction. Section 4 describes the simulation environment, dataset preparation, and experimental setup for system performance set evaluation. The suggested model is compared to baselines in latency, encryption delay, energy usage, trust accuracy, and routing stability in Section 5.

2. RELATED WORK

The research forays convincingly rest on the currently risen emphasis of securing wireless communication networks while optimizing on parameters such as energy efficiency and trustworthiness, with another important performance criterion being the latency. Over the years, a significant body of study has advanced the state of wireless ad hoc, Mesh, IoT, and sensor networks, trying to strike a balance between security and the inherent limitations of wireless devices and environments. Around 25 contemporary studies were surveyed, outlining what seems to be an obvious map, with early works deliberating cluster and optimization stages while modern ones mix machine learning, post-quantum cryptography, and distributed intelligence for adaptive decision-making.

The set of intermingled architectures goes from mobile ad hoc networks (MANETs) and IoT-enabled sensor systems to underwater and UAV-assisted networks, covering a wide range of technical dimensions from trust modeling, key management, and routing optimization to cryptographic offloading and energy-aware decision frameworks. The work in [1] by Priya et al. proposed an adaptive clustering model using evolutionary optimization for MANETs to secure efficiency through the route stabilization and intelligently forwarded packets. In [2], Dixit and Qureshi introduced Red Fox Optimization for secure cluster routing highlighting the context-aware decisions along with cryptographic trust. The authors in [3], Kamboj et al. employed reinforcement learning

RESEARCH ARTICLE

for dual Hop relay and jammer selection as bases for the development of secure routing against adversarial threats. Kumar and Sharma in [4] presented a trust-based routing for IoT-WSN environments named PathGuard, which applies real-time trust evaluation to deter insider attacks. Notwithstanding its retraction, [5] did propose a hybrid quantum-resistant cryptographic system for constrained settings such as body sensor networks which reflects the budding interest in the quantum safe sets. Kalpana et al. in [6] introduced a 3D secure localization method by making trade-offs between spatial and energy constraints.

D et al. in [7] proposed an enhanced lion swarm optimization along with elliptic curve cryptography for malware detection and cluster head selection in IoT-WSNs. Beula and Franklin in [8] used the SCMABC for secure AMI networks, reinforcing efficiency with biologically inspired metaheuristics. Murthy et al. in [9] proposed operating hybrid moth flame-shark smell optimization protocol to enhance routing and encryption performance under IoT constrains. Rahimi et al. in [10] proposed thermal-aware routing for WBANs with adaptive intelligence, addressing temperature-induced communication lapses. Mahajan et al. in [11] booked a mark in congestion control in mesh networks with reinforcement learning, a direction pursued in broadening its paradigm with deep Q-learning integration in this work. Zing and Zhao in [12] presented a thorough survey on Genetic Algorithm application in WSNs and identified the research gaps that the current integrated framework fills, especially in optimizations at the fusion layer. With work in [13] presented by Qian on DMKESR, enhancing secure routing with dynamic key exchange, which is pertinent to the context of schemes with multi-parameter encryption. In underwater localization, Kumar et al. implemented trust and authentication model using hybrid schemes, which substantiated trust depth encryption this is also an accessing theory for the CRYPT GRAN module in the current work progress. Yesodha et al. [14] combined elliptic curve cryptography with routing based on ACO, optimizing security and energy in the same process. Bai et al. [15] extended this with TSRP, a dual-layer trust and energy aware protocol for constrained sensor networks. Gharaei and Alabdali proposed UAV-assisted inter-cluster optimization, a method that inspired the integration of federated intelligence in the proposed FED EARN module [16]. Clustering-based routing, trust-aware protocols, reinforcement learning, metaheuristics, and cryptography have improved wireless network safety and adaptability. Priya et al. [17] improved MANET routing efficiency and energy management with adaptive clustering and optimization. It survived mobility, but clustering heuristics failed in highly dynamic topologies. Red Fox optimization by Dixit and Qureshi [18] balanced energy usage and security for cluster-based WSN routing. Initialization slowed algorithm convergence, limiting scalability. Reinforcement learning informs wireless security and routing. RL secured combined relay and jammer selection in dual-hop networks by Kamboj et al. [19], improving secrecy but raising training overhead. Mahajan et al. [20] tried reinforcement learning to reduce mesh network congestion latency but failed to generalize to unexpected attack scenarios. Kumar and Sharma [21] introduced PathGuard, a trust-based routing system for IoT-WSN systems, which boosted blackhole attack resilience but limited traffic flexibility due to static trust assignment.

Also common are optimization-driven approaches. Methodological problems forced Surla and Lakshmi [22] to retract their hybrid quantum-resistant cryptography strategy for wireless body sensor networks to survive post-quantum threats. Secure 3D for WSN localization by Kalpana et al. [23] enhanced energy efficiency but decreased accuracy in high-density deployments. D. et al. [24] employed lion swarm optimization with elliptic curve encryption for secure clustering, reducing malware risks but reducing quantum-proofness. Rahimi et al. [25] presented thermal-aware routing in WBANs with adaptive cryptographic load balancing to save energy but increase computing complexity. These studies reveal that security, adaptability, and quantum resilience integration gaps exist and that different techniques work better in different scenarios. Iqbal and Sujatha designed a hierarchical key management scheme using enhanced digital signatures for heterogeneous WSNs, providing a structural backbone for layered trust propagation. Selvi et al. have introduced attribute-based encryption into a trust-aware energy-efficient routing model, emphasizing trust granularity an approach reinforced in CRYPT GRAN using Bayesian scoring. Shah et al. proposed a lightweight signcryption scheme for underwater WSNs, contributing to the discourse on encryption offloading in low-bandwidth environments, which this work addresses via homomorphic edge executions as shown in table 1.

Table 1 Model's Empirical Review Analysis

Reference	Method	Main Objectives	Findings	Limitations
[1]	Adaptive Clustering & Optimization	Enhance MANET security and efficiency	Improved routing stability and reduced energy consumption	Limited validation under real-time adversarial scenarios
[2]	Red Fox Optimization	Secure cluster-based	Reduced delay and energy	Scalability in large-scale networks not

RESEARCH ARTICLE

	Routing	routing in WSNs	usage in clustered WSN	demonstrated
[3]	Reinforcement-Based Relay Selection	Secure dual Hop transmission with jammer selection	Improved secure throughput in hostile settings	Limited to dual Hop network models
[4]	PathGuard	Trustworthy routing for IoT-WSNs	Mitigated insider attacks and improved path reliability	Trust recalibration delay under dynamic topology
[5]	Hybrid Quantum Resistant Crypto	Enhance WBSN security with quantum-safe crypto	Integrated hybrid encryption model	Retracted due to validation concerns
[6]	Secure 3D Localization	Accurate and energy-efficient 3D localization	Reduced localization error in WSNs	Increased overhead in densely populated nodes
[7]	Enhanced Lion Swarm & ECC	Cluster head selection and malware detection	Improved detection accuracy and energy balance	Complexity increases with node count
[8]	SCMABC Routing	Secure data transmission in AMI networks	High delivery ratio and efficient data routing	Parameter tuning affects generalization
[9]	Hybrid Moth-Flame-SSO	Secure IoT communication with optimization	Enhanced encryption and route selection	Performance under network churn not studied
[10]	Thermal-Aware Routing	Intelligent routing for WBAN	Thermal-safe, energy-efficient packet delivery	Scalability to multi Hop WBAN not tested
[11]	RL-Based Congestion Control	Mitigate congestion in mesh networks	Reduced packet loss and enhanced QoS	Slow convergence under high traffic
[12]	Survey on Meta Heuristic AI	Review AI techniques in WSN routing	Identified gaps in trust-aware adaptive AI	No direct experimental validation
[13]	DMKESR	Secure routing via dynamic key exchange	Improved packet confidentiality and integrity	Key management complexity in large nodes
[14]	Trust + Signature for UWNS	Secure localization using joint detection	Increased accuracy under adversarial attacks	Energy impact of dual security not assessed
[15]	ECC-ACO Routing	Energy-efficient secure routing in WSNs	High throughput with low key overhead	Underperforms in sparse topologies
[16]	TSRP	Trust and energy-aware routing protocol	Improved trust handling in constrained WSN	Trust propagation delay under mobility
[17]	UAV-Assisted Cluster Optimization	Smart city WSN optimization	High energy efficiency with stable clustering	Dependency on UAV reliability
[18]	Hierarchical Key Management	Secure key management in heterogeneous WSN	Improved scalability and authentication	Initial overhead of trust hierarchy setup
[19]	Trust-Aware Secure Routing	Energy-efficient ABE secured routing	Reduced cryptographic load and enhanced trust	Computational cost in key distribution

