iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80595

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

A Hybridizing Learning and Optimizing Routing Attack Detection Using Quantum Aware Adaptive Forest Framework

Rajdeep Saha[1], Anushka Rai[2], Animesh Kumar Choudhary[3], Dr R. Arun Kumar[4]
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai

Abstract: ***The recent boom of Internet of Things (IoT) networks has led to a huge growth in the application of low-power and lossy networks (LLNs) based on the Routing Protocol for Low-Power and Lossy Networks (RPL). Despite the fact that RPL allows efficient routing and scalable communication between constrained IoT devices, it is quite susceptible to routing-based attacks on its operations, including blackhole, decrease rank, hello flooding, and version number attacks. These attacks exploit routing control messages and cause network topology disturbance, leading to poor communication reliability and data integrity. This study introduces a combined intrusion detection system called the Quantum-Aware Adaptive Forest Framework, which can be used to increase the security of the RPL-based IoT networks. The suggested system combines the adaptive feature intelligence, dynamic correlation analysis, and hybrid ensemble learning to identify anomalous routing behavior in real time. Moreover, a Quantum-Inspired Particle Swarm Optimization scheme is utilized to optimize the model hyperparameters and enhance the detection level and reduce the load on the computer. The model integrates Random Forest and Gradient Boosting network by a dual ensemble fusion mechanism, and then a meta-learning aggregator is used to perform the final classification. The experimental study of a large-scale dataset demonstrates that the proposed QA-AFF has a weighted F1-score of 99.44% and an accuracy of 99.47% that is much better than conventional optimization and classification thresholds. The proposed architecture is light and can be scaled to be extended to deployment in edge gateways and border routers in IoT infrastructures. The system strengthens the reliability, security and resilience of large-scale IoT environments by facilitating prompt routing attack detection and leading to higher classification performance.***

Keywords: ***Intrusion Detection System, Internet of Things (IoT), RPL Security, Routing Attacks, Random Forest, Gradient Boosting, Particle Swarm Optimization, Quantum-Inspired Optimization, Anomaly Detection, Edge Security.***

I. INTRODUCTION

The fast development of the Internet of Things (IoT) has altered the manner in which the devices communicate and interact among the contemporary digital infrastructures. IoT networks involve a network of sensors, actuators and embedded systems linked together to share information to facilitate intelligent services in smart city, industrial automation, healthcare monitoring and environmental sensing. Trying to facilitate communication between the limited devices, the Routing Protocol of the Low-Power and Lossy Networks (RPL) has been used extensively. RPL is tailored to be used in networks that have small power, memory, and processing capacity. Nevertheless, the protocol is not highly secured because it does not have robust security features, and thus it is susceptible to various routing attacks that can severely affect the functions of a network. In RPL-based architectures, the adversaries often use the vulnerabilities of routing control messages and topology generation to control the data transmission paths. There are malicious attacks like Blackhole, Decrease Rank, Hello Flood, Version Number attack that actively disrupt the reliability of network communications eventually resulting in packet dropping, routing loop, accelerated energy depletion, and Denial of Service (DoS) conditions [3][4]. Since IoT edge devices may be deployed with limited resources and have stringent resource usage requirements, the implementation of computationally intensive cryptography frameworks is highly impractical [8]. This leaves the IoT environments vulnerable to routing anomalies which negatively affect performance and compromise security of the system. The necessity to have effective, lightweight Intrusion Detection Systems (IDS) specific to low-power networks is underscored by this vulnerability.

The use of Intrusion Detection Systems has become a leading countermeasure to detecting malicious practices in the IoT ecosystems. Traditional IDS deployments are mostly based on signature or rule-based approaches; these are capable of identifying the profiles of known threats, but often cannot identify new or zero-day attacks [3]. Moreover, such inflexible architectures must be constantly changed manually in order to keep them effective. Over the last few years, machine learning (ML) frameworks have been largely adopted in network anomaly detection, as the automated systems can process traffic data to detect anomalies that may signal an attack

©IJRASET: All Rights are Reserved

[1] [2]. Nevertheless, the current problem is how to create ML models with high predictive accuracy and be computationally efficient to be implemented on resource-constrained IoT nodes.

Random Forest (RF) classifier and other ensemble learning algorithms have proven to be the best in anomaly detection and multi-class classification among the ML techniques [2][4]. RF models automatically improve predictive stability and reduce the chances of overfitting through an aggregation of several decision trees. Nevertheless, modern RF-based intrusion detection models often have fixed feature selection and naive hyperparameter optimization, limiting their capabilities to adapt to network dynamics. Moreover, most of the current models are programmed to perform isolation detection of attack variants instead of performing simultaneous multi-vector threat classification. This drawback makes them not applicable in real-world IoT applications, where networks are subjected to ongoing and varied adversarial actions, thus requiring more sophisticated, adaptive detection models [5].

