International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(4s) 2026 pp. 468-491
https://doi.org/10.70917/ijcisim-2026-2530
Article

A Post-Quantum Cryptographic Approach for Secure Fine-Grained Access Control in Next-Generation Systems

Harish Parshuram Bhabad [1], Anand Singh Rajawat [2]

Department of Computer Science and Engineering, Sandip University, Nashik, India.
Email:ID: bhabadharish@gmail.com, ORCID ID: 0009-0008-2849-7027
Department of Computer Science and Engineering, Sandip University, Nashik, India.
Email:ID: anandsingh.rajawat@sandipuniversity.edu.in, ORCID ID: 0000-0001-5940-5799

Abstract: The Internet of Things (IoT) and Industrial IoT (IIoT) technologies experience rapid growth, which leads to better data-driven operations in modern systems that especially benefit sustainable supply chain management environments. The systems experience growing threats because hackers develop advanced cyberattacks and quantum computing technology will soon break existing cryptographic methods. The paper presents a solution to the identified problems which establishes a post-quantum security framework that combines Post-Quantum Cryptography (PQC) with Particle Swarm Optimization (PSO) feature selection and hyperparameter-tuned XGBoost classification and Attribute-Based Access Control (ABAC) security solutions. The model operates in IoT-enabled sustainable supply chain systems which need security, trust, resilience to protect their logistics and warehouse and inventory processes. PSO selects the best features to reduce computation requirements while XGBoost improves intrusion detection by categorizing supply chain data traffic into Normal and Malicious and Attack groups. ABAC provides precise access management, which enables secure decision-making based on contextual information for supply chain processes. The experimental results show that the proposed model achieved accuracy of 97.50%, precision of 99.01%, recall of 98.95%, F1-score of 98.98%, and an AUC of 0.997, which exceeds the performance of Random Forest and SVM. The encryption process now takes 120 ms to 40 ms while the decryption process maintains its previous duration

Keywords: IoT, Industrial IoT, Post-Quantum Cryptography, Particle Swarm Optimization, XGBoost, Attribute-Based Access Control.

1. INTRODUCTION

The Internet of Things (IoT) and Industrial Internet of Things (IIoT) and edge computing technologies have developed to provide systems the ability to process data in real time while executing automated intelligent functions [1]. The technologies find their applications in sustainable supply chain management which requires the processing and exchange of extensive data streams [2], [3]. The protection of sensitive information needs secure communication methods together with restricted access procedures. The system requires both detailed access control mechanisms and robust encryption methods to safeguard data confidentiality andintegrity [4], [5]. The increasing number of connected devices brings new security challenges which require upgraded security systems to defend against these threats.

The IoT-enabled sustainable supply chain environment generates multiple data streams from sensors and smart logistics systems which create both high-dimensional and diverse data [6]. The systems encounter major security problems because cyberattacks have increased and quantum computing technology has emerged [7]. Traditional cryptographic techniques become vulnerable to quantum attacks which endanger secure communication methods [8], [9]. The distributed supply chain system design creates problems which affect trust and data integrity and access control mechanisms [10]. The presence of redundant data and lack of efficient processing further increase

computational complexity. The challenges faced by supply chain security operations lead to decreased security and operational reliability.

The existing solutions to these problems include Attribute-Based Encryption (ABE) Ciphertext-Policy ABE (CP-ABE) blockchain-based access control and Post-Quantum Cryptography (PQC). The machine learning models Support Vector Machine (SVM) Random Forest (RF) Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) help detect intrusions [11]. The methods function as separate units because they do not connect their encryption and feature optimization and intelligent classification processes [12]. The system requires extensive processing power while it can only function in fixed environments, which makes it unsuitable for real-time supply chain protection [13].

To overcome these limitations, this paper proposes an improved post-quantum security framework that integrates PQC, Particle Swarm Optimization (PSO)-based feature selection, XGBoost classification, and Attribute-Based Access Control (ABAC). The framework provides secure communication and efficient data processing for IoT-enabled sustainable supply chain systems. XGBoost improves intrusion detection accuracy, while ABAC provides fine-grained access control. The novelty of this work lies in combining quantum-resistant cryptography with intelligent machine learning and access control in a unified framework which delivers improved security trust and supply chain environment resilience. The Key Contributions are:

- To critically analyze existing blockchain-based and post-quantum cryptographic models used for security and sustainability in supply chain management systems.
- To identify the limitations and security vulnerabilities of conventional and pre- quantum approaches in IoT-enabled sustainable supply chain environments.
- To design an improved post-quantum security framework for enhancing security, trust, and resilience in sustainable supply chain systems.
- To develop an intelligent intrusion detection model using PSO-based feature selection and XGBoost classification for accurate threat detection.
- To implement fine-grained and context-aware access control using Attribute-Based Access Control (ABAC) in supply chain environments.
- To evaluate the performance of the proposed model in terms of accuracy, precision, recall, latency, and overall security effectiveness.