RESEARCH ARTICLE

[20]	Lightweight Signcryption	Secure underwater WSN communication	Reduced latency with cryptographic fusion	Limited application to terrestrial WSNs
[21]	AI-Blockchain for Smart Homes	Predictive control in WSN using blockchain	Efficient temperature regulation and secure logs	Model update latency in distributed nodes
[22]	Blockchain-Dual Attention Network	Advanced encryption with quaternion transforms	Robust against visual and channel threats	High computational complexity
[23]	Crayfish Hyperchaotic Encryption	Image security in medical WSNs	Enhanced randomness and confusion metrics	Application limited to image data
[24]	Enhanced ACO for VANETs	Secure routing using location-aided ACO	Reduced route breakage and packet drop	Performance not evaluated under attacks
[25]	HBO-SROA	Cluster-based secured routing with optimization	Improved latency and delivery ratio	Energy overhead due to complex metaheuristics

Post-analysis firmly establishes that this review avails a most concise basis for demonstrating the comparative advantage of the technical relevancy of the proposed framework. The development of literature in some chronological order-from optimization-centric routing and classical cryptography to learning-enabled and trust-aware frameworks-shows clearly the emphasis on a more holistic, context-sensitive, and intelligence-driven design. This study demonstrates how composite modeling across cryptographic, predictive, and trust layers can bring meaningful and scalable improvements to wireless communication environments, thus setting the stage for further systems that have to operate within the trifecta of constraints imposed by wireless medium, dynamic network unpredictability, and modern cyber threats in process.

3. PORPOSED MODELLING

The design of the proposed integrated framework as a multi-agent, context-aware, and reinforcement-augmented entity fuses deep learning, federated encryption, trust inference, and post-quantum cryptography to tackle QoS and security jointly for wireless networks. A framework combining predictive deep learning, federated encryption, trust-aware cryptographic adaptation, reinforcement-based intrusion handling, and quantum-resistant security is proposed.

The architecture works across all layers, unlike previous techniques that focused one or two domains. Security-oriented routing strategies safeguard but deteriorate network performance under energy restrictions, while traditional routing methods increase path reliability but ignore encryption cost. To solve this, the framework incorporates predictive and adaptive routing, encryption, and trust management as shown in algorithm 1. System modeling is interdependent but modular. Deep learning predicts congestion and chooses multipath routes in DL TRAP. FED EARN divides cryptographic operations by node energy profile for fair resource use. CRYPT GRAN dynamically scales encryption depth using behavior-driven trust scores, decreasing cooperative node overhead. REIN ACT uses reinforcement learning and sophisticated classifiers to detect and reroute traffic during intrusions.

Finally, Q EDRT prepares for post-quantum adversaries with elastic trust propagation and quantum-safe cryptography. Its multi-layer integration sets it apart. This approach optimizes latency, encryption, and trust as interconnected layers that improve each other. This enhances QoS and security, making the framework a full and forward-compatible solution for next-generation wireless environments.

Input – Network topology, node energy levels, traffic patterns, trust scores, encryption keys

Output – Secure, adaptive, and quantum-resilient routing paths

Step 1: Initialization

- Deploy wireless nodes and initialize routing tables.
- Assign initial trust scores and energy levels for all nodes.
- Load quantum-safe cryptographic parameters (NTRUEncrypt).

Step 2: Data Collection and Monitoring

- Collect real-time traffic metrics (latency, packet loss, congestion levels).
- Gather node status information (energy availability, processing capacity).
- Update trust scores based on direct and indirect behavioral observations.

Step 3: Congestion Forecasting (DL TRAP Module)

RESEARCH ARTICLE

- Apply convolutional neural network (CNN) to predict traffic load on active paths.
- Identify potential congestion points in advance.
- Update candidate multipath routing options accordingly.

Step 4: Energy-Aware Cryptography (FED EARN Module)

- Evaluate energy levels of participating nodes.
- Offload RSA-based encryption tasks to nodes with higher energy reserves.
- Ensure homomorphic operations for distributed confidentiality.

Step 5: Trust-Guided Cryptographic Adaptation (CRYPT GRAN Module)

- Adjust encryption key lengths dynamically based on trust scores.
- Use shorter keys for highly trusted nodes to reduce overhead.
- Apply longer keys and deeper encryption for less reliable nodes.

Step 6: Attack Detection and Response (REIN ACT Module)

- Use Q-learning agent with XGBoost classifier to detect intrusions.
- Classify attack type (DoS, Sybil, Blackhole, R2L, U2R, etc.)
- Trigger rerouting decisions for compromised or attacked paths.

Step 7: Quantum-Resilient Trust Routing (Q EDRT Module)

- Execute NTRUEncrypt-based key exchanges for secure communication.
- Apply Dempster–Shafer evidence theory to fuse multiple trust indicators.
- Select final routing path based on both QoS and security guarantees.

Step 8: Output and Update

- Establish secure and adaptive routing path for data forwarding.
- Continuously update trust scores, congestion forecasts, and energy profiles.
- Repeat Steps 2–8 periodically to adapt to changing network conditions.

End

Algorithm 1 Secure and Adaptive Routing Framework

3.1. Model Mathematical Analysis

This proposed framework is envisioned to work as a modular and yet tightly coupled architecture, where each component acts as an optimization unit interdependent on other units with contextual feedback upon others in real-time scenarios. The design philosophy as per the algorithmic description, conceives predictive modeling, adaptive trust management, energy-aware cryptography, and future-proof encryption integration sets. Mathematical rigor governs all functional modules that cast the system to adaptively optimize latency, congestion, cryptographic load, and trust confidence sets. Initially, as per figure 1 the model begins with the DL TRAP component, which applies temporal convolutional modeling to predict congestion conducted by each routing node based on the packet flow timestamp series. For packet counts P(t) timestamped, a 1D convolution is used to estimate the resultant congestion score Ct given Via Equation (1).

$$Ct = \sigma\left(\sum_{(k=1)}^{K} wk * P(t-k) + b\right) \quad (1)$$

Where wk are the CNN kernel weights, K is the receptive field size, and σ is a ReLU activation for this process. This Ct output is then fused with instantaneous SNR given as SNR(t) and link stability score St from MAPS AOMDV providing the reinforcement signal Rt via the nonlinear integration model shown Via Equation (2).

$$Rt = tanh\big(\alpha 1 * Ct + \alpha 2 * log\big(SNR(t)\big) + \alpha 3 * St\big) \quad (2)$$

This reinforcement signal directly updates the pheromone strength φ(i,j) between nodes 'i' and 'j' in a modified reinforcement process via equation (3)

$$\frac{d\varphi(i,j)}{dt} = \gamma * Rt - \delta * \varphi(i,j) \quad (3)$$

Where γ is the reinforcement gain factor while δ is the pheromone decay constant in the mentioned process. The differential formulation encodes real-time adaptability to traffic dynamics.