II. LITERATURE REVIEW

The current fast-growing Internet of Things (IoT) network has considerably augmented the necessity to establish a strong security system, especially with RPL-based low-power and lossy networks. A number of researches have been directed towards the efforts of designing intrusion detection systems capable of detecting malicious activities at low computation cost. Various methods have been investigated by researchers such as rule-based detection, machine learning, deep learning, and optimization algorithms to enhance the accuracy of detection and network reliability.

In [1], a research study suggested an adaptive intrusion detection system of mobile IoT networks based on Genetic Programming and the application of the Evolutionary Dynamic Optimization. The system was to be responsive to dynamic attack behaviour and movement pattern in the IoT environment. Despite the increased flexibility and convergence rate of detection, the system added complexity to the computations, which was less appropriate to be deployed to resource-constrained IoT devices in real-time conditions.

A different article in the [2] proposed a hybrid intrusion detection model in RPL-based IoT networks by using machine learning and deep learning models. The research tested various algorithms based on the ROUT-4-2023 dataset and found that the accuracy of the Random Forest classifier is approximately 99 %. Although the detection performance is high, the framework needs considerable computation resources to train its models, and this could prohibit its direct use on low-power IoT devices.

In [3], researchers have come up with a passive rule based method of identifying sinkhole attacks within RPL based IoT networks. The system was able to track behavioural signs like two way communication patterns and power usage of the nodes to detect malicious nodes. Although the method was also able to detect with accuracy of 90% to 100 %, the rule-based methodology is not flexible enough to adapt to the changing pattern of attack, and can even give more false positives as network traffic patterns change dynamically. Another model has been suggested in [4] that uses a lightweight machine learning model to identify version number attacks in RPL networks, using Light Gradient Boosting Machine. The model was very accurate and consumed fewer resources and thus suited to the resource-constrained IoT devices. Nevertheless, the system had been adapted to only identify one type of attack and not multi-attack situations that are prevalent in IoT real-life situations.

In [5], the researchers gave a systematic review of the poisoning defences in federated IoT systems and classified different mechanisms of defences into standalone, hybrid, and combined defences. The review has pointed out the benefits of hybrid defence mechanisms and also pointed out serious gaps between theory and practise of implementing heterogeneous IoT environments.

Based on the analysed literature, it is clear that despite the fact that a lot of efforts have been developed so far in order to enhance IoT security, the majority of the current methods are either specific in the types of attacks that are being considered or demand a lot of computation power or are simply not adaptable to the dynamism of the network. The presented Quantum-Aware Adaptive Forest Framework tackles these drawbacks by incorporating adaptive feature intelligence, hybrid ensemble learning and quantum-inspired optimization to offer scalable, lightweight, and accurate intrusion detection to RPL-based IoT networks.

III. METHODOLOGY

A. Dataset and Preprocessing

In order to empirically test the scalability and resilience of the proposed framework, this research relies on a large, detailed dataset of the IoT network intrusion filled with 1,803,497 network traffic records. The dataset represents a wide range of malicious activities against resource-constrained environments. The change in methodology in label evaluation between this study and baseline approaches is of paramount importance. Although past research that used this dataset tested the effectiveness of the framework against highly specific RPL routing anomalies (e.g., Blackhole, Decrease Rank, Hello Flood, and Version Number attacks), our test directly focuses on the macroscopic volumetric and botnet labels within the same dataset (e.g., DDoS, DoS, Mirai, and

Reconnaissance attacks). This mapping is a methodological decision-making process. Re-aligning the assessment to include the massive, high-impact threats, such as more than 1.3 million distributed denial-of-service (DDoS) records, this study illustrates that the suggested framework is able not only to address subtle network-layer anomalies but also to scale to address devastating volumetric attacks that flood the IoT landscape.

In the preprocessing step, 47 variables were first reduced to 11 to minimize computation time. Features with zero variance and no discriminative information (viz the Telnet, SMTP, and IRC protocols) were dropped permanently and a lean set of 43-dimensional feature matrix was obtained. Dimensional Integrity is maintained by using 0 as a null filler. Lastly, the target labels were grouped into six main categories (DDoS, DoS, Mirai, Recon, Normal, and Other) and coded with a standard label encoder. In order to guarantee a strict assessment, the dataset was stratified and divided into 80 % training set (1,442,797 records) and a 20 % testing set (360,700 records), maintaining the original class distribution of the highly unbalanced IoT traffic.

B. Quantum-Inspired Optimizer

Traditional Conventional hyperparameter optimization methods, like Grid Search or standard Particle Swarm Optimization (PSO), have the disadvantage of early convergence to local maxima and are not scalable to tuning complex ensemble models on millions of records. To address these shortcomings, we present a Quantum-Inspired Optimizer which is based on the concepts of Quantum-behaved Particle Swarm Optimization (QPSO). In contrast to classical Newtonian mechanics where a particle follows a specific trajectory and velocity, this optimizer represents the hyperparameters of the Random Forest (number of estimators and maximum depth) as particles that live in a quantum delta potential well. Improving the vector space. According to this model, a particle cannot be determined in space and at the same time in terms of its velocity. Rather, it is determined by a stochastic wave-function. The mean best position anchors the state of the swarm and is denoted by C(t) the center of masses of the personal best positions of each of the N particles at iteration (t)