The following structure is used for the rest of the paper. The first part is Section 2 which shows a thorough survey of the literature and the studies in the corresponding domain. The second part is Section 3 that outlines the suggested approach and system architecture. Next, in Section 4, the results of the experimentation along with performance evaluation are presented and discussed. To finish, Section 5 gives the conclusion and future research areas.

2. Related Works

R. Ganesh et al. [14] gave a comprehensive examination of the Advanced Encryption Standard (AES), which included the topics of structure, key management, security assessment, and obstacles from quantum computing. Their investigation pointed out the requirement of quantum-proof encryption methods in present-day communication systems. Z. B. Jemihin et al. [15] investigated Attribute-Based Encryption (ABE) as a solution for the big-data security problem under the aspect of post-quantum technology. They remarked that ABE allows very precise access control to the data, but at the same time background schemes are still exposed to quantum attacks, thus it becomes clear that the integration of PQC is necessary for the creation of future-proof systems.

K. K. Singamaneni and others, presents a quantum-crypto standard hybrid was suggested for 6G-enabled IoT networks in their article [16]. Despite the fact that the proposed technique displayed improved security and robustness, there were no intricate mechanisms for dynamic access control based on user attributes that would support the merging of PQC with fine- grained access policies. Y. Chen et al. [17] introduced a blockchain-based fine-grained access control model, emphasizing the ability to manage both capabilities and access rights. Their scheme is capable of making secure access decisions, yet the combination with PQC is still a challenge.

S. Li et al. [18] presented the discussion on post-quantum security, regarding the opportunities as well as the challenges. They mentioned the advantages that quantum computers will have over classical encryption and how it will be substantial that practical PQC gets deployed in IoT and cloud systems. Shruti et al. [19] reviewed and discussed the current status of ABE schemes for the upcoming wireless IoT networks and showed that the access control driven by attribute-based policies is very effective. However, they mentioned certain shortcomings regarding high-dimensional network traffic features and the combination of ABE with ML -based attack detection.

A. A. Khan et al. [20] investigated PQC applied to blockchain-based cloud auditing systems, highlighting the importance of multimedia privacy. Their method makes sure the data are protected while not tackling the issue of access request evaluation in real-time under dynamic network settings. M. MahdaviOliaee and Z. Ahmadian [21] dealt with ciphertext- policy attribute-based encryption for very precise flexible access control over arithmetic circuits. Their solution guarantees the security of computing, but at the same time, it does not utilize feature optimization or ML -assisted classification for intrusion detection.

C. Y. Wu and co-workers [22] presented a decentralized multi-authority ABE scheme that is suitable for scalability in IoT access control. Although the framework improves both scalability and security, it is not integrated with post-quantum encryption and automated attack detection mechanisms. W. Wang and colleagues [23] were first to showcase the concept of using a smart contract token-based privacy-preserving access control system for industrial IoT. The created model guarantees accountability and traceability, yet it lacks the implementation of feature selection or classification optimization for the real-time detection of threats.

Within the current research, there is a lot of discourse around attribute-based access control, encryption and post-quantum security for IoT and cloud systems. There is, however, a lack of integrated solutions that combine quantum-resistant cryptography, optimized feature selection, real-time traffic classification, and fine-grained access enforcement in the majority of the works, thus indicating the requirement of a unified, intelligent and future-proof security framework for IoT-enabled sustainable supply chain systems. Table 1 compares existing studies with the proposed framework based on security components.

Table 1. Research Gap Table

Ref	PQC	ML-Based IDS	Feature Selection	ABAC	Supply Chain	Limitation
[14]	✗	✗	✗	✗	✗	Classical encryption only
[15]	Partial	✗	✗	✓	✗	Vulnerable to quantum attacks
[16]	✓	✗	✗	✗	✗	No dynamic access control
[17]	✗	✗	✗	✓	✗	No PQC integration
[18]	✓	✗	✗	✗	✗	Conceptual study
[19]	✗	Partial	✗	✓	✗	No optimized IDS
Proposed	✓	✓	✓	✓	✓	Integrated framework

2.1 Problem Statement

- Access control and encryption methods at present are still classical cryptographic based, which would not be able to stand the quantum computing attacks and therefore no long-term security for next generation systems can be assured [15].
- The majority of the present security frameworks fail to incorporate smart ML –based traffic classification with access control which results in a limited capacity for the real- time detection and mitigation of the malicious activities [19].

- IoT and network traffic datasets containing high-dimensional and redundant features suffer from low classification accuracy and increased computational complexity [22].
- The access control models of today remain very coarse and lack the ability to distinguish between user attributes and system conditions and security threats that have been detected, this joint consideration is still missing [23].

2.2 Challenges Overcome

The unified framework that combines PQC with optimized ML and fine-grained access control is the basis of the proposed work which solves several critical security issues in next- generation systems. It utilizes quantum-resistant cryptographic protocols to eliminate the weakness of classical encryption to quantum attacks, cuts down on the complexity of high- dimensional data via efficient feature-pruning, enhances the real-time spotting of harmful activities through a well-tuned XGBoost classifier, and allows for context-aware access decisions by fusing classification results with attribute-based access control. This results in a system operation that is not only secure and efficient but also future-proof.