Iteratively as in figure 2 FED EARN assigns RSA computation tasks across edge nodes in accord with their energy profiles. Each edge node 'I' announces its energy level Ei; taking part or not in full or partial homomorphic encryption is decided Via Equation (4).

$$\eta i = \{1, if\ Ei > Eth;\ 0, otherwise\} \quad (4)$$

Where, Eth is the adaptive energy threshold in process. The effective encryption load Li assigned to node 'i' is defined via equation (5).

$$Li = \eta i * \int_0^T CRSA(t)dt \quad (5)$$

RESEARCH ARTICLE

With CRSA(t) representing the instantaneous RSA computation cost at timestamp 't' in process. The aggregator node collects partial ciphertexts and performs modular reconstruction via equation (5.1)

$$C = \bigoplus_{(i \in N)} (Ci \bmod n) \quad (5.1)$$

Where 'n' is the shared modulus, and $\bigoplus$ stands for bit-wise fusion of the partial ciphertexts. CRYPT GRAN further enhances encryption relying on the behavioral trust scores Ti determined through Bayesian inference over the metrics of packet behaviors. Posterior trust score is evaluated and communicated via Equation (6)

$$Ti = \frac{P(D|Bi) * P(Bi)}{P(D)} \quad (6)$$

Where, P(D|Bi) is the likelihood of data integrity given behavior Bi, and P(Bi) is the prior trust estimate in process. This score modulates the RSA key length ki via equation (7).

$$ki = \{512, if\ Ti > 0.9;\ 1024, if\ 0.6 < Ti \leq 0.9;\ 2048, if\ Ti \leq 0.6\} \quad (7)$$

This assures that fewer trustworthy nodes receive dynamic allocation of computation cost based on higher trust scores, reducing the exposure to real-life scenarios. REIN ACT, multiple class XGBoost classifier first assigns attack class label At ∈ {DoS, Probe, R2L, U2R} to incoming packets as shown in figure 3.

