The Scientific Temper
SEPTEMBER 2026 Vol. 17 (9): 6872-6896
ISSN: 0976-8653, E-ISSN: 2231-6396
DOI: 10.58414/SCIENTIFICTEMPER.2026.17.9.2541
A WEB OF SCIENCE JOURNAL

RESEARCH ARTICLE

Secure Constrained Application Protocol Communication and Adaptive Attack Detection with Reinforcement Learning and Hermitian Cryptography

*[1,2]RADHIKA PATEL · [3]AMIT NAYAK

[1]*Assistant Professor, Department of Information Technology, Devang Patel Institute of Advance Technology and Research, Faculty of Technology & Engineering, Charotar University of Science and Technology, Changa 388421, Anand, Gujarat, India.*

[2]*Department of Computer Engineering, Chandubhai S. Patel Institute of Technology, Faculty of Technology & Engineering, Charotar University of Science and Technology, Changa 388421, Anand, Gujarat, India. radhikapatel.it@charusat.ac.in*

[3]*Head of the Department, Computer Science & Engineering, Devang Patel Institute of Advance Technology and Research, Faculty of Technology & Engineering, Charotar University of Science and Technology, Changa 388421, Anand, Gujarat, India. amitnayak.it@charusat.ac.in*

Corresponding author: radhikapatel.it@charusat.ac.in

ABSTRACT

In resource-constrained Internet of Things (IoT) environments, application-layer protocols such as the Constrained Application Protocol (CoAP) provide lightweight and efficient communication mechanisms. Increasing interconnectivity introduces growing risks of data breaches and susceptibility to Distributed Denial of Service (DDoS) attacks. Traditional public key encryption schemes impose significant computational overhead and exhibit vulnerability to emerging quantum computing threats. A hybrid security framework is introduced to address such challenges by combining lightweight encryption with intelligent threat detection. Initial processing begins with min-max normalization of IoT data, enhancing computational stability and improving feature consistency. The Hybrid Quantum Hermitian-based Cryptographic System (HQHCS) follows, using quantum random number generation and Hermitian matrix operations to generate dynamic, non-repeating session keys. This cryptographic design supports fast, symmetric encryption and strengthens resilience against classical and quantum attacks. To detect malicious activity, a Reinforcement-based Deep Q-Learning (RDQL) classifier models intrusion recognition as a Markov decision process. By leveraging reward-based adaptation, the model learns to distinguish evolving DDoS patterns with minimal supervision. Implementation is carried out in MATLAB, and evaluation is performed across five established IoT security datasets: CIC-DDoS2019, UNSW-NB15, BoT-IoT, CIC-IDS2017, and CSE-CIC-IDS2018. Results demonstrate encryption and decryption times of 10 and 12 seconds, respectively, for 500MB data files, accompanied by an energy usage of 43.82 joules. RDQL consistently surpasses 99% accuracy in classifying malicious traffic. An ablation analysis verifies performance consistency across various attack scenarios. This hybrid framework ensures real-time confidentiality, energy efficiency, and robustness for CoAP-based IoT deployments through the integration of quantum-resilient encryption and dynamic intrusion detection.

Keywords *Constrained application protocol; Internet of things; Intrusion detection system; Reinforcement learning; Distributed denial of service*

Received: 5th September, 2026 **Accepted: 7th September, 2026** **Published: 28th September, 2026**

INTRODUCTION

The IoT becomes a paradigm of technology that allows many smart devices to communicate with each other and share data seamlessly, locally or globally, without human intervention. Today, embedded sensors (including temperature monitors, gas detectors, motion sensors, surveillance cameras, etc.) are still being rapidly deployed in modern environments. IoT has penetrated into various fields and by 2025, it is expected that more than 75 billion devices are active (Singh et al., 2024; Yalli et al., 2024). The IoT system is generally divided into three layers: perception layer responsible for collecting data from the physical world and sensing it (Hasan & Patle, 2024); network layer for transmitting the collected data between the interconnected devices (Shahin et al., 2024); and application layer for processing the data and providing intelligent services to the end-users (Zahra et al., 2024). Efficient communication is essential in such multi-layered architectures, especially when considering the power, memory and processing constraints of most IoT devices.

Communication protocols are still essential for enabling smooth data transfer in resource-limited IoT applications. To enable effective network data transfer, multiple communication protocols have been incorporated in IoT systems. Among all the protocols, CoAP is a lightweight application layer protocol based on User Datagram Protocol (UDP) (Sarkar et al., 2025; Khalil et al., 2025). It is mostly used for simple devices and networks with minimal overhead, simple operation, and asynchronous messages. It is also lightweight, unlike the complex Message Queuing Telemetry Transport (MQTT) and Advanced Message Queuing Protocol (AMQP), making it suitable for battery-powered systems and resource-constrained environments. However, CoAP is very susceptible to cyber attacks, particularly Denial of Service (DoS) attacks (Anna et al., 2024).

A variant of DoS is an amplification attack, in which an attacker sends a small spoofed request to a CoAP server using the victim's IP address, causing the server to reply with a much larger payload to the victim. This leads to unwanted traffic surges that make services inaccessible. These attacks take advantage of the statelessness of UDP and the open access properties of CoAP, which makes real-time detection and mitigation difficult in IoT environments. As the world becomes increasingly digital, security becomes a critical element to protect personal and organizational information, particularly in the age of IoT and machine-to-machine communication. With the rise in frequency and sophistication of cyberattacks, the security of IoT devices is becoming increasingly important to prevent data breaches, blackmail, and unauthorized access, underscoring the need for robust cybersecurity measures in interconnected systems (Francis et al., 2024).

The most common way to secure CoAP communication with encryption and authentication is still Datagram Transport Layer Security (DTLS). Each CoAP message is wrapped in a secure record, which reduces the risk of eavesdropping and tampering. But DTLS requires a complex handshake process and computationally heavy operations, making it inappropriate for low-power, resource-constrained IoT deployments (Felix, 2024). The latency, energy consumption, and compatibility issues are the reasons, DTLS is not widely used in real-world IoT applications.

To address these challenges, this research seeks to investigate the nature and impact of DoS amplification attacks against CoAP, classify its variants, and categorize behavioural patterns. To overcome these challenges, this research introduces a lightweight and adaptive security framework for CoAP-based IoT environments. The framework aims to provide collaborative protection of resource-constrained communications and detect emerging cyber threats while preserving computational efficiency.

Contributions

The contributions of the research are ,

- A HQHCS framework is developed for lightweight CoAP communication. HQHCS combines simulated quantum-random bit generation, entropy extraction, session-key derivation, and Hermitian matrix transformations to generate dynamically refreshed encryption subkeys while limiting computational overhead.

- A RDQL model is developed for adaptive multi-class cyberattack detection. The detection process is formulated as a Markov Decision Process (MDP), in which network observations constitute states, attack labels constitute actions, and classification performance determines the reward.

- HQHCS and RDQL are integrated into a multi-layer CoAP security framework, enabling confidentiality and adaptive attack detection within a common security architecture. HQHCS protects communication traffic, whereas RDQL identifies malicious traffic and supports mitigation decisions.

- The framework is experimentally evaluated using five benchmark intrusion-

detection datasets, with separate analyses of encryption efficiency, network performance, attack classification, and component-level ablation.

LITERATURE REVIEW

Research on IoT security is oriented toward lightweight cryptography and intelligent threat detection. The importance of Deep Learning (DL) and hybrid frameworks for classification and countering emerging attacks is increasing, with a focus on adaptive, integrated, and low-overhead solutions to address modern IoT challenges.

Lightweight Cryptography and Secure Communication in IoT Systems

In recent years, a large number of possibilities for lightweight encryption and secure communication models have emerged for constrained IoT environments. Aljaedi et al. (2025) proposed a much more powerful encryption scheme based on Quantum methods and chaotic maps with minimal computational complexity. The method employed the Improved Butterfly Optimization Algorithm (Quantum-IBOA) to optimize the encryption parameters to ensure that the algorithm was efficient even on the most limited devices. Arias-Jimenez et al. (2025) came up with a solution that combined Ephemeral Diffie–Hellman Over COSE (EDHOC) with the Static Context Header Compression (SCHC) protocol to optimize energy efficiency in constrained IoT environments. The integration provided session keys exchange with virtually no communication overhead. This was suitable for energy-constrained devices in smart agriculture and smart cities, ensuring security while minimizing energy consumption. Sezer & Akleylek (2024) designed and implemented a secure Privacy-Preserving Lattice-Based Blockchain (PPLBB) platform for protecting the communications in Internet of Medical Things (IoMT). The solution uses lattice cryptography in the blockchain framework to provide quantum-resistant privacy, while computational efficiency was upheld. Kalphana et al. (2024) proposed an advanced detection mechanism for Android ransomware through a Squirrel Search Optimization (SSO) optimized DL-based classifier with Hybrid Homomorphic Elliptic Curve Cryptography and Blowfish cryptography (HHECCB). The framework combines symmetric and asymmetric encryption schemes to protect the confidentiality of the data, while DL facilitates the correct predictions of attack patterns, granting dual protection to mobile environments.

Deep Learning and Hybrid Security Frameworks for IoT Attack Classification and Mitigation

With the recent advances in DL, attack classification models have become significantly powerful in IoT security setups. Sheela et al. (2024) improved wireless sensor network-based transmission with Reinforcement Learning and Homomorphic Encryption (RLHE) by employing Reinforcement Learning (RL) to enable adaptive routing decisions, while Homomorphic Encryption (HE) allowed encrypted computations to maintain data privacy. Further, Gajendran et al. (2024) introduced a blockchain-assisted Elliptic curve Cryptography- based Federated Q-Learning (ECFQL) framework to provide light encryption along with distributed learning on healthcare nodes. Kumar & Keshri (2024) introduced an optimization-driven adaptive security model to counter DDoS attacks in IoT, with tuning mechanisms incorporating optimization methods to dynamically enhance the defense. In contemporary literature, Razaq et al. (2024) proposed a Deep RL-based Physical Layer Security (DRL-PLS) framework for dynamic allocation of communication resources and securing parameter selection for IoMT environments. Shaik & Yamarthi (2024) proposed a Secret Elliptic Curve–Bidirectional Gated Recurrent Unit-Residual Network (SEC-BiGRU-ResNet) framework, integrated with Amended Merkle Tree approach (AmerT), Secret Elliptic curve cryptography (SEllC), blockchain framework Interplanetary File System (IPFS), and Attention Bidirectional Gated unit assisted Residual network (Att-BGR), to secure the transmission of IoT data and enhance classification accuracies through deep residual learning-based blockchain. A Federated Bayesian Optimization XGBoost (FBOXGBoost) framework was introduced by Guembe et al. (2024) to improve cyberattack detection in IoMT systems. This model utilizes multimodal sensory data such as network flow and patient vitals, keeping the data private using the FL approach, and detects newly evolved threat patterns without compromising any medical data. In parallel, Hizal et al. (2024) developed a DL-based Intrusion Detection System (DL-IDS), that integrates Deep Neural Network (DNN), Convolutional Neural Network (CNN) and Long Short-Term Memory (LSTM) for IoT-DDoS attack detection, using multilayer neural structures to capture complex traffic variations and enhance detection accuracy.