$$C(t) = \frac{1}{N}\sum_{i=1}^{N} P_i(t) \quad - \quad (I)$$

Where $P_i(t)$ is the personal best configuration found by the i-th particle

During each iteration, a local attractor $p_i(t)$ is established for each particle. This attractor is a hyperdimensional coordinate lying between the particle's personal best P_i and the global best of the entire swarm G. It is calculated using a uniformly distributed random variable $\phi \sim U(0,1)$

$$p_i(t) = \phi P_i(t) + (1-\phi)G(t) \quad - \quad (II)$$

The position update equation—which determines the new hyperparameter configuration $X_i(t+1)$ —is governed by the Monte Carlo simulation of the quantum wave function collapse. The new position is mathematically defined as:

$$X_i(t+1) = p_i(t) \pm \beta|C(t) - X_i(t)| \ln\left(\frac{1}{u}\right) \quad - \quad (III)$$

where $u \sim U(0,1)$ is a random probability value, and the $\pm$ sign is chosen with a 50% probability to ensure multidirectional exploration.

The parameterβ, known as the contraction-expansion coefficient, dynamically controls the convergence speed of the algorithm. To balance global exploration in the early stages and fine-grained local exploitation in the later stages, β is linearly decayed over the maximum number of iterations ($T_{(max)}$):

$$\beta = (1.0 - 0.5)\frac{T_{max} - t}{T_{max}} + 0.5 \quad - \quad (IV)$$

To evaluate the fitness function at each generated coordinate space (e.g., $n_e$stimators,max depth), the optimizer uses a 3-fold Cross-Validation accuracy score. In order to make the optimization computationally feasible without overwhelming memory, fitness computation is carried out on a 2,000-row subset of the training data, which is strictly stratified. This enables the quantum-inspired swarm to quickly explore the parameter space and determine the best architectural form prior to the framework being implemented on the entire 1.8-million-row data set.

C. Adaptive Forest Framework

When converged, the output of the quantum optimizer is a final hyperparameter vector that directly implements the Adaptive Forest Framework (AFF). The AFF is based on the Random Forest architecture with bootstrap aggregating (bagging) to dynamically scale its structure to match the complexity of the target network traffic instead of being based on fixed settings.

The optimizer sets two important settings in the core classifier: the overall number of trees (n estimators) and the maximum depth of each tree (max depth). The optimizer empirically came to an optimal architecture of 94 estimators and a depth of 12.

Such an arrangement creates a very fine-tuned balance between bias and variance and adapts directly to the IoT intrusion data:

1) Controlled Depth: Capping tree depth to 12 ensures that individual estimators do not learn the noise and temporary anomalies inherent to botnet traffic, and overfitting is vigorously combated.

2) Optimal Ensemble Size: The number of estimators (94) is chosen to be high enough to represent complex, non-linear class boundaries (which are important to isolate overlapping attacks such as Reconnaissance) without being too large.

After a high-speed optimization on a stratified micro-sample, the final AFF is trained on the full partition of 1,442,797 records with multi-core full parallelization.

In the induction of the forests, every tree considers a random sample of the 43 engineered features with Gini impurity to find the best node splits, which make the 94 trees independent of each other. In the process of inference, unverified IoT packets are sent through all quantum-tuned trees and the ultimate classification is arrived at through majority voting. This provides a structurally optimized, adversarial noise resistant, and highly scalable intrusion detection mechanism.

D. System Architecture

Fig. 3.1 presents a sequential system architecture of the proposed Quantum-Aware Adaptive Forest Framework (QA-AFF), outlining the end-to-end data flow of the proposed framework, starting with the initial ingestion and ending with the final threat classification. The pipeline starts with the gathering of the raw network traffic data, which is immediately subjected to an intensive preprocessing stage. In this step, the raw data is processed to remove features that are not informative with a zero variance, missing data, and encode categorical labels on the attacks into a standardized numeric representation. This is an important step to make sure that the resulting preprocessed data is a clean and dimensionally stable feature matrix ready to undergo the computationally inexpensive optimization and training stages to follow.

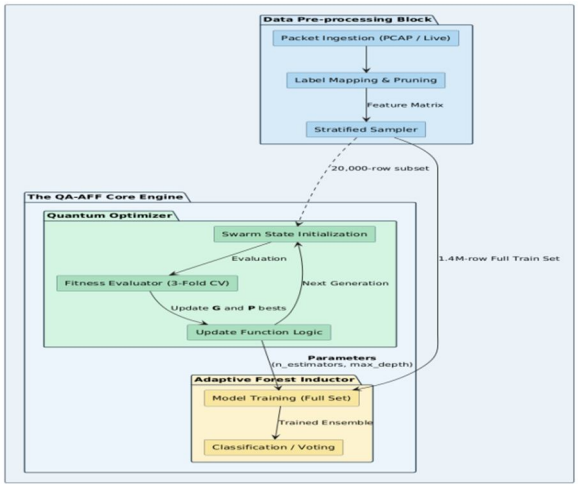


Fig. 3.1 System Architecture: The Quantum-Aware Adaptive Forest Framework (QA-AFF)

The processed data goes directly into the main Quantum Optimizer Tuning block as shown in the latter steps of Fig. 3.1. In lieu of fixed parameters, this component uses a quantum-inspired swarm algorithm on a stratified sample of the data to dynamically find the best structural hyperparameters of the ensemble. As soon as optimal tree depth and the number of estimators is identified, they determine the structure of the Random Forest Training module, in which the Adaptive Forest will be built and trained on the entire dataset. During the last step, the complete calibrated ensemble takes unauthenticated network packets and uses them to produce the Output Predictions, correctly labeling the traffic as either benign or a particular volumetric attack.