3. Methodology

The proposed framework PSO-Optimized XGBoost Framework for IoT Access Classification is as shown in figure 1 its operates in supply chain environments which use IoT technology to create sustainable operations through real-time data collection from their logistics systems and smart warehouses and connected devices. It begins with the acquisition of labeled IoT/IIoT network traffic from the Edge-IIoTset dataset, which is then subjected to cleaning, encoding, and normalization preprocessing to enhance data quality. PSO-based feature selection is used to choose an optimal set of discriminative features in order to reduce the dimensionality and increase the efficiency of the classification process. The features selected are added to user, device, and contextual attributes to create structured access requests, which are then transmitted securely through post-quantum cryptography (PQC) encryption in order to ensure that they are safe from quantum-era attacks. After the decryption, a hyperparameter tuned XGBoost classifier to distinguish between to one of three categories: Normal, Malicious, or an Attack type. A fine-grained access control mechanism enacts allow or deny decisions based on the classification result. There is a complete logging and monitoring of access activities and decisions through security measures for audit and forensic analysis, and the overall effectiveness of the framework is finally assessed with the help of performance metrics such as accuracy, precision, recall, F1- score, and latency.

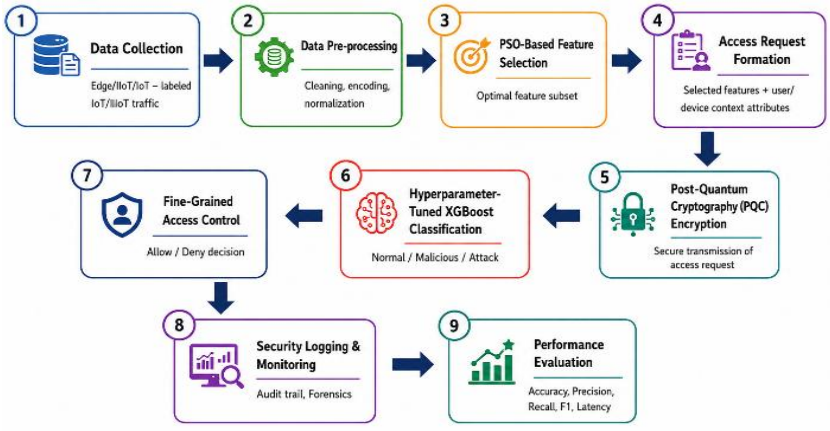

Figure 1: Proposed PSO-Optimized XGBoost Framework for IoT Access Classification

3.1 Data Collection

The dataset used for this study is the Edge-IIoT [24] dataset Cyber Security Dataset of IoT & IIoT, which was exclusively collected from realistic IoT and edge computing testbeds and is available on Kaggle. With its almost 2.2 million records of network traffic, the dataset contains approximately 1.6 million Normal instances and over 600,000 instances of different attacks, among others, and thus covers multiple scenarios envisioned for the next-generation systems. The dataset is rich in metrics, offering a set of 61 features that have been derived from packet, flow, and system levels, thereby making it suitable for both intrusion detection and access control applications. The traffic data

for this study is divided into three main categories: Normal, Malicious, and Attack Type, which facilitates the proposed framework's effective learning and distinguishing between the legitimate activities and the security threats.

Table 2: Class Distribution of Normal and Attack Instances

Class Type	Number of Instances
Normal	1,600,000
Malicious	600,000+
Attack Types	Various categories (e.g., DDoS, MITM, Backdoor, etc.)

Table 2 is true labels of normal instances and various types of attacks in the Edge-IIoT dataset.

3.2 Data Preprocessing

Data pre-processing is an indispensable operation in the suggested framework, which is focused on enhancing the data quality, consistency, and reliability prior to feature selection and classification. Pre-processing guarantees that the ML model will efficiently discover valuable patterns in the dataset and by doing so, it eliminates the risk of errors or biases caused by missing, inconsistent, or unscaled data. In this research, the data pre-processing pipeline involves three fundamental actions: dealing with missing and inconsistent values, conversion of categorical attributes into numerical ones, and scaling of numerical features.

3.2.1 Handling Missing and Inconsistent Values

Network traffic datasets often suffer from missing entries or inconsistencies due to factors like packet loss, measurement errors, or logging problems. If these anomalies are not corrected, they can degrade the performance of the model or introduce bias. At this stage, the missing values are either filled in using statistical methods such as mean, median, or mode or the corresponding records are deleted if they are minor and do not influence the general data distribution. Suppose x_i^{imputed} is a feature with missing values, then it can be filled in using the mean as given in Eq. (1)

$$x_i^{\text{imputed}} = \frac{1}{n}\sum_{j=1}^{n} x_{ij}\,, x_{ij} \in \text{observed values of feature } i \quad (1)$$

This stage will be responsible for ensuring that all available features have numerical entries which can be used during feature selection or modeling protocols.