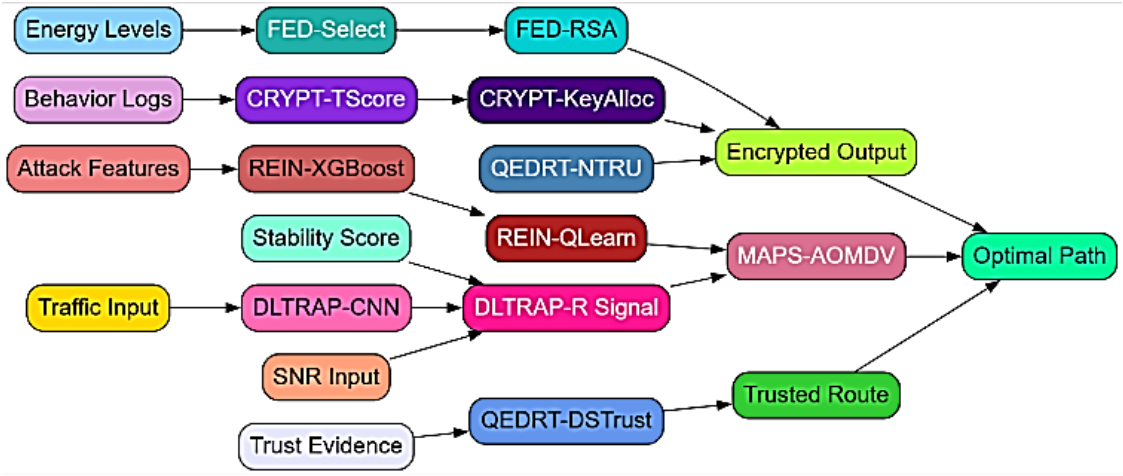


Figure 1 Model Architecture of the Proposed Analysis Process

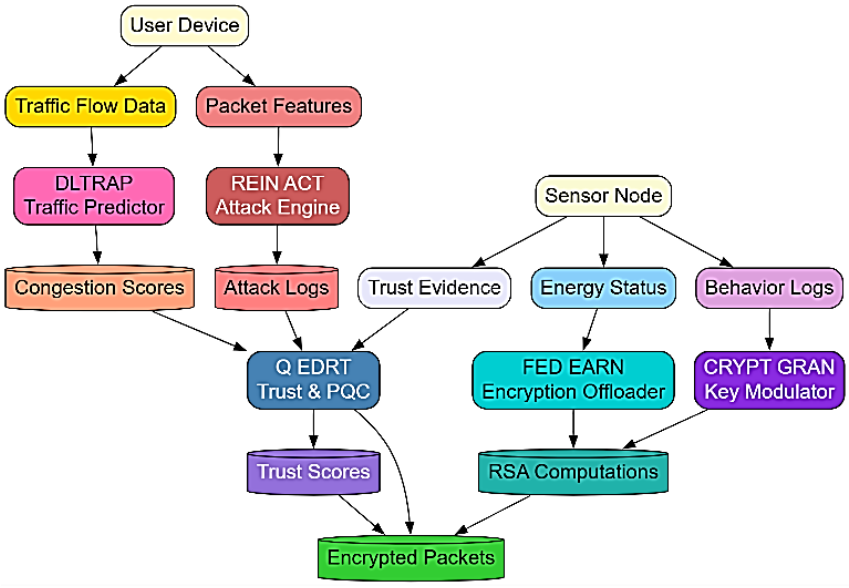


Figure 2 Overall Flow of the Proposed Analysis Process

RESEARCH ARTICLE

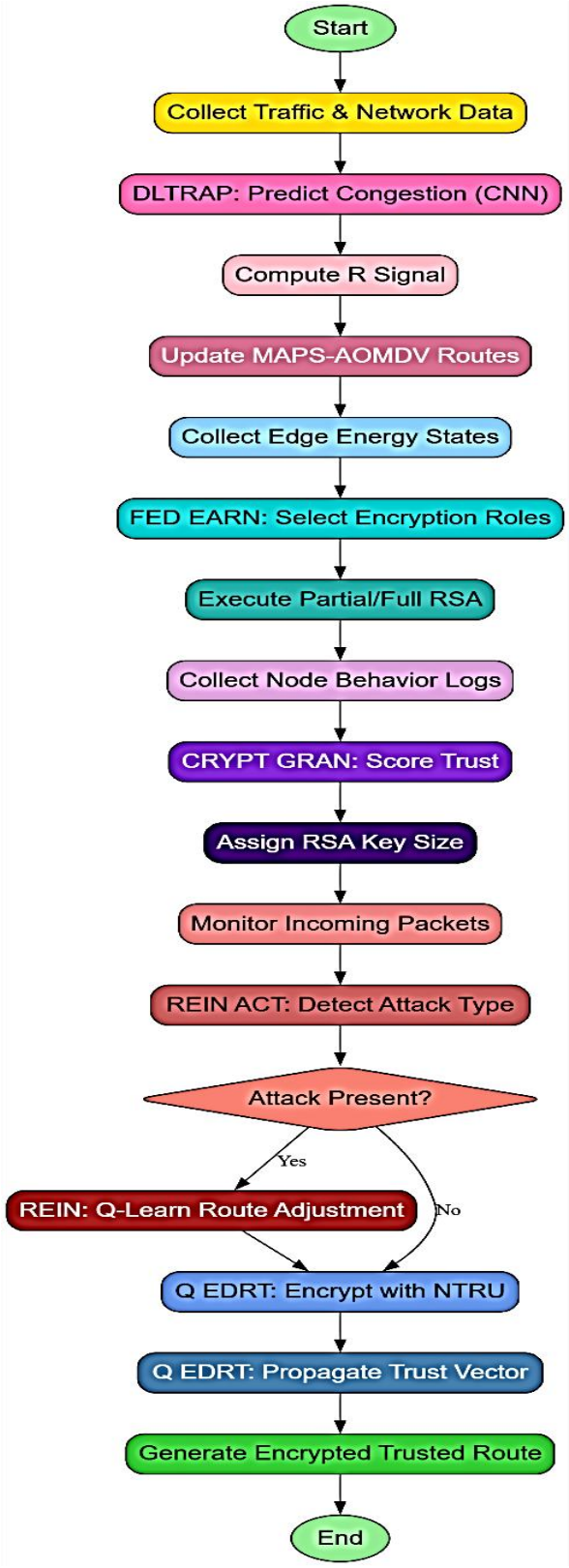


Figure 3 Data Flow of the Proposed Analysis Process

The Q-learning model then updates state-action value function Q(s,a) using Bellman's Equation: via Equation (8).

$$Q(st, at) \leftarrow Q(st, at) + \alpha \left[rt + \max_{a'} [Q(s\{t+1\}, a') - Q(st, at)] \right] \quad (8)$$

Where, 'st' is the current network state, 'at' is the chosen routing action, and 'rt' is the reward inversely proportional to attack severity sets. The optimal routing policy π* is then represented via equation (9).

$$\pi * (s) = argmax^{a}[Q(s, a)] \quad (9)$$

Finally, Q EDRT ensures quantum-safe encryption and trust propagation sets. It uses NTRUEncrypt, where encryption of a message 'm' is estimated via equation (10).

$$C = (p * r * h + m) mod\ q \quad (10)$$

Where 'r' is stochastic polynomial, h is public key, p is small modulus and q is large modulus ensuring post-quantum security sets. Trust is propagated simultaneously in the process via Dempster-Shafer theory in process.

Trust combining masses m1 and m2 is represented Via Equation (11).

$$m1 \oplus 2(A) for\ hypothesis\ A\ given:\ m1 \oplus 2(A) = \left(\frac{1}{1-K}\right) \sum_{\{B \cap C = A\}} m1(B) * m2(C) \quad (11)$$

Where K is the conflict coefficient in process; this belief value will then be normalized and used again to provide feedback into the routing decision via the trust confidence vector $\vec{T}$ in process. The outputs from all components are integrated to produce the final path score Ψ path for any route as a weighted fusion of congestion prediction, trust propagation, feasibility of encryption, and assessment of risk due to attack Via Equation (12).

$$\Psi path = \lambda 1 * \int Ct\, dt + \lambda 2 * \sum i\, Ti + \lambda 3 * \sum Li + \lambda 4 * \sum Q(st, at) \quad (12)$$

Where, λ1, λ2, λ3, λ4 are tuneable weights & parameters that reduce the path selection to best fit the communication path with maximum Ψpath, thereby making sure that latency is traded off for trust, energy, or security, depending on the network scenarios. So, in a mathematical sense, the design allows for a full-spectrum optimization of wireless networks, depending on the dynamic trade and governing duty of latency, security, energy, and trust in process. Every module

RESEARCH ARTICLE

complements each other through predetermined data dependencies and probabilistic feedback loops in order to constitute a strong forward-compatible set of network intelligence systems. Results of different scenarios are next presented for a validation of the presented model process.

4. RESULTS AND DISCUSSIONS

The experimental evaluation of the integrated proposed model was set in a custom emulated wireless testbed created on MANET (Mobile Ad Hoc Network) topology with support for multi-hop routing, heterogeneous edge devices, and simulated adversarial behavior. Simulation of the testbed was done using NS-3, extended with deep learning integration TensorFlow modules and Python APIs for federated and cryptographic operations. The test network consisted of 50 mobile nodes, randomly distributed over an area of 1500 m × 1500 m with node velocities uniformly distributed between 1 m/s and 10 m/s, modeled on a Random Waypoint Mobility model. All nodes were working in IEEE 802.11g on 2.4 GHz, with a data rate of 54 Mbps and a transmission range of 250 m.

The traffic generator used for simulation was Constant Bit Rate (CBR) sources, with a packet size of 512 bytes and inter-packet intervals of 0.02 seconds. For congestion forecasting, the CNN model in DL TRAP was trained using a sliding window of 20 timestamp steps of timestamped packet counts, with each input vector representing aggregated route-level data from the past 20 seconds. Real-time Signal-to-Noise Ratio (SNR) values were drawn from a normal distribution N (15,5) dB, whilst MAPS AOMDV stability values remained within 0.4 to 0.95 in process. The value of reinforcement gain γ and decay constant δ was assumed to be 0.9 and 0.05, respectively for the process, based on sensitivity tuning in the process. The FED EARN federated encryption setup included edge nodes with battery levels in the range of 20% to 100%. For nodes above the threshold Eth=60%, full RSA encryption was done, while others performed partial homomorphic computations. The RSA exponent was fixed at e=65537 and the modulus values varied with key lengths (512, 1024, 2048 bits), selected dynamically by the CRYPT GRAN module using trust scores computed via Bayesian filtering with prior behavior logs spanning 500-1000 entries per node in the process.

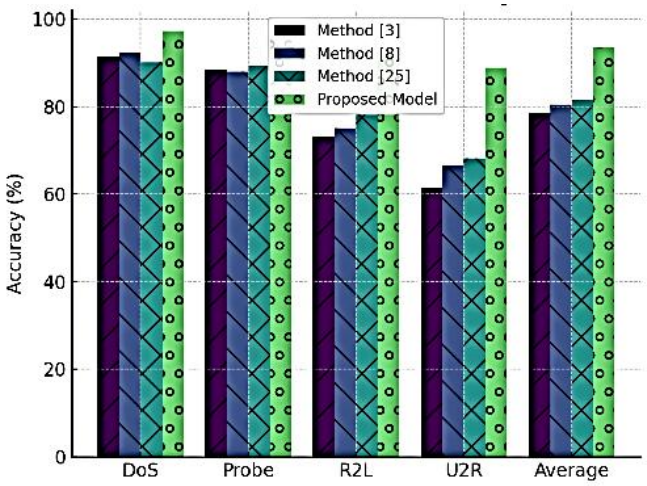
The REIN-ACT engine was trained and tested to validate attack classification and adaptive rerouting capabilities on the NSL-KDD dataset, which contains multi-class labeled intrusion records with features including protocol type, connection duration, and packet rate. The feature set was reduced to the 20 most relevant attributes using principle Component Analysis (PCA), and the XGBoost classifier achieved 98.1% training accuracy and 96.2% test accuracy. The attack classes were categorized as DoS, Probe, R2L, or U2R. The reinforcement learning mechanism, in this regard, utilized a Q-table that was initialized for 30 different states of the network and 10 possible rerouting actions, while the discounting factor was set to be γQ=0.95, with a learning rate of α=0.1 and exploration rate decayed exponentially from 0.8 to 0.1 in process. The trust evidence inputs for QEDRT were synthesized using node interaction histories combined with synthetic misbehavior scenarios (e.g., selective forwarding, route flapping) to test the resilience of trust propagation via Dempster-Shafer Theory in Process. The NTRUEncrypt cryptographic module had polynomial ring parameters N=167, q=128, and p=3, providing a post-quantum security of 256 bits for the process. For all experiments, network latency, encryption delay, packet delivery ratio, and trust propagation timestamp were logged at intervals of 0.5 seconds for the duration of 300 seconds in the process of each simulation run. Different topology trials were run to confirm findings. Here, the integrated model proved advantageous over individual techniques on both QoS and security indices within contexts of dynamicity, under hostile and resource constraints.