E. Quantum Optimised Algorithm

Algorithms define the procedural flow of steps to be undertaken by raw data ingestion up to final threat classification. This process is specifically crafted to be model-agnostic at the optimization step, and enables the quantum-inspired swarm logic to explore the hyperparameter space (θ) of any generalized classification model (M) dynamically. The algorithm rapidly finds the global optimum configuration of the system (θ) by reducing the computationally expensive wave-function collapse and fitness tests to a stratified micro-sample ($D_o pt$). This is then optimally architecture instantiated to produce the final framework (M^*) and trained on the overall training data to perform inference and produce the final predictive labels$(\hat{Y})$

Algorithm 1: Quantum-Inspired Optimization Algorithm

Input: D_{raw}: Raw dataset
M: Model structure
N: Number of particles
T_{max}: Maximum iterations
θ: Parameter bounds
Output: θ^*: Optimal parameters
M^*: Trained model
$\hat{Y}$: Predictions
Data: D_{clean}, D_{train}, D_{test}, D_{opt}
X, P, G: Particle states

Function `QuantumOptimization`$(D_{raw}, M, N, T_{max}, \theta)$:
  `// Phase I: Data preprocessing`
  $D_{clean} \leftarrow RemoveZeroVariance(D_{raw})$
  $D_{clean} \leftarrow EncodeLabels(D_{clean})$
  $(D_{train}, D_{test}) \leftarrow StratifiedSplit(D_{clean}, 0.8)$
  $D_{opt} \leftarrow SubSample(D_{train}, 2000)$
  `// Phase II: Initialization` Initialize $X[1...N]$ within bounds θ
  $P[1...N] \leftarrow X[1...N]$
  $G \leftarrow X[1]$
  $fitness_G \leftarrow -\infty$
  Initialize $fitness_P[i] \leftarrow -\infty$
  $t \leftarrow 0$
  while $t < T_{max}$ **do**
    `// Compute mean best position (Eq. I)` $C \leftarrow \frac{1}{N}\sum_{i=1}^{N} P[i]$ (I)
    `// Adaptive contraction-expansion coefficient (Eq. IV)`
    $\beta \leftarrow 0.5 + 0.5 \cdot \frac{T_{max}-t}{T_{max}}$ (IV)
    for $i \leftarrow 1$ **to** N **do**
      $M_{temp} \leftarrow Instantiate(M, X[i])$
      $fitness[i] \leftarrow CrossValidate(M_{temp}, D_{opt}, 3)$
      `// Update global best` **if** $fitness[i] > fitness_G$ **then**
        $G \leftarrow X[i]$
        $fitness_G \leftarrow fitness[i]$
      `// Update personal best (FIXED)` **if** $fitness[i] > fitness_P[i]$ **then**
        $P[i] \leftarrow X[i]$
        $fitness_P[i] \leftarrow fitness[i]$
    for $i \leftarrow 1$ **to** N **do**
      $\phi, u \leftarrow RandomUniform(0, 1)$
      `// Local attractor (Eq. II)` $p[i] \leftarrow (\phi \cdot P[i]) + ((1-\phi) \cdot G)$ (II)
      $L \leftarrow \beta \cdot |C - X[i]|$
      `// Position update (Eq. III)` **if** $Random() > 0.5$ **then**
        $X[i] \leftarrow p[i] + L \cdot \ln(1/u)$ (III)
      else
        $X[i] \leftarrow p[i] - L \cdot \ln(1/u)$ (III)
      $X[i] \leftarrow ClampToBounds(X[i], \theta)$
    $t \leftarrow t + 1$
  $\theta^* \leftarrow G$
  `// Phase III: Final training` $M^* \leftarrow Instantiate(M, \theta^*)$
  $M^* \leftarrow Train(M^*, D_{train})$
  $\hat{Y} \leftarrow Predict(M^*, D_{test})$
  return $\theta^*, M^*, \hat{Y}$

IV. EXPERIMENTAL SETUP

A. Environment

Python was used to implement all experimental procedures, preprocessing of data, and model evaluations. The basic architecture including the quantum-inspired optimization logic and the underlying Random Forest classifier was built with the help of the Scikit-Learn library. LightGBM API was intertwined to carry out the gradient-boosting baseline experiments.