3.2.2 Encoding Categorical Features

Protocol type, device type, and attack category are examples of categorical features in the dataset that cannot be directly handled by ML algorithms and thus must be transformed into numerical representation. This is accomplished by means of encoding techniques, such as one hot encoding, wherein each category is signified as a binary vector, so that the classifier can comprehend the categorical data without creating any misleading ordinal relationships. By encoding categorical features in this manner, the model is enabled to discover patterns from non-numeric characteristics efficiently, which is a contribution to the precise classification of network traffic into Normal, Malicious, or Attack types.

3.2.3 Normalization of Numerical Features

Numerical characteristics in network traffic data frequently come with variable ranges which could be the case of packet size, flow duration, or byte count, among others. Features having wider ranges may take charge of the learning process and lead the classifier astray. In order to prevent such situations, min-max normalization or z-score standardization is conducted. Min-Max Normalization is given in Eq. (2)

$$x_i^{\text{norm}} = \frac{x_i - x_i^{\min}}{x_i^{\max} - x_i^{\min}} \quad (2)$$

Where, $x_i^{\min}$ and $x_i^{\max}$ are the minimum and maximum value of feature x_i. Z-Score Standardization is given in Eq. (3)

$$x_i^{\text{std}} = \frac{x_i - \mu_i}{\sigma_i} \quad (3)$$

Normalization has been a technique that ensures feature x_i. with its respective mean μ_i and standard deviation σ_i, and all other features participate uniformly and thus, it will be beneficial in speeding up training and making it less prone to errors in ML algorithms.

3.2.4 Data Splitting Procedure

In the beginning, the data set was shuffled randomly to avoid any possible bias that could be caused by the data order. Following this, the data was divided into three non- overlapping groups: 70% of the data was the training set for model building, 15% was the validation set during hyperparameter tuning, and the remaining 15% was the test set. Stratified sampling was applied in all splitting phases to maintain the original class distribution of Normal, Malicious, and Attack traffic in all subsets. Therefore, it ensures a fair evaluation and prevents the performance results from being influenced by the class imbalance.

3.3 Feature Selection Using PSO

Feature selection is an important process that has a very positive impact on ML model performance because it eliminates irrelevant or redundant features thus improving classification accuracy, reducing computational complexity, and enhancing interpretability. In this study PSO has been used to pick out the best features from the Edge-IIoTset dataset for precise classification of network traffic into Normal, Malicious, and Attack types. PSO is based on the social behavior of birds or fish looking for food, where every particle denotes a possible solution in this instance, a feature subset and the swarm collaborates in the search for the best feature combination.

3.3.1 Initialization

Initially, the algorithm assigns random positions and velocities to each particle in the swarm. Particles are represented by different combinations, and their position vector $X_i(0) = \left[X_1^i, X_2^i, \dots, X_D^i\right]$ will reveal the features selected, while the velocity vector $V_i(0) = \left[V_1^i, V_2^i, \dots, V_D^i\right]$ will show the rate and direction of the particle's motion in the feature space. Here, D is the total number of features available in the dataset, and $i = 1,2, \dots, N$ corresponds to each of the particles in a swarm of N members are given in Eq. (4)

$$X_i(0) = \left[X_1^i, X_2^i, \dots, X_D^i\right], \quad T_i(0) = \left[T_1^i, T_2^i, \dots, T_D^i\right] \quad (4)$$

3.3.2 Fitness Evaluation

Each feature subset (particle) is assessed in terms of quality through the use of a fitness function that is determined by the XGBoost classifier's performance. Here, fitness is represented by the classification accuracy of the network traffic into three classes: Normal, Malicious, or Attack, using the features that were selected is given in Eq. (5)

$f(X_i) =$ Accuracy of XGBoost using features X_i (5) This textual component was replaced by- the fitness function favored subsets of features that maximize classification performance while minimizing redundancy.

3.3.3 Velocity Update

Every single particle modifies its velocity taking into account its former velocity, its own best position (P_{best}), and the global best position (G_{best}) that was discovered by the swarm is given in Eq. (6)

$$V_i(t+1) = w \cdot V_i(t) + c_1 \cdot \text{rand}_1 \cdot \left(P_{\text{best}} - X_i(t)\right) \quad + c_2 \cdot \text{rand}_2 \cdot \left(G_{\text{best}} - X_i(t)\right) \qquad (6)$$

Where, w denotes the inertia weight that determines the degree of exploration, c_1 and c_2 are the respective acceleration factors, and $\text{rand}_1, \text{rand}_2 \in [0,1]$ both belonging to the interval of [0,1] add random variation to the process.

3.3.4 Position Update

As velocity is updated, some columns of the position of the article are updated to describe the new subset of candidate features as given in Eq. (7)

$$X_i(t+1) = X_i(t) + V_i(t+1) \qquad (7)$$

This new subset will be re-evaluated at the next iteration to see its dictate on classification performance.

3.3.5 Global Best Update

The particle with the highest fitness is chosen as the global best (G_{best}), which signifies the most optimal subset found by the swarm is given in Eq. (8)

$$G_{\text{best}} = \arg\max_{i} f(X_i) \qquad (8)$$

This position guides the swarm toward convergence on the best feature combination.