Recent research has demonstrated the effectiveness of RL and optimization techniques for adaptive decision-making under complex and uncertain operating conditions. Li et al. (2026) proposed a Robust Optimization-based

Cargo vessel, Research vessel, and Experiment allocation (ROCREA) framework incorporating a Multi-distribution Adaptive Hybrid Differential Evolution (MAHDE) algorithm to improve decision stability under uncertainty. This demonstrates the importance of robust optimization when system conditions vary dynamically. Li et al. (2026) developed a Stochastic Programming model for Berth And Experiment Allocation (SPBAE) framework incorporating Proximal Crossover Bottom-left Weighted Average Algorithm (PCBWAA). optimization, demonstrating the applicability of learning-based strategies to complex decision-making under uncertain conditions. Furthermore, Li et al. (2026) formulated multi-objective joint scheduling model to integrate Berth Allocation, Quay Crane Assignment, and Experiment Arrangement (BCAEA). Integrated Q-Learning with Enhanced Particle Swarm Optimization(QLEPSO) through adaptive strategy selection and parameter control, demonstrating that RL algorithms enhance optimization performance in large-scale and dynamic decision problems. Although these research focus on marine-port scheduling rather than IoT security, their underlying principles of adaptive learning, uncertainty handling, and optimization-assisted decision-making were relevant to dynamic IoT environments. In the proposed framework, these principles motivate the use of RDQL for adaptive traffic-state analysis and attack classification under changing network conditions. Table 1 provides comparative analysis of existing methods with the proposed model.

Table 1: Comparative analysis of existing methods and proposed HQHCS-RDQL

Existing method	Cryptographic approach	Learning / optimization approach	Main contribution	Limitation	Key improvements in proposed HQHCS-RDQL
RLHE	HE and quantum-safe key exchange	RL	Secure WSN transmission, encrypted model aggregation, and RL-based decision-making	Designed mainly for WSN privacy and distributed learning; does not target CoAP attack detection	HQHCS provides lightweight CoAP data encryption, while RDQL performs adaptive attack detection rather than RL-based model/client optimization
PPLBB	Dilithium lattice-based signatures and Zero-Knowledge Proofs (ZKP)	—	Privacy, authentication, integrity, and blockchain security for CoAP-based IoMT	Relies on blockchain and focuses primarily on authentication, integrity, and privacy	HQHCS provides lightweight Hermitian-based confidentiality without blockchain, while RDQL adds adaptive intrusion detection
ECFQL	Extended Elliptic Curve Cryptography (ECC)	Federated Q-Learning	Secure distributed IoMT learning with blockchain-based update validation	Requires Federated Learning (FL) and blockchain infrastructure; healthcare-oriented	HQHCS-RDQL avoids federated/blockchain infrastructure and directly combines CoAP encryption with RL-based attack detection
DRL-PLS	Physical Layer Security (PLS)	DRL	Secure IoMT transmission through device selection, beamforming, and artificial noise	Protects mainly against physical-layer eavesdropping; no cryptographic CoAP protection	HQHCS provides cryptographic confidentiality, while RDQL detects network attacks rather than optimizing physical-layer resources
SEC-BiGRU-ResNet	AMerT, SEIIC, IPFS	Att-BGR	IoT data encryption, integrity, decentralized storage, and attack classification	Blockchain/IPFS introduces additional infrastructure and storage overhead	HQHCS-RDQL provides lightweight communication security without IPFS and replaces conventional DL classification with adaptive RDQL

FBOXGBoost	No cryptographic mechanism provided; privacy was primarily addressed through FL by keeping raw data locally.	FL + Bayesian optimization + Extreme Gradient Boosting (XGBoost)	Enables privacy-preserving IoMT cyberattack detection using multimodal patient and network data without centralizing raw data.	Lacks integrated cryptographic protection and adaptive reinforcement-learning-based attack detection for resource-constrained CoAP-IoT environments.	Integrates lightweight cryptographic protection with adaptive RDQL-based attack detection for resource-constrained CoAP-IoT environments.
DL-IDS	—	DNN, CNN, LSTM	IoT DDoS detection and classification	Focuses on attack detection without communication encryption	HQHCS adds confidentiality and RDQL enables adaptive security decisions beyond conventional DL classification
EDHOC-SCHC	EDHOC	—	Lightweight key establishment, packet compression, and energy-efficient CoAP/ Low-Power Wide-Area Network (LPWAN) communication	Improves secure communication efficiency but does not perform attack detection	HQHCS extends communication protection with Hermitian-based encryption, while RDQL provides adaptive intrusion detection
HHECCB	HHECC + Blowfish	SSO + DL	Android ransomware detection and cloud-data protection	Designed for Android malware rather than CoAP network security	HQHCS-RDQL is specifically oriented toward constrained CoAP-IoT communication and network attack detection
ROCREA	Not focused on cryptographic security	Robust optimization with MAHDE under uncertainty	Provides robust decision-making for complex scheduling under uncertain and congested conditions	Focuses on marine-port scheduling and does not address IoT security, cryptographic protection, or adaptive intrusion detection	Extends robust decision-making under uncertainty from scheduling to adaptive IoT attack detection, while additionally providing cryptographic protection for CoAP communication
SPBAE-PCBWAA	Not focused on cryptographic security	Stochastic programming with Sample Average Approximation (SAA) and Proximal Policy Optimization (PPO)	Improves resource allocation and scheduling under uncertainty	Does not address secure CoAP communication or real-time IoT attack detection	Applies adaptive learning principles to dynamic network traffic and DDoS detection rather than resource allocation, while integrating lightweight cryptographic security.
BCAEA-QLEPSO	Not focused on cryptographic security	QLEPSO with adaptive parameter control	Demonstrates the effectiveness of combining RL and swarm optimization for complex decision-	Applies RL to port scheduling rather than cybersecurity and does not provide cryptographic protection or	Extends the use of Q-learning from optimization strategy selection to real-time security decision-making and attack classification, combined with an

			making	DDoS detection	independent cryptographic protection layer.

Research Gaps in Lightweight Cryptography and IoT Security

Existing research on lightweight encryption, DL, RL, and optimization demonstrates progress in IoT security; however, several challenges remain. These include scalable hybrid cryptography for real-time environments, balancing resource efficiency with encryption strength, adaptive detection of rapidly changing attacks, and the integration of complementary security mechanisms for heterogeneous IoT applications. Recent RL and optimization research further demonstrates effective decision-making under uncertainty, but mainly focuses on scheduling and resource allocation rather than CoAP security. Limited attention has therefore been given to integrating lightweight cryptographic protection with adaptive intrusion detection while maintaining computational efficiency in resource-constrained environments. To address these gaps, the proposed HQHCS-RDQL framework combines Hermitian-based cryptographic protection with RDQL-based adaptive attack detection, aiming to provide secure, efficient, scalable, and responsive security for CoAP-enabled IoT systems.

Problem Statement

With limited processing capability, IoT devices face difficulty in implementing cryptographic techniques that are both efficient and secure. For instance, CoAP protocols continue to be subjected to DoS amplification attacks that threaten the availability and reliability of IoT services. Cryptographic methods have high computational overheads and, in some situations, lack adaptability in identifying and combating new attack patterns in a real-time setting. A novel, lightweight, and adaptive solution is proposed, integrating RL-based detection with Hermitian-based lightweight cryptographic mechanisms. This framework aims to provide robust security, enhancing the performance, scalability, and longevity of IoT devices.

ROBUST SECURITY FRAMEWORKS FOR COAP UNDER DDOS THREATS

The suggested framework comes with a multi-layer resistant defence to ensure safe communication and smart attack detection in a CoAP-based IoT setting.

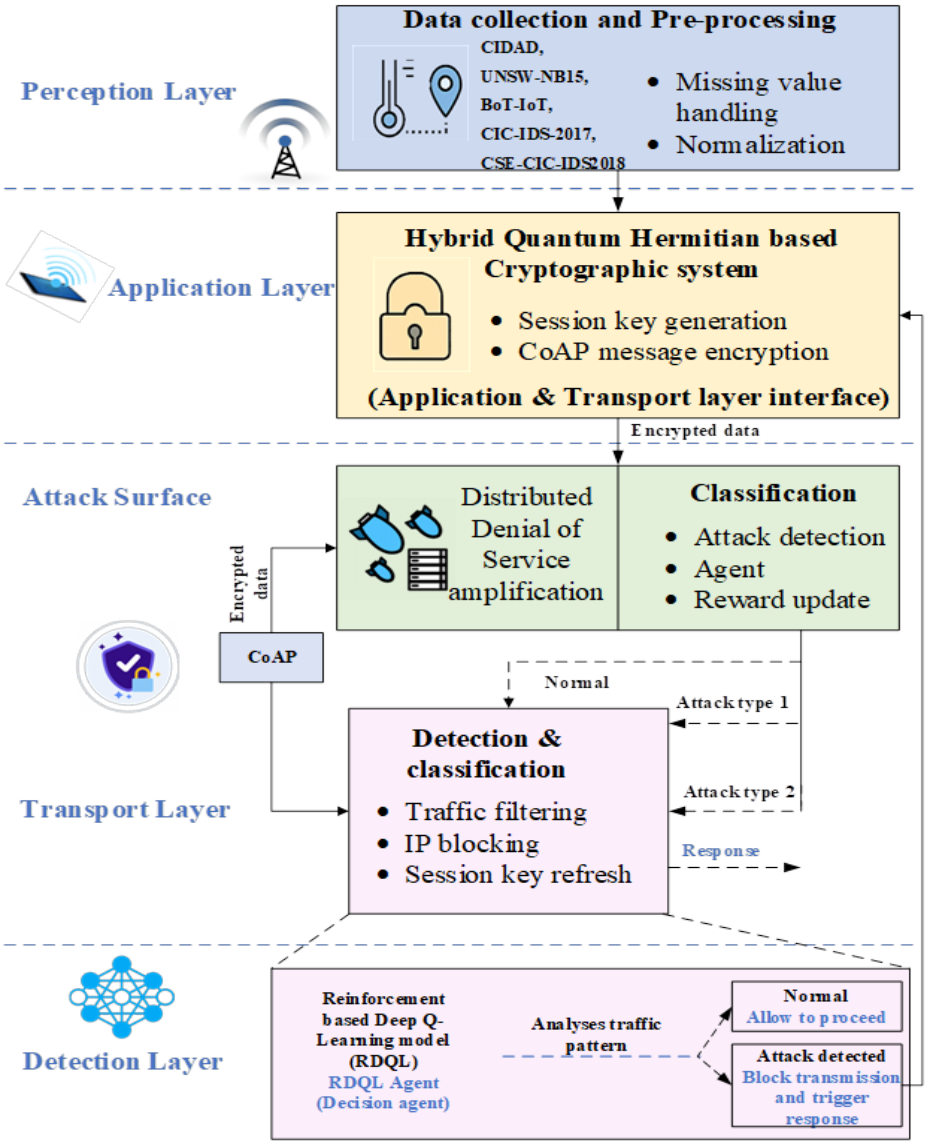


Fig. 1. Multi-layered system model for secure CoAP-based IoT communication and DDoS detection

The framework is split into four main layers: perception, application, transport, and detection. Real-time data are obtained from various IoT devices sourced from benchmark datasets, which are then sent over a secure CoAP channel, while communications between sensor nodes at the transport layer are encrypted through HQHCS.

To ensure proactive threat mitigation, multi-class DDoS attacks are detected and classified using an RL-based DL model. An RDQL agent acts as the decision-making engine, triggering appropriate responses such as session key regeneration or malicious traffic blocking. Each layer in this architecture plays a crucial role in achieving end-to-end security, adaptive intelligence, and communication robustness throughout the system lifecycle. Fig. 1 depicts a layered defense framework integrating HQHCS encryption and RDQL-based DDoS detection to ensure secure communication in CoAP-based IoT environments.

Dataset Description

The experimental evaluation uses five publicly available intrusion-detection datasets: CIC-DDoS2019, UNSW-NB15, BoT-IoT, CIC-IDS2017, and CSE-CIC-IDS2018. These datasets are selected to provide heterogeneous network-traffic patterns and to evaluate the generalization of RDQL across different intrusion environments. The datasets contain both benign and malicious traffic generated under different network and attack conditions.