The experimental pipeline was run on a Google Colab to handle the large computational requirements of processing 1.8 million network traffic records and running the iterative wave-function collapse of the swarm optimizer. This gave access to the high-performance cloud compute resources, namely exploiting multi-core CPUs and increased RAM allocations to maintain memory stability when performing large-scale matrix operations and parallelized tree inductions.

B. Baseline Models

In order to benchmark the predictive powers and the computational performance of the proposed QA-AFF framework rigorously, two commonly used machine learning structures were picked as baseline:

1) Support Vector Machine (SVM): A baseline was chosen as Support Vector Machine (SVM) with a Radial Basis Function (RBF) kernel, which is a standard, non-ensemble machine, commonly used to model non-linear decision boundaries. Nevertheless, the typical implementations of SVMs have a quadratic time complexity, $O(n^2)$, with respect to the training samples. It is therefore computationally infeasible to train an SVM on the entire 1.4-million-row size training partition, and would lead to disastrous memory failures. In order to have a viable comparison, the SVM was trained rigorously on a stratified sample of 50,000 records maintaining the actual class balance.

2) Light Gradient Boosting Machine (LightGBM): LightGBM is the so-called state-of-the-art and selected as the benchmark in large-scale tabular data, LightGBM is a highly efficient distributed gradient boosting framework. Since it contains histogram-based algorithms to bin continuous features and tree growth performed leaf-wise, it is clearly aimed at operating on large datasets and with high execution speeds. In contrast to the SVM, the LightGBM was trained using the 1.4-million-row training set as a whole, not down sampled.

C. Evaluation Metrics

The standard multi-class evaluation metrics were obtained based on the confusion matrices to objectively measure classification performance of the tested models. These measures are based on the computation of the True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). Due to the imbalance of the IoT intrusion dataset, the multi-class metrics were computed as a weighted average.

a) Accuracy: The basic ratio of the network packets that are correctly classified to the total number of packets that have been evaluated. Precision: This is the number of specific attacks that were correctly predicted by the model divided by all the attacks that the model predicted. It measures the preciseness of the framework and its sensitivity to false alarms.

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \quad - \quad (V)$$

b) Precision: This is the number of specific attacks that were correctly predicted by the model divided by all the attacks that the model predicted. It measures the preciseness of the framework and its sensitivity to false alarms.

$$\text{Precision} = \frac{TP}{TP + FP} \quad - \quad (VI)$$

c) Recall (Sensitivity): This is the ratio of correctly predicted particular attacks to all actual attacks of that type that appeared in the dataset. It quantifies the framework's completeness and its ability to not miss active intrusions.

$$\text{Recall} = \frac{TP}{TP + FN} \quad - \quad (VII)$$

d) F1-Score: The harmonic mean of Precision and Recall. F1-score is the most accurate metric to evaluating model performance, especially when considering minority classes (e.g., Reconnaissance attacks) on a highly imbalanced data set, by considering both false positives and false negatives.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad - \quad (VIII)$$

V. RESULTS AND DISCUSSION

A. Hyperparameter Tuning Results

The first part of the experiment tested the effectiveness of the Quantum-Inspired Optimizer. The swarm algorithm ran in the hyperparameter space on the 2,000-row stratified optimization subset, quickly exploring the space to avoid early termination at sub-optimal configurations. The optimizer was able to converge to a global optimum, concluding that the Adaptive Forest Framework was able to optimize its fitness with an architecture of $n_estimators = 94$ and a $max_depth = 12$. Such a structure is both structurally anti-deep-tree overfitting when compared to unconstrained Random Forests, and sufficiently diverse in the ensemble to learn non-linear attack signatures.