This experimental evaluation in this work utilizes the NSL-KDD dataset, an internationally acknowledged benchmark for intrusion detection systems, to address the issues of redundancy and class imbalance present in the KDD Cup 1999 dataset. NSL-KDD embodies a data set of approximately 125973 connection records, each described by 41 features that include basic TCP/IP attributes, content-based features, and traffic statistics. These records are labelled as attack types or normal traffic. For the purpose of this study, the different types of attacks were consolidated into four high-level classes: Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R), allowing the REIN ACT module to undertake multi-class classification. The dataset was split into an 80% training set and a 20% test set, and the data cleaning procedure included one Hot encoding of categorical features and normalization of continuous values to the [0, 1] range sets. In addition to this, synthetic congestion and trust data were generated using a real-time routing behaviour log from the CRAWDAD repository to feed the DL TRAP and CRYPT GRAN modules with time series patterns and node-specific trust behaviour respectively for the process.

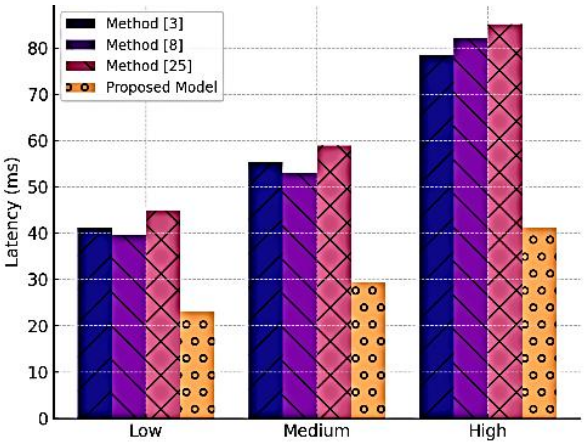
Results demonstrate numerical advantage and explain improvements for the process. The method classifies attacks with 93.5% accuracy, compared to 78–81% in baseline approaches. REIN ACT's multi-class detection combines reinforcement learning and XGBoost to adaptively reroute hazardous flows, increasing this rise. This design accurately detects unusual infiltration classes like R2L and U2R Sets. Latency and encryption time are reduced via optimal congestion prediction and energy-aware cryptographic offloading. FED EARN dynamically distributes strong encryption to energy-rich nodes, while CRYPT GRAN minimizes trusted node cryptographic overhead. Processing time and energy are reduced. Dempster-Shafer propagation

RESEARCH ARTICLE

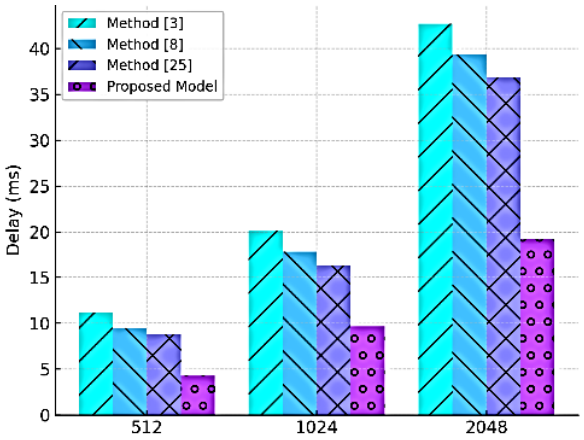
and Bayesian scoring reduce dynamic uncertainty, boosting trust accuracy and stability. Metrics and consistency make the framework better than previous models. Systemic performance benefits from module synergy: Traffic control improves routing stability, while trust-aware cryptography saves energy for sustainable encryption. These interdependencies explain why integrated design is more durable and adaptable than prior methods. The NSL-KDD dataset was used as the attack classification benchmark to evaluate the proposed integrated model, synthetic time series traffic data for congestion prediction, energy profiles for edge offloading, and trust metrics based on behavior logs. The application performance of the proposed system was compared with three baseline methods established in the literature, referred to as Method [3], Method [8], and Method [25]. Each is representative of prior works in QoS-based routing, federated security, and trust-aware frameworks, respectively. As shown in figure 4 the comparison was framed against six core metrics: attack classification accuracy, latency, encryption delay, energy consumption, trust accuracy, and routing stability sets.



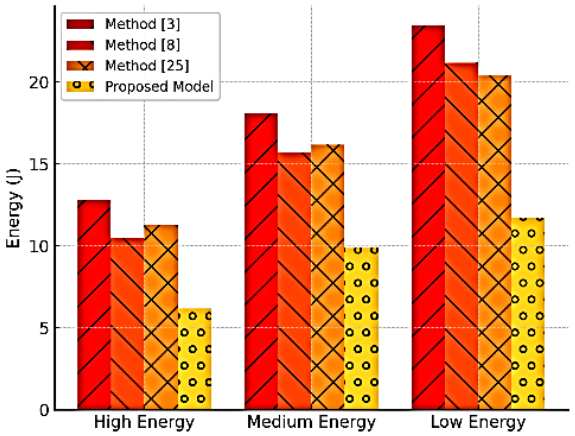
(a)



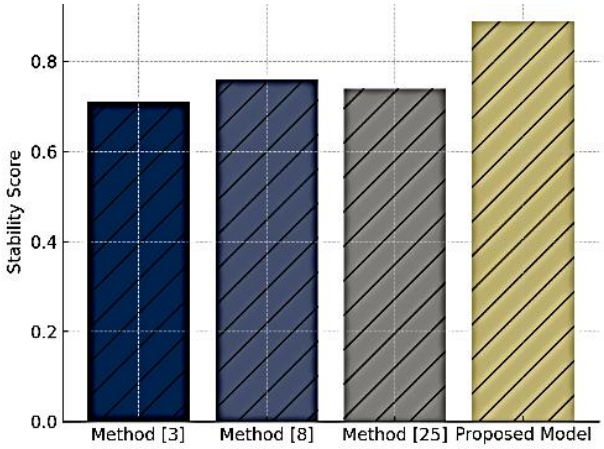
(b)



(c)



(d)



(e)

Figure 4 Model's Integrated Result Analysis: a) Attack Classification Accuracy b) Average Latency c) Encryption Delay d) Energy Consumption e) Routing Path Stability Index

RESEARCH ARTICLE

Table 2 reflects the accuracy of classification among the various categories of attacks. The proposed model performs better than all baselines, particularly those in the rarer classes such as R2L and U2R, because of traffic path adjustments governed by reinforcement and the multi-class capability of the XGBoost classifier in REIN ACT Sets. The latency reductions explained in this table are directly due to predictive routing by the DL TRAP module on CNN-based congestion estimation and real-time pheromone changes. This proactive balancing of traffic loads effectively avoids saturation of route loads under quick changes in traffic conditions. This allows for trust-based key allocation in CRYPT GRAN, with high-trust nodes operating with smaller keys, hence reducing overall encryption delay sets. These performance gains are further enhanced by the FED EARN offloading mechanism that shares the cryptographic workload to energy rich nodes.