3.3.6 Time-Varying Inertia Weight

In the process of searching, the inertia weight $w(t)$ is adjusted in a way that it is decreased at the end of the period using a time-varying function to find the right ratio between exploration and exploitation is given in Eq. (9)

$$w(t) = \exp\left(-\frac{b \cdot t}{T}\right) \cdot b \qquad (9)$$

Where T is the total number of iterations, while b is a parameter that manages the decay rate. This mechanism facilitates the shifting of the swarm from the global search stage to the refinement of the best feature subset stage.

3.3.7 Convergence and Termination

The algorithm stops when a stop criterion is achieved, for instance, reaching a certain number of iterations or obtaining a desired fitness value. At the end, G_{best} is returned as the best feature subset, which will be applied for XGBoost classification and the associated fine- grained access control. The PSO-based feature selection, therefore, guarantees the simultaneous usage of the most informative features by the framework, leading to the enhancement of accuracy, reduction of computational cost, and increase of interpretability in detecting Normal, Malicious, and Attack traffic in the coming generation of IoT and edge networks.

Pseudocode: PSO-Based Feature Selection for Edge-IoT Traffic Classification

Input:	Dataset D with features F, Number of particles N, Max iterations T
Output:	Best feature subset G_{best}
1. Initialize particles	
For each particle i	
Randomly choose features (position X_i)	
Randomly set velocity V_i	
Set personal best $P_{\text{best } i} = X_i$	
2. Evaluate fitness of all particles using XGBoost accuracy	
3. Set global best G_{best} = particle with highest fitness	
4. Repeat for t = 1 to T	
For each particle i	
a. Update velocity	
$V_i(t+1) = w \cdot V_i(t) + c_1 \cdot \text{rand}_1 \cdot \left(P_{\text{best}} - X_i(t)\right) + c_2 \cdot \text{rand}_2 \cdot \left(G_{\text{best}} - X_i(t)\right)$	
b. Update position (feature selection)	
$X_i(t+1) = X_i(t) + V_i(t+1)$	

c. Evaluate fitness with XGBoost
d. Update personal best
If fitness > fitness ($P_{\text{best } i}$)
$P_{\text{best } i} = X_i$
Update global best
G_{best} = particle with highest fitness
5. Stop when max iterations reached
6. Return G_{best} as optimal feature subset

3.4 Access Request Formation

Access Request Formation This is a very significant step that links network traffic classification and fine-grained access control. During this phase, the feature set which has been optimized in the PSO-based feature selection step is integrated with the user/device contextual features to build structured access requests. Every access request is a real-time attempt at interaction by a user or an IoT device and includes chosen traffic characteristics in addition to contextual values like user role, assigned permissions, device type, access time, etc. Access request is semantically rich by allowing both behavioural traffic characteristics and contextual information to make the request semantically rich and evaluate access control on a fine-grained basis. This hierarchical representation allows the system to take finer more dynamic decisions about authorizing a person or entity and only with the pressure of both security classification result and contextual policy criteria met.

3.5 Post-Quantum Cryptography Encryption

Secure communication and access control is important in the era of IoT and edge computing to ensure sensitive data and resources are safeguarded. The existing encryption techniques might not be adequate to protect against a growing quantum computer capability. The proposed framework resolves this by integrating PQC and XGBoost classification and ABAC to ensure the security of access requests in a multi-class classification scenario. Under this practice, the quantum-resistant scheme is used to communicate and ML to classify access requests correctly and in the appropriate context in Figure 2.