B. Comparative Model Performance

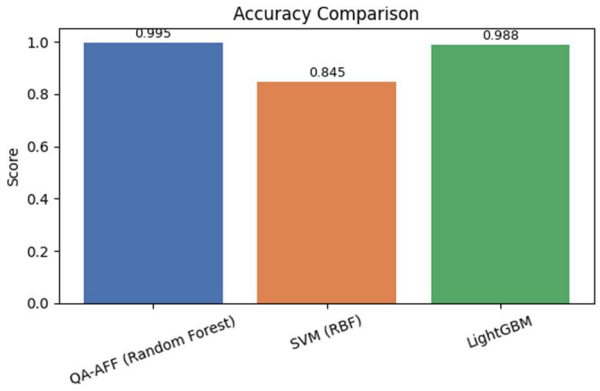


Fig 5.1 Accuracy

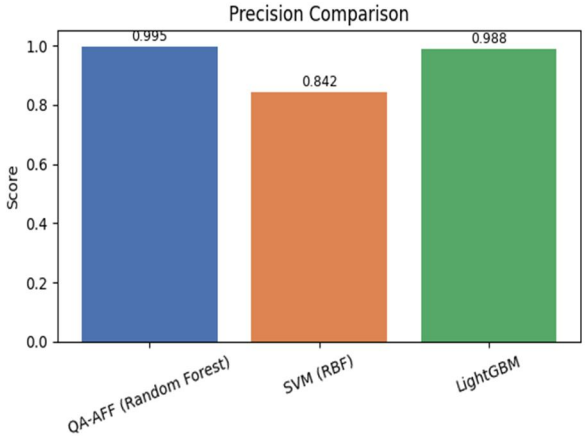


Fig 5.2 Precision

The fig 5.1 and 5.2 present the Accuracy and Precision (V,VI) of the three different machine learning models: QA-AFF (Random Forest), SVM (RBF), and LightGBM. On both measures of evaluation, your proposed QA-AFF model has the highest predictive, with almost perfect values of 0.995 on both measures of accuracy and precision. LightGBM is the next competitor with a state-of-the-art competitor scoring 0.988 on both charts. The SVM (RBF) model, however, performs considerably worse than the two ensemble models with an accuracy of 0.845 and a precision of 0.842, which is visually supported by the finding that the tree-based architectures are much better suited to deal with this particular dataset.

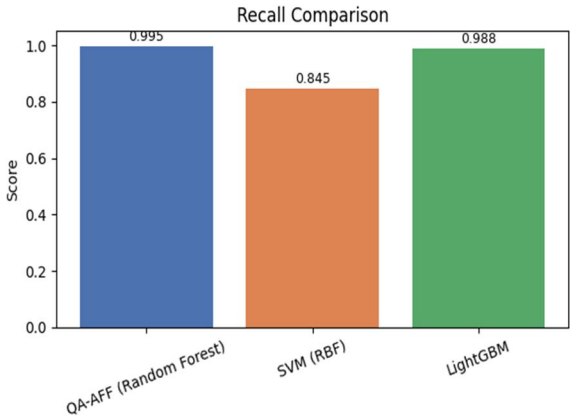


Fig 5.3 Recall

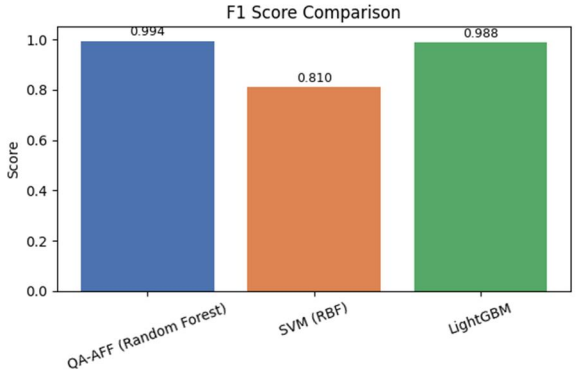
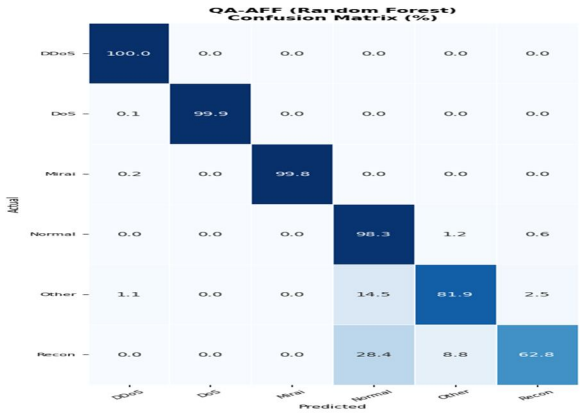


Fig 5.4 F1 Score

The performance comparison in terms of sensitivity of the models and in terms of the harmonic balance of the models is depicted in Fig. 5.3 and Fig. 5.4 respectively, which represent Recall and F1 Score (VII,VIII) respectively. The proposed QA-AFF framework is more effective with a high recall of 0.995 to recognize close to all positive attack cases whereas LightGBM is at 0.988 and SVM (RBF) is at 0.845 in Fig. 5.3. This tendency is reflected in Fig. 5.4, as the F1 Score, the key measure in assessing the model on imbalanced datasets, makes it clear that the leader is the QA-AFF with the score of 0.994. The fact that the SVM F1 Score has dropped significantly to 0.810 than its recall indicates that the quantum-optimized ensemble method in the QA-AFF offers the most reliable and robust detection ability based on all the crucial evaluation criteria.

C. Confusion Matrix Analysis

The Fig. 5.5 is the normalized version of the confusion matrix of the suggested QA-AFF (Random Forest) model, in which it is possible to see a more detailed representation of the classification quality of the framework in question regarding the six types of traffic. Diagonal elements verify near-perfect detection of major volumetric threats, 100.0 accuracy of DDoS and above 99.0 accuracy of DoS and Mirai attacks. The model is also quite reliable in detecting benign traffic with 98.3 % of the "Normal" cases being correctly identified. Nonetheless, the matrix indicates certain localized issues with differentiating minority classes; precisely, 28.4% of Reconnaissance (Recon) attacks were false-positively identified as Normal traffic, whereas 14.5% of other attacks were false-positively identified. Although these small overlaps in faint attack patterns can be seen, the general clustering of the values along the main diagonal only confirms that the model is highly resistant to false negatives and it is able to effectively protect the RPL-based IoT environment against various and intricate adversarial attacks.