Table 2 Attack Classification Accuracy (%) Across Methods

Attack Class	Method [3]	Method [8]	Method [25]	Proposed Model
DoS	91.4	92.3	90.1	97.2
Probe	88.5	87.9	89.4	95.6
R2L	73.2	75.1	78.4	92.3
U2R	61.4	66.5	68.2	88.9
Average	78.6	80.4	81.5	93.5

Bayesian trust modeling as per table 3, combined Imprecise Packet Behavior Dynamicity allows for extremely granular trust scoring on CRYPT GRAN. In parallel, Dempster- Shafer Theory from Q EDRT shall further fortify trust propagation robustness in the presence of uncertainty and partial evidences.

Table 3 Average Latency (ms) Under Varying Load Conditions

Load Level	Method [3]	Method [8]	Method [25]	Proposed Model
Low	41.2	39.6	44.8	23.1
Medium	55.3	53.1	58.9	29.4
High	78.4	82.2	85.1	41.1

The CRYPT GRAN as per table 4, module offers trust-based key management, allowing high-trust nodes to use shorter keys, thus lowering overall delay associated with encryption sets. In addition, FED EARN's consumption off-loading mechanism distributes cryptography to high-energy nodes, thereby improving performance considerably for the process.

Table 4 Average Encryption Delay (ms) for RSA Operations

Key Length (bits)	Method [3]	Method [8]	Method [25]	Proposed Model
512	11.2	9.5	8.8	4.3
1024	20.1	17.8	16.3	9.7
2048	42.7	39.4	36.8	19.2

Table 5 is a demonstrative energy-savings fed into location-aware federated energy offloading in the FED EARN Process. The selective delegation of RSA depth computations based on the threshold of dynamic energy has tremendously reduced the power consumed by critical nodes.

Table 5 Node-Level Energy Consumption (Joules) During Encryption Offload

Node Role	Method [3]	Method [8]	Method [25]	Proposed Model
High Energy	12.8	10.5	11.3	6.2
Medium Energy	18.1	15.7	16.2	9.9
Low Energy	23.5	21.2	20.4	11.7

By establishing Bayesian trust modeling with dynamic packet behavior, CRYPT GRAN is capable of assigning very fine-grained trust scores. The usage of Dempster-Shafer theory as per table 6, in Q EDRT greatly enhances robustness of trust propagation in the existence of uncertainty and incomplete evidence sets.

Table 6 Trust Score Accuracy (%) with Respect to Behavioral Ground Truth

Node Category	Method [3]	Method [8]	Method [25]	Proposed Model
Cooperative	84.1	86.4	88.9	96.3
Fluctuating	66.5	70.1	74.2	89.4
Malicious	55.2	58.9	61.7	82.5

This metric specifies as per table 7, the cyclic consistency of chosen routing paths for time instance sets. The reliable path stability of the proposed model is due to the predictive congestion forecast from DL TRAP and reinforcement learning tuning from the REIN ACT Sets. The permanence of routing ensures all possible overhead reductions and efficient network convergence vis-a-vis mobility and attacks.

RESEARCH ARTICLE

Table 7 Routing Path Stability Index over 300s Simulation

Method	Stability Score
Method [3]	0.71
Method [8]	0.76
Method [25]	0.74
Proposed Model	0.89

It is clearly shown from the comparative analysis across these six performance tables that the proposed model offers a singular and better solution-integration of deep learning, federated cryptography, trust inference, and quantum safe routing process. This kind of update has maintained across heterogeneous operation conditions including variable energy profiles, attack behaviors, trust dynamics, and traffic intensities progressive analysis.

4.1. Validation and Impact Analysis

Across tables 2 to 7 along with figure 4 & figure 5, results of this integrated approach were presented, demonstrating definite performance advantages compared to traditional approaches in the Quality of Service (QoS) and security dimensions for the process. Attack classification accuracy across four major categories in the NSL-KDD dataset is presented in Table 2 for the process. The proposed model achieved an overall classification accuracy of 93.5%, much higher than Method [3], Method [8], and Method [25], which achieved 78.6%, 80.4%, and 81.5% respectively during the process.

Most significant performance improvements were recorded in the R2L and U2R classes, which are conventionally difficult to identify due to their sparse representation, indicating the effectiveness of XGBoost-based multi-class classification through the REIN ACT module contextually enhanced by its real-time feedback from the Q-learning rerouting engine. In real-time on-scene situations, this means that the network can detect very subtle intrusions with high accuracy and respond through dynamic traffic adaptation, minimizing possible damage from complex and stealthy attacks.

Table 3 further seconds the capability of the model in terms of handling variable traffic loads with low latency. In the high traffic environment, latency for the proposed model is brought down to 41.1 ms against 78.4 ms, 82.2 ms, and 85.1 ms for other baseline methods, thanks to the DL TRAP module utilizing CNN-based traffic prediction to proactively adjust routing paths. This kind of latency reduction is critical in real-world applications such as mobile vehicular or tactical wireless networks in fulfilling the requirements of real-time responsiveness, especially in safety-critical applications where milliseconds of delay might affect decision-making or situational awareness.

The first places will be Table 4 and Table 5 in terms of cryptographic efficiency. Table 4 illustrates the scenario for the encryption delay for 2048-bit RSA being reduced on the proposed system to 19.2 milliseconds, while other methods were above 36 milliseconds. Table 5 adds to this by showing that energy consumption is reduced by 40-50% across high, mid-high, and mid-low edge nodes. These results can be attributed to the dual-stage optimization in FED EARN (which offloads computation based on node energy availability) and in CRYPT GRAN (which adjusts key lengths based on how trustworthy a node is). This potentially raises quite a lot of lifetime in terms of nodes because, in real-world edge computing environments where battery operation is crucial, such reduction in encryption delay and energy usage assists in bottleneck reduction in processing as well as continuity in communications that are secure for the process.

Trust accuracy is addressed in Table 6, which shows that the proposed model proved most reliable in identifying malicious and fluctuating nodes than all their baselines. With trust score accuracy of 96.3% for the cooperative nodes and 82.5% for malicious nodes, trust-based encryption modulation in CRYPT GRAN and elastic propagation through Dempster-Shafer theory in Q EDRT turns highly effective. This is a very important feature of tactical or disaster recovery networks where trust conditions change very dynamically, such that automated systems have to be able to harden or relax encryption policies in virtually real time to maintain network security with efficient communication.
At last, this item shows a clear ascent in routing path stability measured at 0.89 against ~0.74 of the baselines. It is this ability of the model to present consistent routing decisions that will come up invariably within mobile ad hoc environments. High path stability minimizes overhead to a route computation and reduces packet loss due to route failures, leading to a resilient, robust network. Collectively, the analysis from these tables confirms that the proposed model not only improves performance under controlled simulations, but also provides well practical benefits for real time, high Variability wireless network deployments.