For the proposed framework, the datasets are used as general-purpose intrusion benchmarks rather than as direct CoAP-amplification datasets. Each dataset is independently preprocessed to obtain the traffic features required by RDQL. Irrelevant attributes are

removed, the selected numerical features are normalized, and the resulting records are transformed into the 20-dimensional state representation used by the DQN. The original traffic labels are subsequently mapped to the four RDQL output categories: normal traffic, DDoS, spoofing, and malware, according to the attack characteristics represented in each dataset. Dataset-specific labels that do not correspond directly to these categories are grouped according to their closest attack type used by the proposed classification scheme.

The processed state vectors are then provided to RDQL for attack classification. This setup enables evaluation across heterogeneous datasets while maintaining a consistent input representation and classification space. The CoAP-specific aspect is provided by the proposed framework rather than by the datasets themselves: HQHCS is responsible for securing CoAP communication, whereas RDQL provides traffic classification and adaptive security decisions. Thus, the experimental results show the general attack-classification capability and cross-dataset applicability of RDQL, but do not claim that the chosen benchmark datasets directly reflect CoAP amplification traffic.

Data Refinement Process

The first step involves organizing the dataset and filling in missing data that affect the detection accuracy. Entries that are missing are replaced by the mean of the column, which is shown in Eqn. (1).

$$x_{new} = \frac{\sum x_i}{n} \tag{1}$$

where, x_{new} denotes the filled new value, $\sum x_i$ is the sum of the values in the column, n is the number of non-missing values in the column. This approach maintains consistency of data across the dataset, with each missing point representing the central tendency of the feature it represents. Then, to equalize the influence of the features and improve the processing speed, normalization is performed by min-max scaling, as expressed in Eqn.(2).

$$x_{scaled} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{2}$$

where, x_{scaled} is the normalized value, x is the value of the data point, $x_{\min}$ and $x_{\max}$ are the minimum and maximum values in the feature. This transformation maps all the feature values to a standard range between 0 and 1, which makes the features uniform and avoids domination by features with larger numerical scales. This cleaning, averaging and normalization process makes the dataset reliable and ready for accurate multi-class detection of DDoS amplification attacks in the subsequent phases (Rao et al., 2024).

Hybrid Quantum Hermitian-based Cryptographic System for Encryption

A secure and lightweight communication protocol is achieved by using a HQHCS, which provides strong session key exchange and CoAP message encryption in IoT environments. The system combines the concepts of quantum cryptography and Hermitian transformations to provide increased security and computational efficiency on unreliable networks like UDP. The stream of raw quantum bits is produced by a Quantum Random Number Generator (QRNG), as expressed in Eqn. (3).

$$\{b_i\}_{i=1}^{N} \tag{3}$$

where, b_i is the i^{th} bit generated from the quantum events and N is the total number of bits generated. Raw bits are inherently quantum random and unpredictable. To overcome minor biases due to device imperfections, a Von Neumann extractor is used by processing bits in pairs, yielding a bias-free random string R, which is used in cryptographic operations. A secure hash function is then used to generate the session key $K_{session}$, as shown in Eqn. (4).

$$K_{session} = Hash(R) \tag{4}$$

where, $K_{session}$ is the 256-bit session key used for encryption, R is the high-entropy quantum random string, $Hash(\cdot)$ denotes a cryptographic hash function ensuring uniform key distribution (Mansoor et al., 2024).

Hermitian-based transformations are used in the generation of subkeys to further strengthen security against quantum and classical attacks. New quantum randomness and Hermitian matrix operations are used in each round of encryption. The round subkey $K_i^{'}$ is computed using Eqn. (5).

$$K_i^{'} = H \cdot (K_i \oplus Q_i) \tag{5}$$

where, $K_i^{'}$ is the transformed subkey for the i^{th} encryption round, H is the Hermitian matrix operator satisfying $H = \hat{H}$, K_i is the classical subkey generated from $K_{session}$, Q_i is a 128-bit quantum random block injected per round, $\oplus$ denotes the bitwise XOR operation, $\cdot$ represents matrix multiplication.

The quantum random block Q_i blinds the round key, ensuring that even if partial information about K_i is leaked through side-channel attacks, the secrecy of Q_i upholds overall security. The Hermitian matrix H introduces a structured linear transformation, adding resilience against predictive key-scheduling attacks and preserving orthogonal properties beneficial for quantum-based cryptography (Vardhan et al., 2024).

By repeatedly refreshing subkeys using quantum randomness and Hermitian transformations, the HQHCS ensures both forward and backward secrecy. Even if a subkey $K_i^{'}$ is compromised, subsequent keys remain secure due to fresh quantum randomness, and previous keys remain protected under the irreversibility of Hermitian transformations and the unpredictability of QRNG outputs. HQHCS fortifies IoT communications by providing a lightweight yet robust encryption framework resistant to both classical cryptanalysis and quantum-enabled brute-force attacks.

The implementation configuration of the HQHCS is specified to ensure reproducibility. The Hermitian transformation employs a 4×4 matrix, constructed from a randomly generated complex matrix A^T and its conjugate transpose according to $H=\frac{A+A^T}{2}$. A MATLAB-based QRNG simulation generates a 128-bit random sequence per encryption block, which is processed using Von Neumann extraction, retaining the 01 and 10 bit pairs while discarding 00 and 11 pairs. The random sequence extracted is used for session-key generation and round-wise key diversification. It uses a 256-bit session key, a 128-bit quantum-random block, and hashes using SHA-256. The HQHCS is a 10-round encryption scheme, where the quantum-random block is used in each round. This configuration is kept the same for all experimental datasets to allow for consistent evaluation and reproducibility.

Reinforcement-based Deep Q-Learning for Multi-Class Cyberattack Classification

Although HQHCS provides strong encryption and secure data transmission, comprehensive cybersecurity requires the ability to detect and classify cyber threats in real-time. As network attacks in IoT and distributed systems increase in number, dynamic and intelligent detection mechanisms are necessary. An RDQL model is proposed for detecting DDoS attacks and multiple attack types with high precision. Deep Q-Learning (DQL) continuously learns from the changing attack patterns, minimizing false positives and improving overall network resilience through autonomous learning. This multi-class classification model, alongside HQHC encryption, ensures data security and threat prevention. RL plays a crucial role in automation and intelligence for detecting cyberattacks in large-scale IoT and network systems. Traditional methods rely on expert input, whereas DQL is designed to optimize through iterative learning automatically. It becomes a very useful tool to deal with large and high-dimensional datasets that represent modern-day cyber threats. With integration with DQL, the system is able to detect DDoS attacks accurately and distinguish between various types of attacks, thereby slightly shifting the IoT infrastructure towards a more secure domain. In addition, the framework eliminates the need for manual model tuning and data preprocessing, thus providing a flexible and efficient solution in dynamic attack scenarios in real time.

The selection of RDQL is motivated by the ability of RL to support adaptive decision-making under changing system conditions. Recent RL and optimization research have demonstrated the effectiveness of Q-learning, adaptive strategy selection, and uncertainty-aware optimization for complex decision-making problems. These principles are relevant to IoT security, where network traffic and attack patterns vary dynamically. Accordingly, RDQL is employed in the proposed framework to learn traffic-state representations and select appropriate attack classifications based on observed network conditions. Unlike optimization approaches primarily designed for scheduling and resource allocation, the proposed RDQL applies adaptive learning to intrusion detection in CoAP-based IoT environments. Its integration with HQHCS further enables the framework to address both secure communication and adaptive attack detection within a unified architecture.

- *Q-Learning Framework for Multi-Class Attack Detection*

The Q-Learning-based approach models the attack detection process as MDP, where the system learns an optimal attack classification strategy based on state-action-reward interactions. The model iteratively updates the Q-values to gradually approach the global optimal solution, thereby improving the classification accuracy over time.

1. **State Space** S**:** Represents the observed network conditions, such as packet sizes, traffic patterns, and protocol analysis. Such states are crucial for identifying the nature of an attack or determining whether it is normal

traffic.

2. **Action Space** A**:** The actions correspond to the classification decisions that the model makes. For instance:

Action 1: Classify as DDoS.

Action 2: Classify as spoofing.

Action 3: Classify as malware.

Action 4: Classify as normal traffic.

3. **Reward Function** R : The reward R_t is defined to incentivize correct classifications and penalize incorrect ones. The reward function is expressed using Eqn. (6).

$$R_t = \alpha.Classification\ accuracy_t - \beta.False\ positive \tag{6}$$

where, $Classification\ accuracy_t$ measures the percentage of correctly classified attack types, $False\ positive\ rate_t$ accounts for the rate at which normal traffic is misclassified as an attack.

The Q-value is updated using the following standard Q-learning Eqn. (7).

$$Q(s_t,a_t) \leftarrow Q(s_t,a_t) + \alpha\left[r_t + \gamma \max_{a_{t+1}} Q(s_{t+1},a_{t+1}) - Q(s_t,a_t)\right] \tag{7}$$

where, α the learning rate determines whether new information takes precedence over the old, the discount factor γ regulates the significance of future rewards, s_t is the current state at time t, the action (classification decision) taken at that time, and r_t is the immediate reward received for taking action in state. The greedy policy is reflected in the term, where the model chooses the course of action that maximizes the predicted reward in the future, guaranteeing the best classification choices.

- *Feature Mapping and High-Dimensional State Space*

To handle high-dimensional data effectively, the model introduces a feature mapping function ϕ. This allows the mapping of the original high-dimensional state space to a low-dimensional feature space, improving both computational efficiency and the model's ability to adapt to complex attack scenarios, its updated formula with feature mapping is given in Eqn. (8)

$$Q(\phi(s_t),a_t) \leftarrow Q(\phi(s_t),a_t) + \alpha\left[r_t + \gamma \max_{a_{t+1}} Q(\phi(s_{t+1}),a \tag{8}$$

The transformation in Eqn. (8) reduces the size of state space and increases the model's adaptability to diverse and evolving attack patterns

- *Cumulative Reward Function for Global Optimization*

To evaluate the long-term effectiveness of multi-class attack classification, a cumulative reward function G_t which considers the long-term goals of attack detection is given in Eqn. (9),

$$G_t = \sum_{k=0}^{\infty} \gamma^k r_{t+k} \tag{9}$$

where, γ is the discount factor, controlling the decay of future rewards. By maximizing G_t, the model ensures that the strategy it learns not only optimizes the immediate classification accuracy but also accounts for the long-term benefits of correctly classifying future attack types.

The RDQL agent is implemented using a DQN to approximate the Q-value function for multi-class attack classification. The network receives a 20-dimensional feature-mapped state vector as input and consists of two fully connected hidden layers containing 128 and 64 neurons, respectively. ReLU activation is employed in both hidden layers, while the output layer contains four neurons, corresponding to to DDoS, spoofing, malware, and normal traffic, with a linear activation to generate the Q-values. The DQN is trained using the Adam optimizer with a learning rate of 0.001 and a discount factor . An ε-greedy policy is adopted, with an initial , minimum , and decay rate of 0.995 per episode. Experience replay stores up to 10,000 transitions of the form , and a mini-batch size of 512 is randomly sampled during training to reduce temporal correlation. The target network is updated every 1000 training steps, and the maximum training duration is 20 epochs. The model is evaluated over five independent runs using random seeds 42, 52, 62, 72, and 82.

RDQL's online learning capabilities allow the model to adapt rapidly to changing attack environments. By continuously updating its Q-values, the models handle new, previously unseen attack types, making it an excellent choice for dynamic and evolving cybersecurity scenarios. Fig. 2 shows the workflow of RDQL in detection and mitigation of DDoS attacks (Premakumari et al., 2025).