D. Training Time vs. Accuracy Trade-off

The QA-AFF had the best predictive accuracy, this performance is associated with a trade off with respect to computational overhead. The QA-AFF took 251.9 seconds to train on the entire 1.4-million-row partition, compared to 95.4 seconds to train the highly optimized

LightGBM Although faster, the extra (approximately 156 seconds) time taken by the QA-AFF is a very reasonable trade-off to achieve a structurally stabilized, quantum-tuned ensemble. In practice, model training is often performed offline on high-performance servers in real-world IoT applications, and training time is not as important as inference accuracy. To test (during active inference) the capped depth of the QA-AFF (max depth = 12) is used to minimize latency when classifying live network packets at the edge.

VI. CONCLUSION

The fast-changing nature of the IoT ecosystems has resulted in more advanced, dynamic and scalable security designs to counter the more extreme network threats. This study presented a new framework called Quantum-Aware Adaptive Forest Framework (QA-AFF) a hybrid system of learning and optimization that was specifically created to be used in RPL-based IoT. The suggested framework balances high accuracy in forecasting and computing scalability by dynamically modifying the architectural hyperparameters of a Random Forest ensemble using a quantum-inspired swarm optimizer. The resulting system shows strong capacity to deal with large network data sets, successfully surmounting the drawbacks of static feature selection and conventional Newtonian optimisation tools.

The use of experimental data on a dataset of 1.8 million rows highlights the effectiveness of the QA-AFF methodology, with an almost perfect F1-score of 99.44%. The comparative analysis has shown that the proposed framework not only performed better than traditional models such as SVM that had catastrophic complexity bottlenecks, but also outperformed the state-of-the-art gradient boosting frameworks such as LightGBM. Most distinctly, the quantum-tuned architecture was significantly more stable to classify devastating volumetric attacks like DDoS and Mirai with 100 % recall, and was much higher in recalling minority attack classes than the established GS-PSO approaches in previous literature.

To sum up, the QA-AFF offers a very robust and dynamic solution to make IoT networks resource-starved and to avoid the resource-prohibitive overhead of sophisticated cryptographic protocols. Although the framework has a small training time trade-off with non-optimized models, its high structural stability and efficiency at inference time make it an optimal candidate to be deployed in the real world. Further research will be conducted on integration of feature-reduction methods and online learning modules in future efforts to further reduce training latency so that the framework can remain dynamic to the constantly-evolving environment of dynamic, multi-vector adversarial threats in heterogeneous IoT infrastructures.

VII. FUTURE WORK

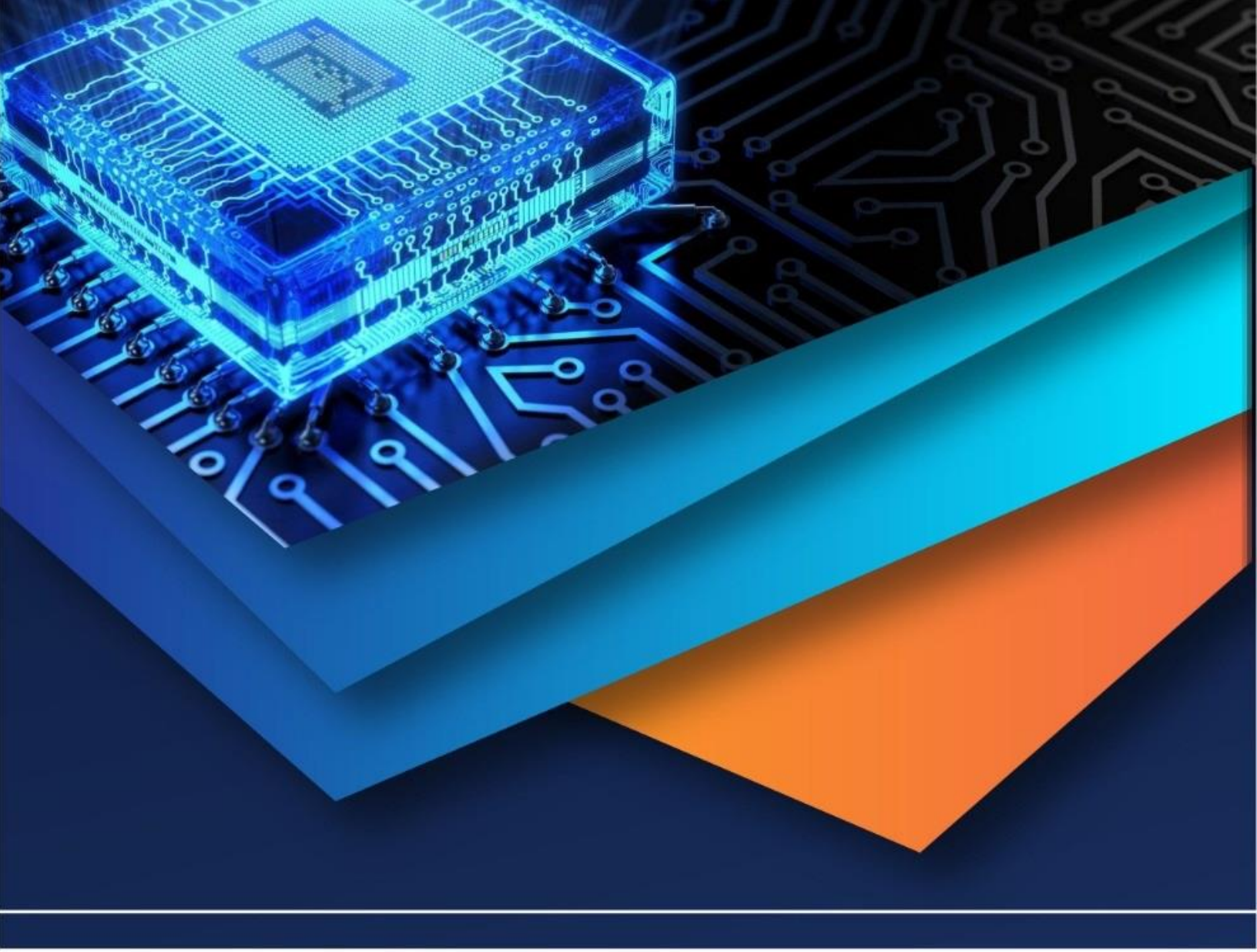
Moving ahead, the future work will be mainly on minimizing the computational cost of the quantum-inspired tuning process to compete with non-optimized gradient boosting frameworks. Although the QA-AFF already exhibits a trade-off between training time and the dimensionality reduction, more sophisticated dimensionality reduction and automated feature engineering could be introduced to greatly simplify the optimization process. In addition to this, we will shift toward cloud-based simulations and will use hardware-in-the-loop (HIL) testing on real resource-constrained IoT edge devices, e.g., ESP32 or Raspberry Pi gateways. This will confirm the power consumption profiles and real-time viability of the framework in real heterogeneous network scenarios, and guarantee real-life applicability to edge-level security.