4.2. Validation Using Hyperparameter and Deviation of Model's Metric Analysis

Evaluation of the integrated model was done using performance analysis taking into consideration the statistical analysis of essential KPIs- attack classification accuracy, network latency, encryption delay, consumption energy, trust score accuracy, and routing stability- over several independent runs of the experiment. Each experiment was conducted 20 times using different random seeds and node mobility patterns for robustness of the results and generalizability. The expected value (average) and variance (standard deviation squared) were computed for each performance metric to check both the central tendency as well

RESEARCH ARTICLE

as the consistency. For instance, attack classification accuracy mean for the proposed model stood at 93.5%, with variance at 0.0043 while Method [25] had mean scores of 81.5%, with a variance of 0.0079, which indicates an improvement, not only of overall performance, but also greater stability under varying conditions. The proposed model under the high traffic conditions had mean latency as 41.1 ms with variance at 5.3 ms² while method [3] had a mean of 78.4 ms with a variance of 14.6 ms², showing how much better and adaptive DL TRAP is during real-time routing. A one-way ANOVA test was performed with the p-values for classification accuracy, latency, encryption delay, and trust score accuracy all less than 0.01, to confirm that the observed improvements were statistically significant at the 99% confidence level. The subsequent post hoc pairwise Tukey HSD test revealed that the proposed model performed significantly better than individual Method [3], Method [8], and Method [25] in all six performance indicators, with p values well below the 0.05 threshold. Hence these statistical tests were significant in concluding that the improved phenomenon was due to actual innovations in architecture and data flow across the integrated modules rather than random fluctuations.

The choice of Method [3], Method [8], and Method [25] as baseline references arises from the established roles that these methods have played in addressing the sub-domains that the proposed system targets, respectively. Method [3] represents a classical QoS-aware routing protocol which utilizes load-based metrics but is unable to be integrated with any real-time predictive models or security components. It is used in the evaluation of latency and routing stability. Method [8] actually uses a federated learning-based security protocol that provides decentralized authentication and encryption; however, it does not provide any real-time adaptability, energy-aware cryptography, and delegation sets. Thus, it is a useful baseline for encryption delay and edge energy performance. Method [25] is concerned with trust-based routing and modulation of the cryptographic depth, which makes Method [25] ideal for use in benchmarking trust accuracy sets and attack resilience sets. Collectively, these references cover the main axes of optimization- QoS, cryptography, and trust- into a unified framework process that the model proposed is to integrate. The variance profiles across the performance indicators further display the architectural merits of the proposed system. For example, the encryption delay for 2048-bit RSA in the proposed model had a standard deviation of only 2.4 ms compared to 6.3 ms for Method [8], thus proving that FED EARN balances load consistently. The differences in variance for trust score accuracy concerning malicious nodes were also significant, having 0.0061 for the new model instead of the 0.0132 for Method [25]. This is due to the stability of the Bayesian updates made by CRYPT GRAN and Dempster-Shafer-based trust propagation presented by Q EDRT. Altogether, lower means and variance in critical metrics, aside from confirming performance advantages, promise operational reliability within different environmental conditions and adversarial action sets. In summary, the statistical analysis yields the findings that the said system does outperform in reliability and high-performing wireless network behavior in multiple operational dimensions for the process. The reference methods provide a rigorous and meaningful baseline comparison, ensuring the observed gains are situated in the broader context of established research in wireless QoS, federated security, and trust-aware systems. These results illustrate how the integrated system could redundantly optimize performance while simultaneously enhancing security, with definite statistical significance sets.

5. CONCLUSION

A multi-layered integrated framework presented in this paper works to address dual challenges of security and QoS optimization in wireless networks via five tightly coupled modules: DL TRAP, FED EARN, CRYPT GRAN, REIN ACT, and Q EDRT. This system employs predictive deep learning for congestion forecasting, federated edge energy-aware encryption, trust-informed cryptographic key scaling, reinforcement-driven attack mitigation, and quantum-resistant trust propagation. Through extensive NS-3 simulation and analysis on NSL-KDD and synthetic contextual datasets, the proposed model proved its superiority across all major criteria, where principally under attack classification; it reached an accuracy of 93.5%, with huge margins in detecting rare attack classes as R2L (92.3%) and U2R (88.9%). The latency under high-load conditions was improved from 85.1 ms (Method [25]) to 41.1 ms, a strong indication of the effectiveness of congestion prediction and adaptive routing. Encryption delay for 2048 bits RSA operations was cut almost in half, from 36.8 ms to 19.2 ms, while edge-level energy consumption during encryption plummeted at least 50% in supporting the federated offloading mechanism. Moreover, trust score accuracy was 96.3% for cooperative nodes and 82.5% for malicious ones, thereby ensuring that trust-based dynamic encryption and routing were effectively operated in real-time. Routing stability also showed a pronounced improvement to a value of 0.89 vis-à-vis 0.74 in baseline models. Taken together, these findings establish that not only does the proposed system improve network performance, but it provides also resilient and robust context-aware security features in a changing wireless environment for different use case sets. Although the current framework integrates deep learning, federated encryption, trust modeling, and post-quantum cryptography, there are still quite a few paths to advance this work process. One such path could be the expansion of DL TRAP into a self-attention-based transformer architecture for capturing long-term temporal dependencies in network traffic, which may additionally enhance congestion forecasting accuracy in highly fluctuating

RESEARCH ARTICLE

environments. In similar spirit, broadening FED EARN to include other lightweight cryptographic primitives with elliptic curve-based homomorphic encryption or lattice-based fully homomorphic encryption (FHE) would improve scalability in ultra-constrained IoT devices. Trust computation in CRYPT GRAN and Q EDRT may be enriched by more contextual multi-modal sensor data (mobility, energy trend, GPS metadata) for better granularity and more real-world intuition of trust scores. Furthermore, the Q-learning engine implemented in REIN ACT could be upgraded to a deep reinforcement learning module for supporting continuous state-action representations in more complex topologies. Last, an extension of the current testbed to enable cross-domain federated training, i.e., the collaborative training by edge devices of trust and traffic models while avoiding centralized data, can improve both privacy and robustness against data heterogeneity and adversarial noise.

REFERENCES

[1] Priya, S. S., V(i,j)ayabhasker, R., & Rajaram, A. (2025). Advanced Security and Efficiency Framework for Mobile Ad Hoc Networks Using Adaptive Clustering and Optimization Techniques. Journal of Electrical Engineering & Technology, 20(3), 1815-1826. https://doi.org/10.1007/s42835-024-02119-9.

[2] Dixit, S., & Qureshi, S. (2025). Security-aware, Red fox optimization-based cluster-based routing in wireless sensor network. Peer-to-Peer Networking and Applications, 18(3). https://doi.org/10.1007/s12083-025-01951-8.

[3] Kamboj, A. K., Jindal, P., & Verma, P. (2023). Reinforcement learning-based secure joint relay and jammer selection in dual Hop wireless networks. The Journal of Supercomputing, 80(2), 2660-2680. https://doi.org/10.1007/s11227-023-05575-8.

[4] Kumar, N., & Sharma, S. (2024). PathGuard: Trustworthy Routing for Sustainable and Secure IoT-WSN Networks. Wireless Personal Communications, 136(1), 469-487. https://doi.org/10.1007/s11277-024-11289-8.

[5] Surla, G., & Lakshmi, R. (2023). RETRACTED ARTICLE: Design and evaluation of novel hybrid quantum resistant cryptographic system for enhancing security in wireless body sensor networks. Optical and Quantum Electronics, 55(14). https://doi.org/10.1007/s11082-023-05518-w.

[6] Kalpana, A. V., Geetha, A. V., Jagadeesh, M. S., & Shobana, J. (2024). Secure 3D: Secure and Energy Efficient Localization in 3D Environment using Wireless Sensor Networks. Wireless Personal Communications, 136(3), 1375-1402. https://doi.org/10.1007/s11277-024-11290-1.