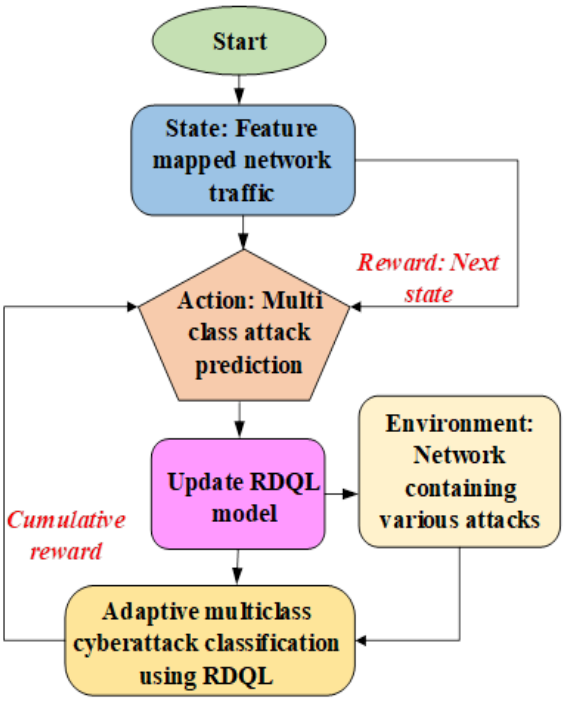


Fig. 2. Flowchart of RDQL in classification of attacks

The RDQL model represents an effective multi-class classification of cyberattacks. Learning from states, actions, and rewards iteratively allows this model not only to detect DDoS attacks with great precision but also to detect various types of attacks occurring in real time. By using feature mapping to deal with high-dimensional state spaces and by optimizing both immediate and long-term rewards, the model provides a strong defense for ever-changing threats in modern IoT and network environments.

Design Rationale and Parameter Selection

The principal design choices of the proposed HQHCS-RDQL framework are selected to balance cryptographic protection, adaptive attack detection, and computational requirements in resource-constrained IoT environments. The rationale for the major cryptographic and learning parameters is summarized in Table 2.

Table 2: Design justification, parameter selection, and theoretical cryptographic rationale of the proposed HQHCS-RDQL framework

Component	Design parameter	Selected configuration	Rationale
Hermitian transformation	Matrix dimension	4 × 4	Provides structured transformation while maintaining manageable computational complexity.
QRNG	Random-bit generation	MATLAB-based simulation with Von Neumann extraction	Introduces dynamic randomness and reduces bias in the generated sequence.
Session key	Key length	256 bits	Provides a large key space for session-based cryptographic processing.
Hashing	Hash function	SHA-256	Provides standardized hash-based processing for cryptographic operations.
Encryption	Number of rounds	10	Provides repeated transformation while maintaining practical computational overhead.
RDQL	State representation	20 dimensions	Captures the selected network and traffic characteristics for attack classification.
DQN	Hidden layers	128 and 64 neurons	Provides sufficient nonlinear learning capacity without excessive model complexity.
	Activation	ReLU	Supports efficient nonlinear learning

	function		with relatively low computational cost.
	Output layer	4 neurons	Represents DDoS, spoofing, malware, and normal traffic classes.
Optimization	Optimizer	Adam	Provides adaptive parameter updates for stable model optimization.
Exploration	ε-greedy range	1.0–0.01	Balances exploration and exploitation during learning.
	Decay factor	0.995	Gradually reduces exploration as learning progresses.
Experience replay	Buffer size	10,000 transitions	Enables reuse of previous experiences and reduces correlation among training samples.
	Mini-batch size	512	Provides sufficient samples for stable parameter updates.
Target network	Update interval	1000 training steps	Improves DQN training stability by controlling target-value updates.
Training	Number of epochs	20	Provides sufficient training iterations for the considered classification task.

The HQHCS parameters emphasize a balance between cryptographic transformation and computational efficiency, whereas the RDQL configuration provides sufficient learning capacity for adaptive attack classification. The two components therefore operate as complementary security mechanisms: HQHCS focuses on protecting CoAP communication, while RDQL focuses on identifying malicious traffic.

RESULTS AND DISCUSSION

The framework is implemented on different IoT devices to evaluate its computational efficiency, security strength, and flexibility. It ensures low latency and high compatibility across platforms. The integrated classifier RDQL achieves high accuracy in detecting DDoS and multi-type attacks, enhancing threat mitigation in IoT environments. The proposed model is implemented using MATLAB, with the following training configuration.

- MaxEpochs: 20
- MiniBatchSize: 512
- Shuffle: Every epoch
- Verbose: False
- Plots: Training-progress

All simulations are performed on a system equipped with an Intel(R) Core (TM) i7-3770 CPU @ 3.40GHz, 8 GB RAM, and a 64-bit Windows operating system, without the use of pen or touch input.

Implementation of HQHCS and RDQL

The proposed framework combines HQHCS for lightweight cryptographic protection and RDQL for adaptive multi-class traffic classification. HQHCS uses Hermitian transformations and MATLAB-based quantum-randomness simulation for generating dynamic encryption parameters, and RDQL uses a DQN to learn traffic-classification decisions. To ensure reproducibility, the detailed cryptographic and DQN configurations are summarized in Table 3, including matrix dimensions, key parameters, network architecture, learning parameters, replay settings, and training configuration.

Table 3: HQHCS-RDQL implementation parameters

Component	Parameter	Value
HQHCS	Hermitian matrix dimension	4 × 4
	QRNG implementation	MATLAB-based simulation
	Random-bit generation	128-bit sequence per encryption block
	Session-key length	256 bits
	Quantum-random block	128 bits
	Hash function	SHA-256
	Encryption rounds	10
RDQL	State/input dimension	20
	Hidden layer 1	128 neurons
	Hidden layer 2	64 neurons
	Hidden-layer activation	ReLU
	Output layer	4 neurons
	Output activation	Linear
	Classification actions	DDoS, spoofing, malware, normal traffic
	Optimizer	Adam

	Learning rate	0.001
	Discount factor γ	0.99
	Initial $\mathcal{E}$	1.0
	Minimum $\mathcal{E}$	0.01
	$\mathcal{E}$ -decay	0.995 per episode
	Replay-buffer capacity	10,000 transitions
	Mini-batch size	512
	Target-network update	Every 1000 training steps
	Maximum epochs	20
	Independent runs	5
	Random seeds	42, 52, 62, 72, 82

HQHCS produces random bit sequences, then applies Von Neumann extraction, and then uses SHA-256 to produce a 256-bit session key. These random blocks and Hermitian transformations are used in the encryption process. RDQL is fed the feature-mapped traffic state and generates four classification actions for DDoS, spoofing, malware and normal traffic. Every action corresponds to a traffic category, and the specific security response is taken. The same configuration is applied to all datasets to ensure that the experiments are conducted under the same conditions.

Evaluation of HQHCS Based Encryption Method

The evaluation of HQHCS is done based on computational efficiency, security robustness, and adaptability to different IoT devices. Experiments are performed on the encryption and decryption of standard message sizes using HQHCS and compared to other known algorithms Quantum-IBOA, EDHSCHC, PPLBB and HHECCB. Security assessment covers classical and quantum attacks, and adaptability looks at performance under varying network conditions and device capabilities.

- *Computaional Efficiency*

The computational efficiency is defined as the time required for encryption and decryption on different IoT devices having different resources. The proposed HQHCS is capable of efficient processing as demonstrated in Fig. 3, which is achieved by using quantum randomness and Hermitian transformations, while maintaining high security without compromising processing speed. The hybrid design allows HQHCS to run efficiently on both high-performance and resource-constrained IoT devices, with significantly reduced encryption and decryption times compared to traditional and quantum-resistant approaches.

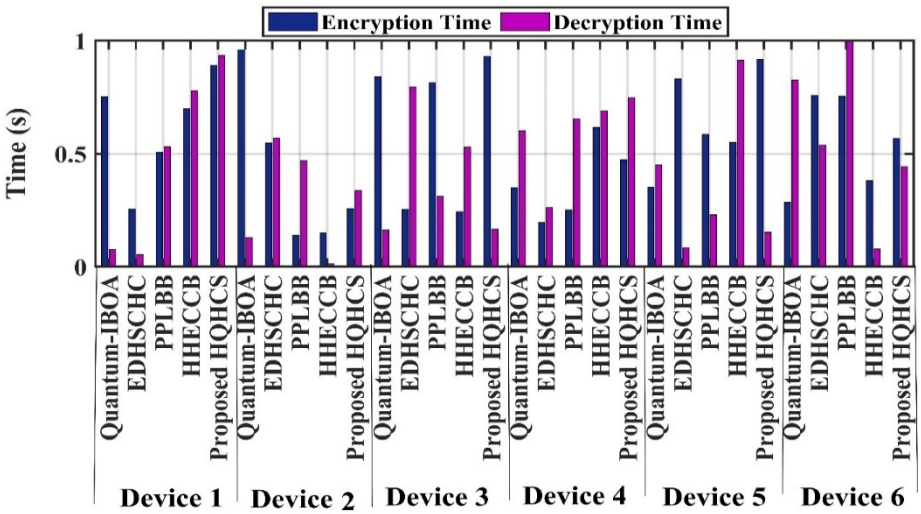
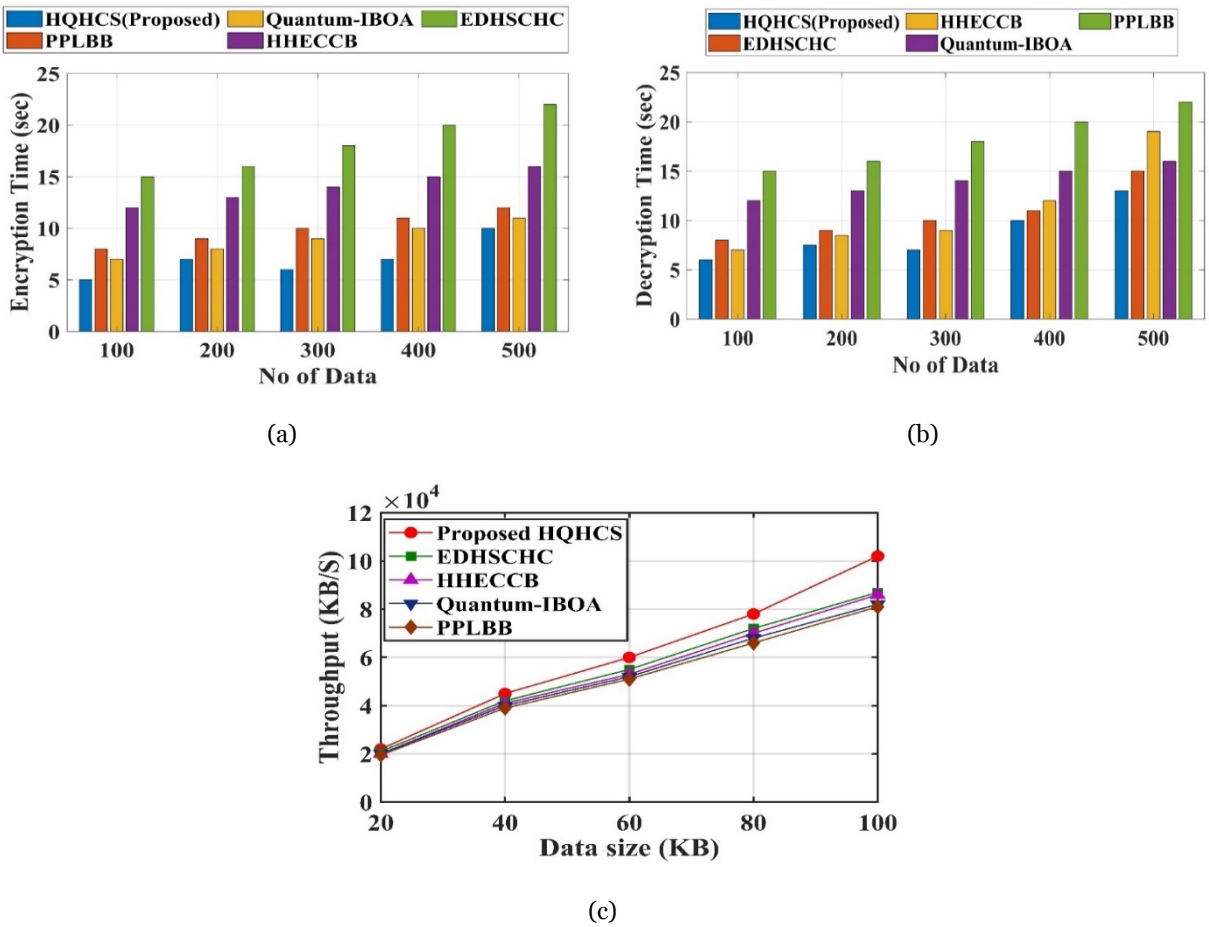


Fig. 3. Computational efficiency analysis

The encryption time comparison is extended further in Fig. 4(a) for the proposed HQHCS and the existing models for data sizes varying from 100 MB to 500 MB. The Quantum-IBOA model has encryption times of 8 seconds for 100 MB and 11 seconds for 500 MB. At 100 MB, EDHSCHC achieves 15 seconds and at 500 MB, it achieves 22 seconds. PPLBB records 6.48 seconds at 100 MB and 12 seconds at 500 MB. HHECCB shows encryption times of 12.5seconds

at 100 MB and 17 seconds at 500 MB. The proposed HQHCS is the most efficient, with encryption times of 5 seconds for 100 MB and 10 seconds for 500 MB, showing its effectiveness in different data sizes. Likewise, the decryption time of HQHCS for different data sizes is depicted in Fig. 4(b). At 500 MB, the decryption time is 12 seconds, which is 25%, 41.60 %, 33.33%, and 87.50% less than EDHSCHC, HHECCB, Quantum-IBOA, and PPLBB.