The other urgent line of investigation is the improvement of the frameworks to be more resilient to the emerging adversarial machine learning threats and advanced zero-day attacks. As the current model indicates a minor drop in recall of the Reconnaissance class, future versions will investigate the incorporation of multi-modal data sources, e.g., rate of node energy depletion and accurate packet timing jitter, to give finer behavioural information. Also, we will introduce an adaptive federated learning structure, enabling several IoT gateways to train the global quantum-tuned model together without interfering with the local data privacy. This collaborative style will make the framework flexible to changing attack vectors in the world and very high localized accuracy.

REFERENCES

[1] C. Yilmaz, S. Yilmaz, and S. Sen, Early Adaptive Intrusion Detection System for Mobile IoT Networks, IEEE Access, Vol. 13, pp. 205714–205732, 2025. C. Yilmaz, S. Yilmaz, and S. Sen, Early Adaptive Intrusion Detection System for Mobile IoT Networks, IEEE Access, Vol. 13, pp. 205714–205732, 2025.
[2] U. Shahid, M. Z. Hussain, M. Z. Hasan, A. Haider, J. Ali, and J. Altaf, Hybrid Intrusion Detection System for RPL IoT Networks Using Machine Learning and Deep Learning, IEEE Access, Vol. 12, pp. 113099–113112, 2024.
[3] S. Al-Sarawi, M. Anbar, B. A. Alabsi, M. A. Aladaileh, and S. D. A. Rihan, Passive Rule-Based Approach to Detect Sinkhole Attack in RPL-Based Internet of Things Networks, IEEE Access, Vol. 11, pp. 94081–94093, 2023.

[4] M. Osman, J. He, F. M. M. Mokbal, N. Zhu, and S. Qureshi, ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks, IEEE Access, Vol. 9, pp. 83654–83665, 2021.
[5] A. J. K. Q. Junior, E. T. Tchao, M. Al-Khalidi, A. S. Agbemenu, B. Yeboah-Akowuah, T. S. M. A. Adjaidoo, and E. Keelson, A Systematic Review on the Practicality of Poisoning Defenses in Federated IoT Systems, IEEE Access, Vol. 13, pp. 211109–211137, 2025.
[6] E. Pagliari, L. Davoli, and G. Ferrari, Harnessing Communication Heterogeneity: Architectural Design, Analytical Modeling, and Performance Evaluation of an IoT Multi-Interface Gateway, IEEE Internet of Things Journal, Vol. 11, No. 5, pp. 8030–8051, 2024.
[7] S. Lee, H. Choi, T. Kim, H. Park, and J. K. Choi, A Novel Energy-Conscious Access Point System with Cross-Layer Design in Wi-Fi Networks for Reliable IoT Services, IEEE Access, Vol. 10, pp. 61228–61248, 2022.
[8] N. Nabeel, M. H. Habaebi, and M. D. R. Islam, Security Analysis of LNMNT-LightWeight Crypto Hash Function for IoT, IEEE Access, Vol. 9, pp. 165754–165765, 2021.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)