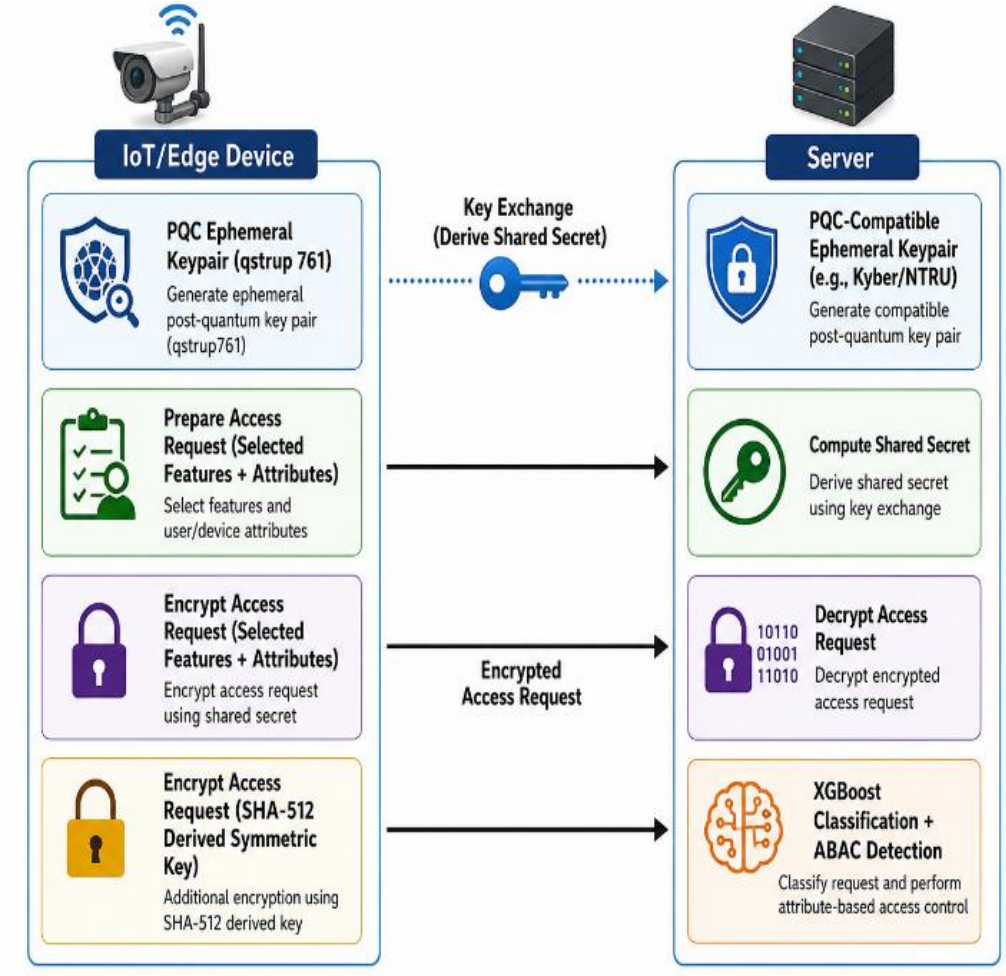

Figure 2: PQC-Based Secure Access Control Framework

The illustration shows the process for securely requesting access between an IoT/Edge device and a server via PQC. First of all, the IoT device makes a PQC temporary keypair and starts the access request by choosing the pertinent features as well as the attributes. After that, the request gets encrypted by PQC encryption together with a SHA-512 derived symmetric key which guarantees the security of data transmission. The server gets the request that is encrypted and then it does a key-exchange using a PQC compatible ephemeral keypair to figure out the secret that is shared. The server then goes on to decrypt the access request and applies XGBoost classification and ABAC to assess the request and enact fine-grained access control. Thus, this whole procedure is able to guarantee that only access requests with approval get through and at the same time offer strong security as well as precise detection of the requests that are malicious or related to attacks.

3.6 Classification using XGBoost

XGBoost has become one of the strongest and most popular algorithms in the classification and regression process in the age of advanced ML methods. XGBoost uses the concept of gradient boosting to construct decision trees sequentially with the aim of reducing errors and enhancing accuracy of prediction. The method provides optimal results when researchers need to analyze extensive and complex datasets. XGBoost is selected due to its high accuracy, scalability, and efficiency in handling large-scale and high-dimensional supply chain data. XGBoost performs multi-classification tasks by combining multiple decision trees to calculate class probabilities through the Softmax function and selects the class with the highest probability for final output. The system delivers effective classification capabilities which solve practical problems according to the information shown in Figure 3.