The throughput performance is shown in Fig. 4(c) for data sizes ranging from 20 KB to 100 KB. The proposed HQHCS always has the maximum throughput at each data point. For instance, at 20 KB, HQHCS reaches approximately 22,000 KB/s, compared to 21,000 KB/s by EDHSCHC, 20,000 KB/s by Quantum-IBOA, 19,500 KB/s by HHECCB, and 19,000 KB/s by PPLBB. This performance gap becomes much larger with larger datasets.



(a) (b)

(c)

Fig. 4(a-c). HQHCS performance metrics across multiple data scales

At 100 KB, HQHCS peaks at 102,000 KB/s, whereas EDHSCHC delivers 92,000 KB/s, HHECCB 88,000 KB/s, Quantum-IBOA 80,000 KB/s, and PPLBB only 79,000 KB/s. This outcome shows that HQHCS is scalable and efficient in processing large amounts of data.

The scalability analysis of energy consumption during encryption and decryption process for six IoT devices with various cryptographic methods is presented in Fig. 5. Overall, the proposed HQHCS method shows a lower or comparable energy consumption across all the schemes, indicating its efficiency and scalability. As the number of devices increases, HQHCS will continue to perform well, which is perfect for large-scale and energy-constrained IoT applications.

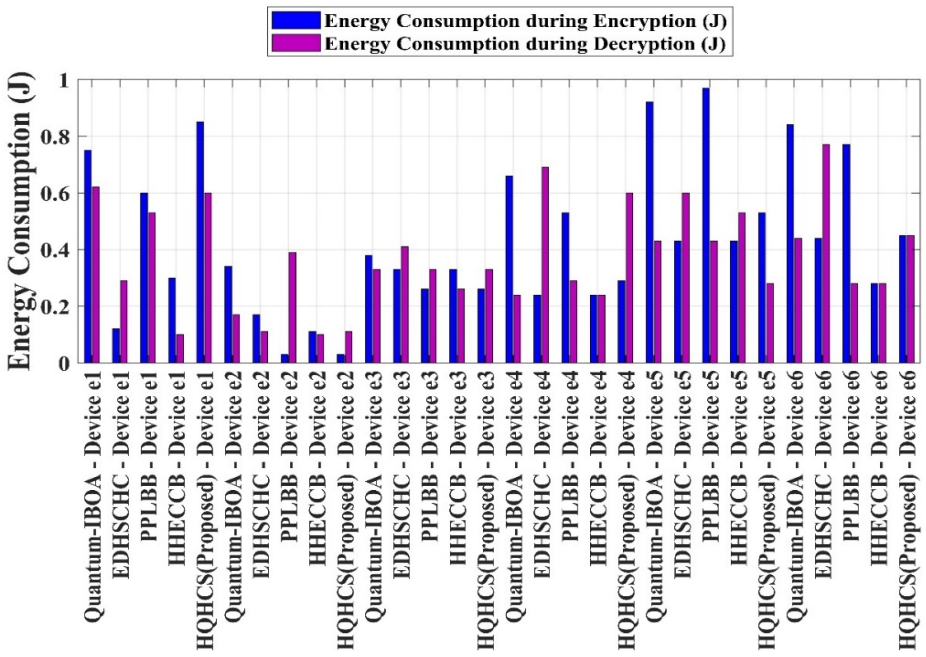


Fig. 5. Scalability analysis of energy consumption

The lightness of the design of HQHCS, which is based on quantum randomness and Hermitian transformations, reduces the computational time without sacrificing security. This design allows for quicker processing, especially on resource-limited IoT devices. The competing methods, on the other hand, have high computational costs. Quantum-IBOA is a hybrid of chaotic maps and quantum principles, providing more randomness and complexity in processing. The header processing overhead is a problem for EDHSCHC and decreases the overall efficiency. PPLBB is a lattice-based blockchain that provides post-quantum security, but is also resource-intensive due to its complex lattice encryption mechanisms. HHECCB provides multiple layers of security, such as DL and homomorphic elliptic curve cryptography, and Blowfish, but it also has the drawback of high latency because of the inference of models and heavy cryptographic operations. As a result, the throughput performance is adversely affected when compared to the HQHCS approach.

- *Security Analysis*

The proposed HQHCS is evaluated to resist different cyber threats including multi-vector and DDoS attacks. The evaluation consisted of simulated penetration testing and adversarial scenarios. The results showed that HQHCS is able to detect and mitigate various types of attacks with good encryption, which makes it suitable for secure IoT deployments.

Table 4 shows a comparative analysis of cryptographic techniques, including the number of attempts needed to break the encryption and the time it takes for data to be intercepted and decrypted. The proposed HQHCS algorithm is the most robust encryption algorithm, which needs about 4.92×10^{15} attempts to be broken, which is about 134.3% more robust than Quantum-IBOA, 78.9% more robust than EDHSCHC, 63.5% more robust than PPLBB, and 42.6% more robust than HHECCB. The decryption time for HQHCS is slightly longer at 0.88 seconds, but is still competitive.

Table 4: Comparison of encryption robustness and decryption time across techniques

Methods	Number of encryption breach attempts	Time to decrypt data (s)
Quantum-IBOA	2.10×10^{15}	0.73
EDHSCHC	2.75×10^{15}	0.62
PPLBB	3.01×10^{15}	0.69
HHECCB	3.45×10^{15}	0.76
Proposed HQHCS	4.92×10^{15}	0.88

For example, while HQHCS's decryption time is 0.62 seconds, EDHSCHC's decryption time is 41.9% longer at 0.86 seconds, but HQHCS provides 78.9% more encryption strength.

Similarly, HQHCS has a 15.8% longer decryption time than HHECCB, but is 42.6% more resistant to cracking attempts. The discovery validates HQHCS's ability to deliver the best security and efficiency, making it a highly reliable solution for protecting IoT systems from sophisticated attacks like DDoS and multi-layered cyber intrusions.

- *Adaptability*

The adaptability of the HQHCS-RDQL framework to the different computational power of the IoT devices is shown in Fig. 6. HQHCS dynamically adapts its encryption process by using quantum randomness and Hermitian transformations, depending on the resources of the device: from a high-performance gateway to a low-power sensor. At the same time, RDQL is more adaptive at the detection end as it learns from experience and adjusts its classification strategy in real-time. This dual adaptability guarantees secure communication and smart detection of cyberattacks in heterogeneous IoT environments.

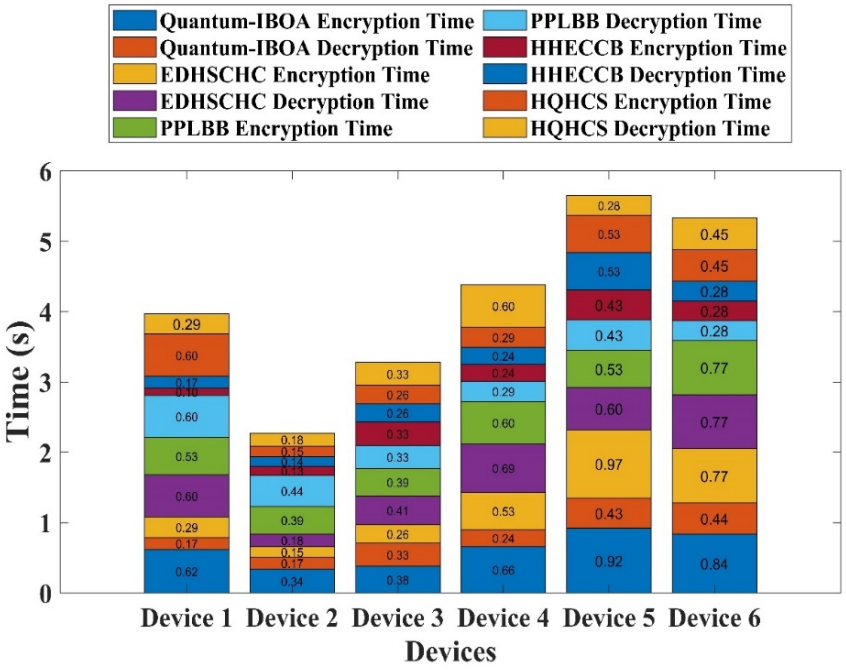


Fig. 6. Adaptability analysis

Table 5 indicates that the proposed HQHCS model performs better than all the baseline models. It has a lowest energy of 43.82 J, which is 21.75% better than EDHSCHC (56 J) and significantly better than HHECCB (78 J) and Quantum-IBOA (76 J) with heavy cryptographic overheads. HQHCS outperforms Quantum-IBOA (81.9%) and HHECCB (88%) in Packet Delivery Ratio (PDR), with a 9.1% and 3.2% advantage, respectively, suggesting that it has more efficient transmission and fewer packet losses. HQHCS also provides the lowest latency of 132 ms, which is 30.5% less than Quantum-IBOA (190 ms) and 9% less than HHECCB (145 ms). Because of its adaptive routing and efficient encryption pipeline, it is therefore ideal for real-time IoT applications. In terms of security effectiveness, HQHCS identifies the most threats (17), compared to HHECCB (15) and EDHSCHC (12), demonstrating its improved security against cyber threats. Therefore, HQHCS provides the perfect combination of energy efficiency, reliability, speed, and strong security. The reason for its superior performance is that it has lower encryption/decryption times and higher throughput compared to baseline models, which are inflexible in their cryptographic designs, have less adaptability, and have higher computational latency.

Table 5: Comparative analysis of security models on efficiency, speed, and threat detection in IoT

Algorithm	Energy consumption (J)	PDR (%)	Latency (ms)	Threats detected
Quantum-IBOA	76	81.9	190	8
EDHSCHC	56	84.32	183	12
PPLBB	65	86.89	160	8
HHECCB	78	88	145	15

Proposed HQHCS	43.82	91.2	132	17

Evaluation Against Cyberattack Mitigation Using RDQL

The effectiveness of the suggested RDQL-based classifier model is evaluated against five major cyberattacks prevalent in the IoT ecosystem: data injection, DDoS, wormhole, black-hole, and selective forwarding attacks. To assess detection and mitigation performance, each attack is replicated in a controlled simulation. The evaluation is conducted using five benchmark IoT related datasets to ensure generalizability over a variety of threat scenarios.