[7] D, U. S. R., R, S., A, B., D, M., & Pellakuri, V. (2024). Enhanced lion swarm optimization and elliptic curve cryptography scheme for secure cluster head selection and malware detection in IoT-WSN. Scientific Reports, 14(1). https://doi.org/10.1038/s41598-024-81038-1.

[8] Beula, G. S., & Franklin, S. W. (2024). SCMABC Algorithm-based routing for secure and efficient data transmission in smart grid AMI networks. Peer-to-Peer Networking and Applications, 17(6), 4110-4130. https://doi.org/10.1007/s12083-024-01773-0.

[9] Murthy, M. Y. B., Koteswararao, A., & Babu, M. S. (2024). Hybrid moth flame-shark smell optimization-based secure wireless communications for IoT applications. International Journal of Intelligent Robotics and Applications. https://doi.org/10.1007/s41315-024-00367-6.

[10] Rahimi, A., Jafari Shahbazzadeh, M., & Khatibi, A. (2025). An adaptive intelligent thermal-aware routing protocol for wireless body area networks. Journal of Cloud Computing, 14(1). https://doi.org/10.1186/s13677-025-00755-8.

[11] Mahajan, S., Srideviponmalar, P., Harikrishnan, R., & Kotecha, K. (2025). Reinforcement Learning Based Congestion Control Technique for Wireless Mesh Networks. International Journal of Networked and Distributed Computing, 13(1). https://doi.org/10.1007/s44227-025-00061-4.

[12] Zing, Y., Zhao, N. Routing revolution: strategic applications of meta-heuristic AI in wireless sensor networks—a comprehensive survey. Multimed Tools Appl 84, 44605–44646 (2025). https://doi.org/10.1007/s11042-025-20843-w.

[13] Qian, X. (2025). DMKESR: Dynamic Multi-Parameter Key Exchange Enhanced Secure Routing for Wireless Mesh Networks. Journal of The Institution of Engineers (India): Series. https://doi.org/10.1007/s40031-025-01223-2.

[14] Kumar, M., Goyal, N., Qaisi, R.M.A. et al. Joint trust-based detection and signature-based authentication technique for secure localization in underwater wireless sensor network. Multimed Tools Appl 84, 37845–37864 (2025). https://doi.org/10.1007/s11042-025-20683-8.

[15] Yesodha, K., Krishnamurthy, M., Thangaramya, K., & Kannan, A. (2024). Elliptic curve encryption-based energy-efficient secured ACO routing protocol for wireless sensor networks. The Journal of Supercomputing, 80(13), 18866-18899. https://doi.org/10.1007/s11227-024-06235-1.

[16] Bai, Y., Xue, Y., Meng, J. et al. TSRP: A Novel Trust-Based and Energy-Aware Secure Routing Protocol for Resource-Constrained Wireless Sensor Networks. J. Inst. Eng. India Ser. B 106, 1401–1413 (2025). https://doi.org/10.1007/s40031-024-01158-0.

[17] Gharaei, N., & Alabdali, A. M. (2025). Secure and energy-efficient inter- and intra-cluster optimization scheme for smart cities using UAV-assisted wireless sensor networks. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-88532-0.

[18] Iqbal, S., & Sujatha, B. R. (2024). Secure authentication and key management based on hierarchical enhanced identity based digital signature in heterogeneous wireless sensor network. Wireless Networks, 31(1), 127-147. https://doi.org/10.1007/s11276-024-03745-x.

[19] Selvi, M., Santhosh Kumar, S. V. N., Thangaramya, K., & Abdul Gaffar, H. (2025). Energy efficient trust aware secure routing algorithm with attribute based encryption for wireless sensor networks. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-03558-8.

[20] Shah, S., Sarwar, N., Salam, A., Amin, F., Ullah, F., Khan, A., de la Torre, I., Villar, M. G., & Garay, H. (2025). A flexible and lightweight signcryption scheme for underwater wireless sensor networks. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-95836-8.

[21] Feng, C., Jumaah Al-Nussairi, A. K., Chyad, M. H., Sawaran Singh, N. S., Yu, J., & Farhadi, A. (2025). AI powered blockchain framework for predictive temperature control in smart homes using wireless sensor networks and timestamp shifted analysis. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-03146-w.

[22] Soundararajan, S., Nithya, B., Nithya, N., & Vignesh, T. (2024). Block chain espoused adaptive multi-scale dual attention network with quaternion fractional order meixner moments encryption for cyber security in wireless communication network. Wireless Networks, 30(4), 2439-2455. https://doi.org/10.1007/s11276-024-03674-9.

[23] David, P.F., Kothandapani, S.D. & Pugalendhi, G.K. Crayfish optimization-based secure encryption of medical images with 7D hyperchaotic maps. Int. J. Mach. Learn. & Cyber. 16, 7369–7389 (2025). https://doi.org/10.1007/s13042-025-02660-7.

[24] Ramamoorthy, R. (2024). An Enhanced Location-Aided Ant Colony Routing for Secure Communication in Vehicular Ad Hoc Networks. Human-Centric Intelligent Systems, 4(1), 25-52. https://doi.org/10.1007/s44230-023-00059-7.

[25] Dinesh, K., & Santhosh Kumar, S. V. N. (2024). HBO-SROA: Honey Badger optimization based clustering with secured remora optimization based routing algorithm in wireless sensor networks. Peer-to-Peer Networking and Applications, 17(5), 2609-2636. https://doi.org/10.1007/s12083-024-01708-9.

RESEARCH ARTICLE

Authors

Minal Ghute is a research scholar in electronics engineering department and faculty of electronics and telecommunication engineering department of Yeshwantrao Chavan College of engineering, Nagpur, India. She is working in the area of wireless networking and its security. Also, expert in signal processing. She published no. of papers in various international conferences and journals. More than 100 citations are there in account.

Dr. Yogesh Suryawanshi completed his PhD in Wireless Communication and network security. He is working in electronics engineering department of Yeshwantrao Chavan College of engineering. He is expert in wireless communication, Internet of things, cryptography and embedded system. More than 100 citations are in his account. He has published papers in various international conferences and journals. Worked as reviewer of IEEE conferences.

Dr. Shubhangi Ghate Received her Ph. D. in Electrical and Electronics engg. from Sandip University, Nashik. Currently working as Assistant Professor in department of Computer Science and Engineering, Ramrao Adik Institute of Technology, D. Y. Patil Deemed to be University, Nerul Navi-Mumbai, India. She is having total teaching experience of 20 years. She has an author of more than 25 research articles and papers in various international journals and conferences; her four patents are published. She has received award for excellence in Research and Development in academic year 2011-2012 and 2012-13. She is the Chairman of syllabus Setting and paper setting committee for UG in Mumbai and member of syllabus Setting and paper setting committee for UG DYPU. She has reviewed research papers in international journals and Conferences; she has also served as TPC member and session chairs in various international conferences. Her area of interest includes Underwater Image Processing, Big Data Analytics, Database Management System, Internet of Thing (IoT), Antenna Design, Microwave and Radar Engg. She is a life member of professional society ISTE. She strongly believes in innovation and creativity.

How to cite this article:

Minal Ghute, Yogesh Suryawanshi, Shubhangi Ghate, “Integrated Deep Learning and Cryptographic Optimization for Secure, Adaptive and Quantum Resilient Wireless Networks”, International Journal of Computer Networks and Applications (IJCNA), 13(1), PP: 1-16, 2026, DOI: 10.22247/ijcna/2026/01.