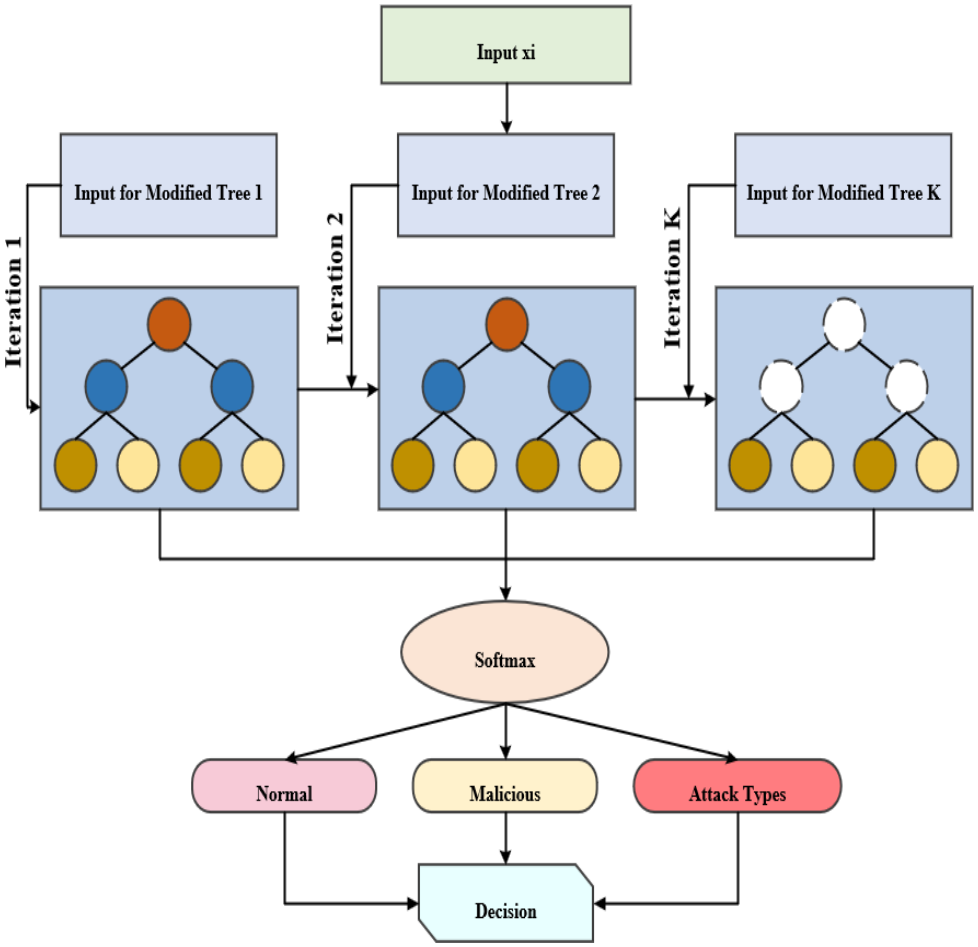

Figure 3: XGBoost-Based Multi-Class Classification Architecture

3.6.1 Input Features

The model takes an input feature set as x_i as the input feature set that indicates a feature vector of the network traffic data. All attributes of the vector are linked to a particular attribute (e.g., size of packets, amount of time spending on a flow, count of bytes) that will be utilized to create predictions. The input feature is given in Eq. (10)

$$x_i = [X_1, X_2, \dots, x_n] \qquad (10)$$

Where n denotes the features number of the dataset.

3.6.2 Decision Trees (Iterations 1, 2, K)

XGBoost algorithm constructs multiple decision trees at a time. The decision tree is trained to the modified one which predicts the class of the input feature at the given input feature x_i. in each iteration. The result of each tree is a raw score also called a logit per class. The response to input x_i of tree k is given in Eq. (11)

$$f_k(x_i) = \text{Logit from Tree } k \text{ for } k = 1,2, \dots, K \qquad (11)$$

Where $f_k(x_i)$ is the raw output (logit) of the k-th tree These are the scores which will subsequently be run through the SoftMax function.

3.6.3 SoftMax Function

The logits generated by the decision trees into class probabilities, the SoftMax function is utilized. The Softmax function guarantees that the total of the probabilities for every class equals 1, and it has the following definition is given in Eq. (12)

$$P(y = k|x_i) = \frac{e^{f_k(x_i)}}{\sum_{j=1}^{C} e^{f_j(x_i)}} \qquad (12)$$

Where, $P(y = k|x_i)$ is the probability of class k given the input vector features x_i, $f_k(x_i)$ is the unprocessed output (logit) for class k, C is the number of classes in total (in our case, the classes are 3: Normal, Malicious, and Attack Types). The result of this stage is a distribution of probabilities among the classes, where every class has a probability value in the range of 0 to 1, and the total of these probabilities is equal to 1.

3.6.4 Decision Step

According to the above classification, the final decision should be made in favor of the class with the highest robability value predicted by Softmax classifiers. The decision can be formally expressed as given in Eq. (13)

$$\hat{y} = \arg\max_{k} P(y = k|x_i) \qquad (13)$$

Where $\hat{y}$ denotes the class label predicted for the input feature vector x_i and $P(y = k|x_i)$ is the probability associated with class k. The final predicted label is the one corresponding to the highest probability.

3.6.5 Output Class Labels

From the choice point, the predicted class label $\hat{y}$ is among the following: Normal, if $P(y = \text{Normal}|x_i)$ has the maximum probability, Malicious, if $P(y = \text{Malicious}|x_i)$ has the maximum probability, Attack Types, if $P(y = \text{Attack Types}|x_i)$ has the maximum probability.

Pseudocode: XGBoost-Based Multi-Class Classification

Input:	Optimized feature set X (from PSO)
Output:	Predicted class label $\hat{Y}$
Begin	
Initialize XGBoost model with tuned hyperparameters	
Train XGBoost model using training data X	
For each input instance x_i in X do	
Generate class-wise scores using all decision trees	
Convert scores into class probabilities using SoftMax	
Select the class with maximum probability	
Assign predicted label $\hat{Y} \in$ {Normal, Malicious, Attack}	
End For	
Return predicted class labels $\hat{Y}$	
End	