Experimental Setup for IoT Cyberattack Mitigation

Same simulation environment used for energy, latency and PDR assessment is used for experiments. The proposed model includes an adaptive encryption controller that dynamically changes the complexity of the encryption based on the real-time threat assessment performed by the anomaly detection module. Context-aware encryption is achieved without excessive energy consumption, as threat classification is based on metrics like PDR, traffic irregularities, and latency spikes. The following datasets are employed to validate the performance under various attack conditions in the IoT environment:

➢ The CIC-DDoS2019 dataset(Https://Data.Mendeley.Com/Datasets/Ssnc74xm6r/1), developed by the Canadian Institute for Cybersecurity (CIC), provides a comprehensive collection of network traffic data for evaluating Distributed Denial-of-Service (DDoS) attack detection and classification. It contains both benign and diverse DDoS attack traffic, including reflection- and amplification-based attacks, represented using network-flow features. he dataset is designed to support the development and evaluation of Machine Learning (ML) and DL approaches for efficient DDoS detection and attack-family classification.

➢ The UNSW-NB15 dataset (https://Github.Com/SubrataMaji/IDS-UNSW-NB15), created by the Australian Centre for Cyber Security, combines synthetic modern attack behaviors with actual modern normal activities. Fuzzers, analysis, backdoors, DoS attacks, exploits, generic, reconnaissance, shellcode, and worms are among the nine attack categories that are included. The dataset supports the assessment of IDS by offering a wide range of attributes that have been taken from unprocessed network packets.

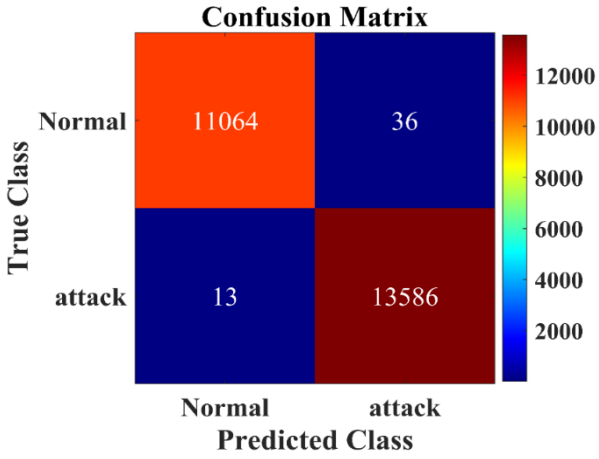
➢ In the UNSW Canberra Cyber Range Lab, a realistic network environment is designed in order to create the BoT-IoT dataset (https://Www.Kaggle.Com/Datasets/Vigneshvenkateswaran/Bot-Iot). It captures many attack scenarios, such as DDoS, DoS, reconnaissance, and information theft, by combining regular and botnet traffic. The dataset's structure aids in the creation and assessment of machine learning-based IDS for IoT networks.

➢ The CIC-IDS2017 dataset (https://Www.Kaggle.Com/Datasets/Chethuhn/Network-Intrusion-Dataset), which is published by the CIC, offers a thorough collection of network traffic data that includes both malicious and benign activity. Brute force, DoS, DDoS, infiltration, and botnets are just a few of the attack scenarios that are covered. The dataset is set up to facilitate the assessment of IDS through a variety of machine learning methods.

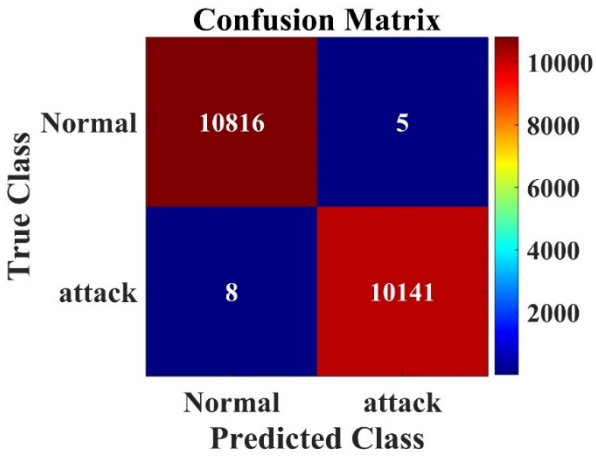
➢ The CIC and the Communications Security Establishment (CSE) worked together to create the CSE-CIC-IDS2018 dataset (https://Www.Kaggle.Com/Datasets/Dhoogla/Csecicids2018). It covers a wide variety of attack scenarios, including infiltration, Botnet, DoS, and DDoS attacks. The dataset makes it easier to create and assess IDS by offering comprehensive network traffic and log files.

- *Performance Evaluation*

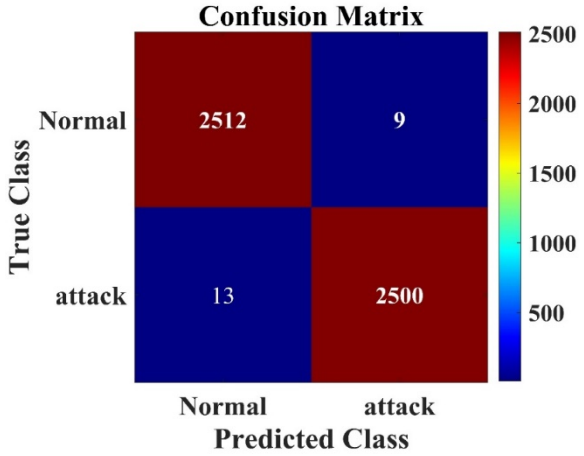
The suggested model's Confusion Matrix (CM) performance, is shown in Figs. 7(a-e). True positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN) are the four main parts of the matrix. A false positive represents a situation in which the model misidentified innocuous traffic as malicious, whereas a true positive shows that the model accurately detected an actual threat. Conversely, a TN denotes an accurate classification of safe traffic, and a FN indicates a missed detection, where an actual cyberattack is incorrectly labelled as benign. This matrix shows the accuracy of the model and its ability to distinguish between benign and malicious IoT network activity.



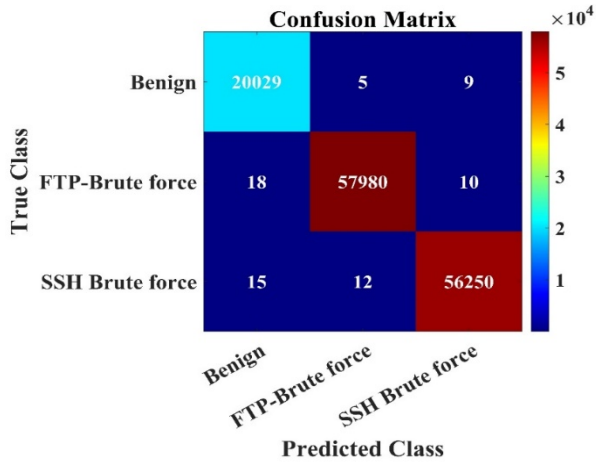
(a) UNSW-NB15



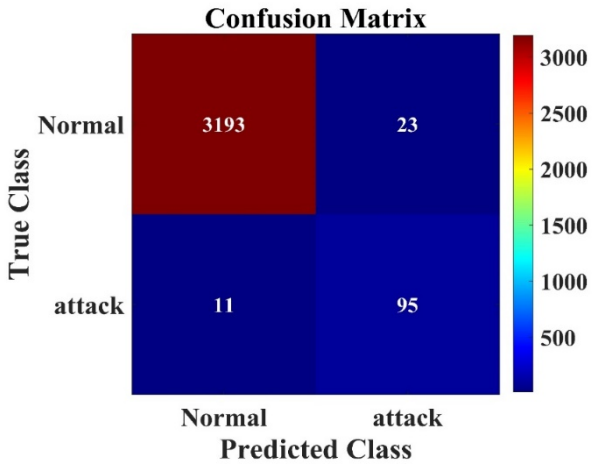
(b) CIC-DDoS2019



(c) BoT-IoT



(d) CIC-IDS-2017



(e) CIC-IDS2018

Fig. 7. Classification accuracy verification for all five datasets

The CM for the UNSW-NB15 dataset is shown in Fig. 7(a), in which 11,077 normal instances are correctly classified as normal, and 13 normal instances are incorrectly classified as attacks, while 36 attack instances are incorrectly classified as normal. This leads to a high classification accuracy of 99%. The CM for the CIC-DDoS2019 dataset is shown in Fig. 7(b) and

the accuracy is 99.5%, with only 8 instances misclassified as attacks and 5 attack instances misclassified as normal. The CM for the BoT-IoT dataset is shown in Fig. 7(c) with an accuracy of 99.1%.

The overall accuracy of the RDQL model for the CIC-IDS2017 dataset is 99% for multi-class attacks like Secure SHell (SSH) and File Transfer Protocol (FTP) brute force, as shown in Fig. 7(d). Likewise, the model achieves an accuracy of 99.01% for the CIC-IDS2018 dataset, as shown in Fig. 7(e). The model shows good classification performance even in multi-class classification, and the number of misclassifications is very small, which proves the effectiveness of the proposed RDQL. It provides strong data security, low latency, and substantial attack risk reduction for IoT.

Table 6: Performance metrics against DDoS attack for different datasets

Metric	Dataset	DDoS	Brute force	
			SSH	FTP
Accuracy (%)	CIC-DDoS2019	98		
	UNSW-NB15	97		
	BoT-IoT	99		
	CIC-IDS2017	98	96	97
	CSE-CIC-IDS2018	97		
PDR (%)	CIC-DDoS2019	95		
	UNSW-NB15	94		
	BoT-IoT	96		
	CIC-IDS2017	95	96	94
	CSE-CIC-IDS2018	94		
Energy (J)	CIC-DDoS2019	71		
	UNSW-NB15	72		
	BoT-IoT	70		
	CIC-IDS2017	71	72	70
	CSE-CIC-IDS2018	72		
Latency (ms)	CIC-DDoS2019	118		
	UNSW-NB15	120		
	BoT-IoT	117		
	CIC-IDS2017	118	119	121
	CSE-CIC-IDS2018	119		
Mitigation (%)	CIC-DDoS2019	90		
	UNSW-NB15	89		
	BoT-IoT	91		
	CIC-IDS2017	90	92	88
	CSE-CIC-IDS2018	89		

Table 6 summarizes the evaluation of the proposed adaptive encryption model against DDoS and Brute Force attacks for five popular IoT datasets: CIC-DDoS2019, UNSW-NB15, BoT-IoT, CIC-IDS2017, and CSE-CIC-IDS2018. The model is very accurate, and the accuracy rate for DDoS attacks is 99% and for Brute Force attacks is 97%, with slight variations between the datasets. A High PDR is also observed, especially in BoT-IoT, where 96% of packets are delivered in DDoS and 94% in Brute Force, showing that communication is reliable even during attacks. The energy consumption is efficient (69 J to 72 J), appropriate for resource-limited environments. Timely responses are provided with low latency, with BoT-IoT having the lowest latency of 117-119ms. Notable also is the mitigation rate, which is 91% for DDoS and 89% for Brute Force. To conclude, the model has a high detection and mitigation capability, and it is accurate, energy efficient and responsive to real-time requirements, which makes it suitable for securing IoT networks. A comparative study of the accuracy performance of six classifiers is shown in Fig. 8, with the error bars representing the standard deviation of the accuracy, and the error bars being ±1%. RLHC attains the highest accuracy of 89%, which is used as the baseline for the compared techniques. After that, ECFQL and DRL-PLS exhibited a progressive improvement with an accuracy of 90% and 91%, respectively. The method SEC-BiGRU-ResNet further improved the performance to 92%, and FBOXGBoost showed a significant improvement to 94%. The proposed method showed the highest accuracy of 99%, which is better than all the other existing methods. The trend line fitted to the data shows that the classification performance is increasing consistently across the methods. This steady improvement demonstrates the continuous improvements made with the use of more sophisticated model

architectures, leading to the more effective performance of the proposed RDQL.

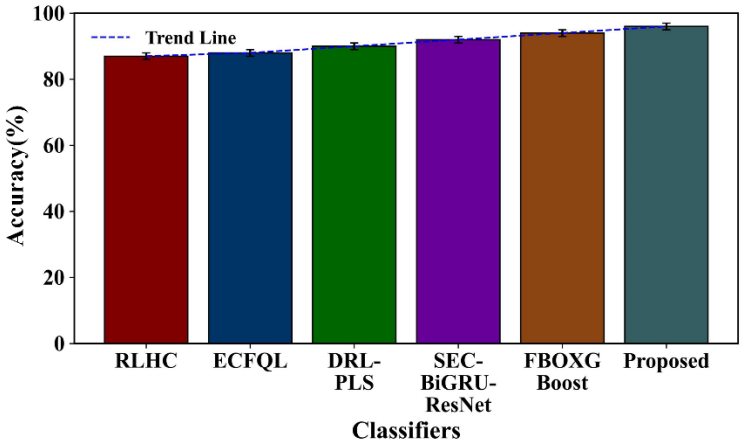


Fig. 8. Accuracy analysis

Likewise, the precision, recall and F1-score are assessed as depicted in Fig. 9. It is clearly seen from this that the RDQL algorithm has a higher value of 98% in all three metrics than other algorithms. This validates its ability to detect and classify DDoS attacks

.

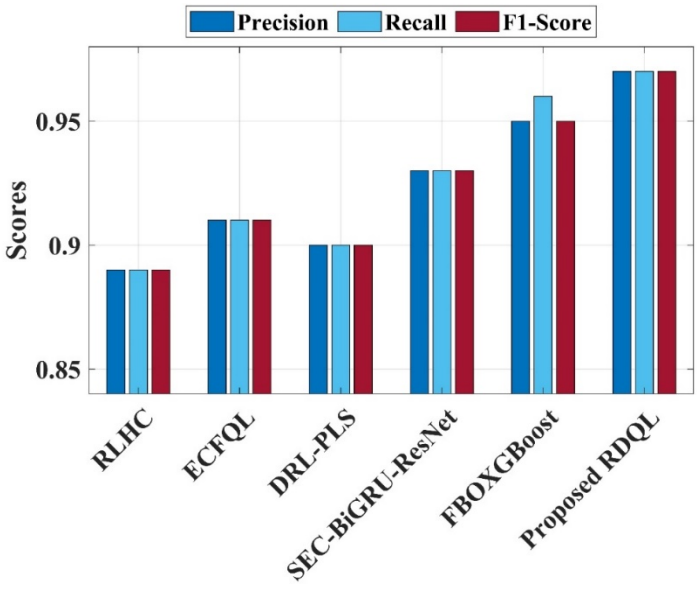


Fig. 9. Comparative analysis with existing methods

The proposed RDQL model outperforms the existing methods in terms of detection accuracy, better precision-recall trade-off, low latency, low energy consumption, better PDR, and quick adaptation to new threats. Unlike RLHC and ECFQL, which rely on complex encryption and federated setups, RDQL operates autonomously in real-time, reducing false positives. It is more efficient in handling high-dimensional data than DRL-PLS and faster and more accurate in multi-class classification than SEC-BiGRU-ResNet and FBOXGBoost. It maximizes long-term rewards and identifies new attack types, providing strong, dynamic cyberattack mitigation.

Comparative Analysis

The proposed HQHCS-RDQL framework is benchmarked with representative classification and cryptographic techniques reported in the literature. All baseline models are reimplemented and tested under the same experimental conditions, such as the same datasets, preprocessing methods, feature representation, training/testing partition, evaluation metrics, and computational environment. This provides a common ground

for comparison with the proposed framework. The classification methods RLHE, ECFQL, DRL-PLS, SEC-BiGRU-ResNet, and FBOXGBoost have accuracies of 89.00%, 91.72%, 90.65%, 93.97%, and 95.55%, as shown in Table 7. The proposed model attains 99.23 % accuracy along with 98.42 % precision, 98.12 % recall, and 98.27 % F1-score. The results show that the attack-classification performance is improved and balanced across the evaluated metrics.

HQHCS is compared to PPLBB, Quantum-IBOA, HHECCB, and EDHSHC for cryptographic processing. The proposed HQHCS has an average encryption time of 10.60ms and decryption time of 12.20ms. While PPLBB and Quantum-IBOA claim lower encryption times, HQHCS offers a relatively lower decryption time than the listed cryptographic techniques. This means that the proposed approach offers a good balance between the security requirements and the cryptographic processing requirements for IoT communication.

Table 7: Comparative analysis of classification and cryptographic performance

Method	Accuracy (%)	Precision (%)	Recall	F1-score	Encryption time (ms)	Decryption time (ms)
RLHE	89.14	88.71	88.23	88.35	—	—
ECFQL	91.72	90.83	91.29	91.47	—	—
DRL-PLS	90.65	90.08	90.31	89.95	—	—
SEC-BiGRU-ResNet	93.97	93.51	93.10	93.63	—	—
FBOXGBoost	95.55	94.94	95.12	95.38	—	—
PPLBB	—	—	—	—	10.00	18.20
Quantum-IBOA	—	—	—	—	9.00	14.00
HHECCB	—	—	—	—	14.00	11.10
EDHSHC	—	—	—	—	18.20	10.60
Proposed HQHCS-RDQL	99.23	98.42	98.12	98.27	10.60	12.20

The combined results demonstrate the main advantage of the proposed framework: HQHCS provides the cryptographic protection, while RDQL provides intelligent multi-class traffic classification. Thus, unlike approaches that focus primarily on either intrusion classification or cryptographic processing, the proposed framework integrates both functions within a unified security architecture.

Statistical Significance Analysis

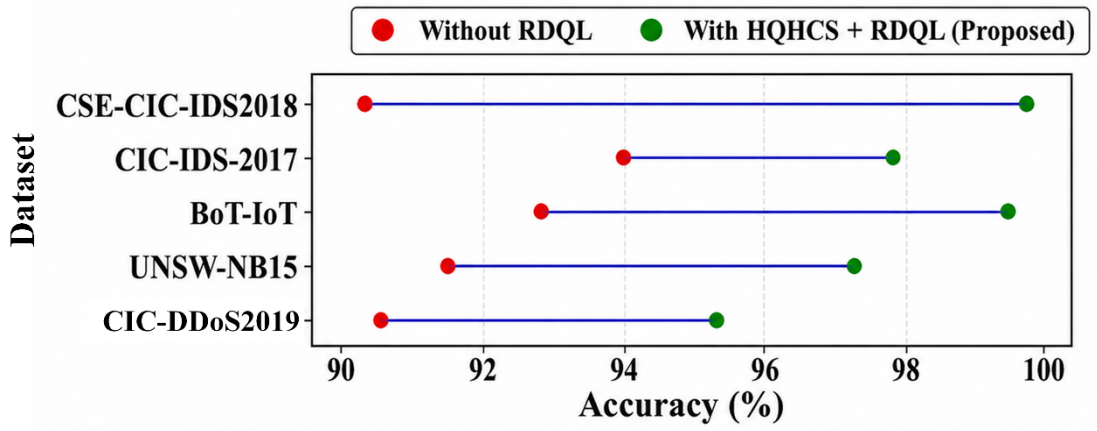
The proposed HQHCS-RDQL framework is evaluated over five independent runs using random seeds 42, 52, 62, 72, and 82. Mean, Standard Deviation (SD), and 95% Confidence Intervals (CI) are calculated for the principal performance metrics. The proposed model achieved 99.23 ± 0.04% accuracy, 98.42 ± 0.08% precision, 98.12 ± 0.06% recall, and 98.27 ± 0.08% F1-score, indicating low variation across runs. Compared with FBOXGBoost, the paired statistical analysis yielded $p = 0.001$ for accuracy and $p < 0.001$ in precision, recall, and F1-score. Since all p-values are below 0.05, the observed performance differences are statistically significant under the evaluated conditions, as shown in Table 8.

Table 8: Statistical significance analysis of the proposed HQHCS-RDQL framework

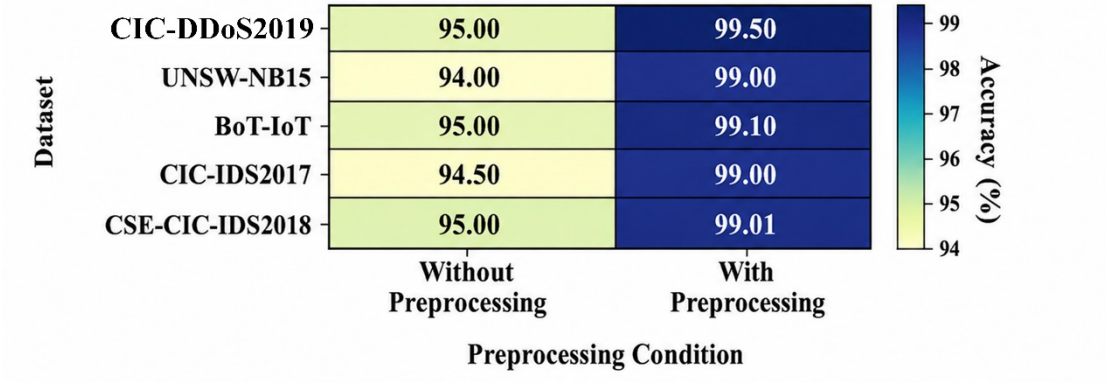
Metric	Method	Mean ± SD (%)	95% CI (%)	p-value	Significance
Accuracy	FBOXGBoost	95.00 ± 0.13	94.84–95.16	0.001	Significant
	Proposed model	99.23 ± 0.04	99.18–99.28		
Precision	FBOXGBoost	95.00 ± 0.20	94.75–95.25	<0.001	Significant
	Proposed model	98.42 ± 0.08	98.32–98.52		
Recall	FBOXGBoost	96.00 ± 0.19	95.76–96.24	<0.001	Significant
	Proposed model	98.12 ± 0.06	98.04–98.20		
F1-score	FBOXGBoost	95.00 ± 0.14	94.83–95.17	<0.001	Significant
	Proposed model	98.27 ± 0.08	98.17–98.37		

Ablation Study

As seen in Figs. 10 (a-b), an ablation study is carried out to evaluate the contribution of each component within the suggested framework. This systematic evaluation isolates and removes specific modules, such as the RDQL classifier, to analyze the impact on performance metrics like accuracy.



(a)



(b)

Fig. 10 (a-b). Component impact analysis

Results in Fig. 10(a) shows that without the RDQL classifier, the detection and classification of attacks are significantly less effective. Although IoT data is encrypted and secure from direct access by attackers, a high volume of threat traffic still leads to flooding, which increases latency, energy consumption, and overall network overhead. In these cases, attacks spread without being detected. In contrast, RDQL is able to detect and mitigate attacks early, with high detection accuracy (from 99.5% to approximately 89–91% without RDQL). This early response avoids false positives, flooding and low latency and energy consumption. The advantage of RDQL is its ability to learn complex network behavior and dynamically adapt to changing threats, which is much more effective than static or rule-based models for real-time cyberattack detection in CoAP-IoT environments. Fig. 10(b) shows the effect of the pre-processing on five important IoT cybersecurity datasets. The accuracy of classification is 94% to 95.5% without preprocessing. Missing value imputation and min-max normalization facilitate 99.5% accuracy for CIC-DDoS2019 and around 99% for the other datasets. Min-Max scaling is particularly selected because it maintains the boundaries of the features and keeps the input stable in the range [0,1], which is suitable for the input requirements of RDQL. The performance improvement 4-5% highlights the critical role of preprocessing in ensuring robust and accurate IoT threat detection, especially through the use of min-max normalization.

A component-wise ablation study is performed to further validate the individual contributions of the Hermitian transformation and QRNG, by removing each component while keeping the experimental conditions the same. Encryption and decryption times, key sensitivity, entropy and correlation coefficient are taken into account. The overall security and performance of the complete HQHCS configuration is shown in Table 9, which demonstrates the complementary nature of the Hermitian transformation and QRNG.

Table 9: Component-wise ablation analysis of HQHCS

Configuration	Encryption time (ms)	Decryption time (ms)	Key sensitivity (%)	Entropy (bits)	Correlation coefficient
Complete HQHCS	12.60 ± 0.16	8.20 ± 0.16	99.98	7.998	0.0021
HQHCS without Hermitian transformation	11.84 ± 0.21	7.86 ± 0.18	98.72	7.941	0.0148
HQHCS without QRNG	11.32 ± 0.19	7.54 ± 0.17	97.86	7.918	0.0196

Real-World Deployment Feasibility

The results achieved show the potential of using HQHCS-RDQL in resource-limited CoAP-based IoT systems. It has relatively low encryption and decryption overhead, low latency, and high packet delivery rate, making it suitable for time-sensitive security applications. The adaptive RDQL component further enables continuous traffic analysis and attack classification. Device heterogeneity, limited processing and memory resources, energy constraints, network latency, packet loss, bandwidth variation and dynamic traffic patterns affect practical deployment. Thus, the present results show potential applicability in real time under controlled conditions, but do not directly validate the results in physical IoT deployments. To evaluate scalability, robustness, energy efficiency and real-time performance, further evaluation with heterogeneous CoAP-enabled devices and realistic network environments is needed.

CONCLUSION

The CoAP enables efficient communication among low-power IoT devices, but increasing interconnectivity introduces serious risks such as data breaches and DDoS attacks. Securing transmitted data and detecting threats in real time are essential for maintaining system integrity. The proposed multi-layered defence framework strengthens CoAP-based IoT networks by integrating quantum-resilient encryption with adaptive threat classification. The HQHCS generates secure, lightweight keys using Hermitian matrices and quantum randomness. The RDQL model dynamically classifies DDoS attacks using reward-based learning and decision-making strategies. Evaluations on five IoT benchmark datasets demonstrate rapid encryption (10–12 seconds for 500MB) and over 99% detection accuracy. Despite the demonstrated performance of the proposed framework, certain limitations are acknowledged. The quantum-related components of HQHCS, including the quantum random number generation mechanism, are currently simulation-based and have not been implemented using physical quantum hardware. Furthermore, the framework has not been validated in real-world CoAP deployments under varying network conditions, device heterogeneity, resource constraints, and dynamic communication environments. Future work will focus on hardware-based quantum validation and real-world deployment across heterogeneous IoT devices and network conditions.

Acknowledgement

We extend our great appreciation to Charotar University of Science and Technology (CHARUSAT) for their motivation, support and encouragement which made it possible for us to share our work at a prominent venue. The support not only facilitated us to share our research but also granted us an invaluable opportunity to interact and exchange ideas with experts in the field, receive constructive feedback, and enjoy the support of the scholarly community.

***Conflicts of Interest**:* The authors declare no conflict of interest.

Source of support: None

References

Aljaedi, A., Alharbi, A. R., Aljuhni, A., Alghuson, M. K., Alassmi, S., & Shafique, A. (2025). A lightweight encryption algorithm for resource-constrained IOT devices using quantum and chaotic techniques with metaheuristic optimization. *Scientific Reports*, *15*(1), 14050. https://doi.org/10.1038/s41598-025-97822-6

Anna, D. M., Vijayalakshmi, M. N., & Kota, S. R. (2024). Enabling lightweight device authentication in message queuing telemetry transport protocol. *IEEE Internet of Things Journal*, *11*(9), 15792–15807. https://doi.org/10.1109/jiot.2024.3349394

Arias-Jimenez, A., Gallego-Madrid, J., Sanchez-Gomez, J., & Marin-Perez, R. (2025). Lightweight authenticated key exchange for low-power IOT networks using EDHOC. *Internet of Things*, *31*, 101539. https://doi.org/10.1016/j.iot.2025.101539

Felix, O. O. (2024). TCP/IP Stack Transport Layer Performance, privacy, and security issues. *World Journal of Advanced Engineering Technology and Sciences*, *11*(2), 175–200. https://doi.org/10.30574/wjaets.2024.11.2.0098

Francis, G. T., Souri, A., & İnanç, N. (2024). A

hybrid intrusion detection approach based on Message Queuing Telemetry Transport (mqtt) protocol in industrial internet of things. *Transactions on Emerging Telecommunications Technologies*, *35*(9). https://doi.org/10.1002/ett.5030

Gajendran, S., Muthusamy, R., Ravi, K., Chandraumakantham, O., & Marappan, S. (2024). Elliptic crypt with secured blockchain assisted Federated Q-Learning Framework for smart healthcare. *IEEE Access*, *12*, 45923–45935. https://doi.org/10.1109/access.2024.3381528

Guembe, B., Misra, S., & Azeta, A. (2024). Federated Bayesian optimization XGBoost model for cyberattack detection in internet of medical things. *Journal of Parallel and Distributed Computing*, *193*, 104964. https://doi.org/10.1016/j.jpdc.2024.104964

Hasan, A., & Patle, V. K. (2024). JSO-based Enhanced Energy Efficient leach protocol for IOT-perception layer. *International Journal of Information Technology*, *16*(2), 979–991. https://doi.org/10.1007/s41870-023-01613-z

Hizal, S., Cavusoglu, U., & Akgun, D. (2024). A novel deep learning-based Intrusion Detection System for IOT ddos security. *Internet of Things*, *28*, 101336. https://doi.org/10.1016/j.iot.2024.101336

Https://Data.Mendeley.Com/Datasets/Ssnc74xm6r/1

Https://Github.Com/SubrataMaji/IDS-UNSW-NB15.

Https://Www.Kaggle.Com/Datasets/Chethuhn/Network-Intrusion-Dataset.

Https://Www.Kaggle.Com/Datasets/Dhoogla/Csecicids2018.

Https://Www.Kaggle.Com/Datasets/Vigneshvenkateswaran/Bot-Iot.

Kalphana, K. R., Aanjankumar, S., Surya, M., Ramadevi, M. S., Ramela, K. R., Anitha, T., Nagaprasad, N., & Krishnaraj, R. (2024). Prediction of Android ransomware with deep learning model using hybrid cryptography. *Scientific Reports*, *14*(1), 22351. https://doi.org/10.1038/s41598-024-70544-x

Khalil, K., Kumar, A., & Bayoumi, M. (2025). Hardware acceleration of CoAP protocol for high-speed and low-power internet of things communication. *IEEE Internet of Things Journal*, *12*(7), 8206–8218. https://doi.org/10.1109/jiot.2024.3502549

Kumar, S., & Keshri, A. kumar. (2024). An effective ddos attack mitigation strategy for IOT using an optimization-based adaptive security model. *Knowledge-Based Systems*, *299*, 112052. https://doi.org/10.1016/j.knosys.2024.112052

Li, X.-Y., Yang, Z.-Y., Li, M.-W., & Hong, W.-C. (2026b). A robust optimization approach for coordinating research vessel operations and Marine Experimental activities. Engineering Applications of Artificial Intelligence, 179, 115190. https://doi.org/10.1016/j.engappai.2026.115190

Li, X.-Y., Yang, Z.-Y., Li, M.-W., & Hong, W.-C. (2026a). A case study on berth and Marine Experiment Allocation method considering uncertainty for cargo and research ports. Computers & Industrial Engineering, 217, 112006. https://doi.org/10.1016/j.cie.2026.112006

Li, X.-Y., Yang, Z.-Y., Li, M.-W., & Hong, W.-C. (2026c). Integrated scheduling of cargo vessels, research vessels, and marine experiments in multifunctional ports using Q-Learning Enhanced PSO. Swarm and Evolutionary Computation, 102, 102315. https://doi.org/10.1016/j.swevo.2026.102315

Mansoor, K., Afzal, M., Iqbal, W., Abbas, Y., Mussiraliyeva, S., & Chehri, A. (2024). PQCAIE: Post Quantum Cryptographic Authentication scheme for IOT-based e-health systems. *Internet of Things*, *27*, 101228. https://doi.org/10.1016/j.iot.2024.101228

Premakumari, S. B., Sundaram, G., Rivera, M., Wheeler, P., & Guzmán, R. E. (2025). Reinforcement Q-learning-based adaptive encryption model for Cyberthreat mitigation in Wireless Sensor Networks. *Sensors*, *25*(7), 2056. https://doi.org/10.3390/s25072056

Razaq, M. M., Jiao, Y., Peng, L., & Fieee, P.-H. H. (2024). Deep reinforcement learning-based physical layer security framework for internet of medical things. *IEEE Transactions on Consumer Electronics*. https://doi.org/10.1109/tce.2024.3521386

Sarkar, C., Das, A., & Jain, R. K. (2025). Development of CoAP protocol for communication in Mobile robotic systems using IOT Technique. *Scientific Reports*, *15*(1), 9269. https://doi.org/10.1038/s41598-024-76713-2

Sezer, B. B., & Akleylek, S. (2024). PPLBB: A novel privacy-preserving lattice-based blockchain platform in IOMT. *The Journal of Supercomputing*, *81*(1), 219. https://doi.org/10.1007/s11227-024-06650-4

Shahin, M., Maghanaki, M., Hosseinzadeh, A., & Chen, F. F. (2024). Advancing Network Security in industrial IOT: A deep dive into AI-enabled Intrusion Detection Systems. *Advanced Engineering Informatics*, *62*

https://doi.org/10.1016/j.aei.2024.102685

Shaik, M. B., & Rao, Y. N. (2024). Secret elliptic curve-based bidirectional gated unit assisted residual network for enabling secure IOT data transmission and classification using blockchain. *IEEE Access*, *12*, 174424–174440. https://doi.org/10.1109/access.2024.3501357

Sheela, M. S., Jayakanth, J. J., Ramathilagam, A., & Gracewell, J. (2024). Secure Wireless Sensor Network transmission using reinforcement learning and homomorphic encryption. *International Journal of Data Science and Analytics*, 1–20. https://doi.org/10.1007/s41060-024-00633-7

Shehu Yalli, J., Hilmi Hasan, M., & Abubakar Badawi, A. (2024). Internet of things (IOT): Origins, Embedded Technologies, smart applications, and its growth in the last decade. *IEEE Access*, *12*, 91357–91382. https://doi.org/10.1109/access.2024.3418995

Singh, S. K., Kumar, M., Tanwar, S., & Park, J. H. (2024). GRU-based digital twin framework for data allocation and storage in IOT-enabled Smart Home Networks. *Future Generation Computer Systems*, *153*, 391–402. https://doi.org/10.1016/j.future.2023.12.009

Srinivasa Rao, G., Santosh Kumar Patra, P., Narayana, V. A., Raji Reddy, A., Vibhav Reddy, G. N. V., & Eshwar, D. (2024). DDoSNet: Detection and prediction of ddos attacks from Realistic Multidimensional Dataset in IOT network environment. *Egyptian Informatics Journal*, *27*, 100526. https://doi.org/10.1016/j.eij.2024.100526

Vardhan, H., Sakshi, Reddy, S. G., Muniraj, I., & Kumar, R. (2024). A symmetric optical cryptosystem based on QZ decomposition and Hermite Gaussian beam speckles. *Optical and Quantum Electronics*, *56*(5). https://doi.org/10.1007/s11082-024-06740-w

Zahra, F. T., Bostanci, Y. S., & Soyturk, M. (2024). LSTM-based jamming detection and forecasting model using transport and application layer parameters in Wi-Fi based IOT Systems. *IEEE Access*, *12*, 32944–32958. https://doi.org/10.1109/access.2024.3371673.