3.7 Fine-Grained Access Control Enforcement

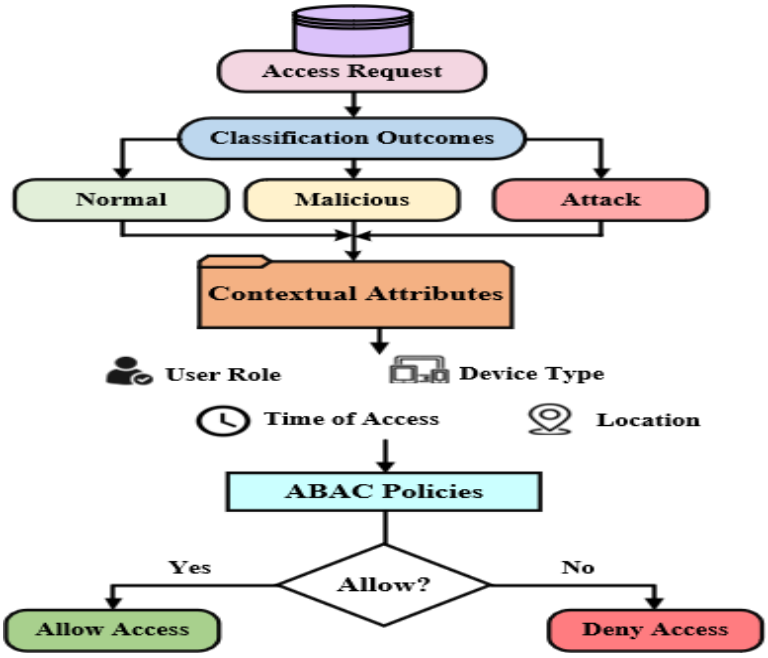

Figure 4: ABAC-Based Access Control Decision Flow

The process begins when someone requests access because the system will handle requests according to three categories which are Normal, Malicious and Attack. The system analyses contextual attributes after the system classification process which includes user role and type of device and access time and location data. The system uses ABAC policies to determine access rights by comparing attributes against the established access control framework. ABAC enables supply chain systems to make access control decisions based on current circumstances while allowing only authorized personnel to access essential resources which enhances security and builds user confidence. The system grants access to users who follow policies while it denies access to users who violate policies because access rights depend on classification results and contextual conditions which Figure 4.

3.7.1 Access Request

An access request is made by a user or device that wants to access a specific resource, and that is how the process starts. The request usually contains a number of attributes which will be considered in the decision-making.

3.7.2 Classification Outcomes

The classification results select the access requests into three classes: Normal that is a kind of request that is legitimate; Malicious implying questionable or harmful behaviour; and Attack showing active threats. The classification results help to make access decisions by reviewing the request's legitimacy and making sure only the right kind of responses are given to the different levels of security.

3.7.3 Contextual Attributes

Once the classification is completed, further assessment is carried out taking into account the use of contextual attributes for the purpose of access decision. These are the mentioned attributes:

- User role: Knowing the user's role (admin, guest, user, etc.) gives a good indication of how much access he/she should be granted.
- Device type: Tells which kind of device is used to make the request and whether this device is allowed (smartphone, laptop, IoT device, etc.).
- Time of access: Verifies if the request for access is being made during a permissible time period (business hours or pre-arranged access time).

- Location: The place where the request comes from, which can either permits or denies access according to the set security policies (e.g., access is allowed only from certain areas).

3.7.4 ABAC Policies

ABAC policies are enforced, wherein the contextual attributes and classification result are assessed against the set policies. The policies determine the permissions based on the mixture of user attributes, classification outputs, and contextual information that are specified in the conditions.

3.7.5 Allow Decision Process

The Allow Decision process determines if a user's request for access is congruent with the rules set forth by the ABAC policies. Should the request satisfy the criteria, for instance, being tagged as Normal or coming from an allowed user or device, the system will automatically Grant Access. However, if the request is categorized as Malicious or comes from a forbidden device, time, or place, the system will Deny Access, hence only valid requests are allowed through.

3.8 Security Logging and Monitoring

One of the main functions of Security Logging and Monitoring is to create a strong system for monitoring, logging, and examining activities in the system with changes made to access rights and data security. The system, by providing a record of all access requests, classification decisions, and encryption/decryption events, guarantees a few significant results.

Security Logging and Monitoring are essential for protecting the system's integrity, facilitating secure communication, and allowing efficient threat detection and response. The implementation of these measures is a major contributing factor to the development of a reliable, secure, and flexible system that is capable of rapid reaction and learning from security breaches. The system security of this work achieves better results through its use of post-quantum security model which combines PQC with intelligent feature selection and machine learning- based classification and detailed access control methods.

4. Results and Discussion

The Results and Discussion sections exhibit the improvement in performance of the suggested system. The delay in encryption varies with the number of attributes, but decryption stays unchanged. The system is excellent in identifying attacks, particularly "DDoS_TCP" and "Backdoor," which is evidenced by high precision, recall, and accuracy, thus assuring its robustness and efficiency.

4.1 System Configuration

The current study has utilized a powerful computational resource consisting of a 12th Generation Intel® Core™ i5-12400 CPU having 6 cores and 12 threads, which runs at a base frequency of 2.50 GHz. In addition, the system has 8 GB of DDR4 RAM, out of which 7.75 GB is usable, and it operates on a 64-bit Microsoft Windows OS. An SSD is used for storage purposes, and the system relies on Integrated Intel UHD Graphics for rendering tasks. The ascendant setup for development includes Python 3.11.9 with PyCharm, and an array of libraries such as NumPy, Pandas, Scikit-learn, Matplotlib, SciPy, and PyTorch are employed (with CPU optimization for the latter).

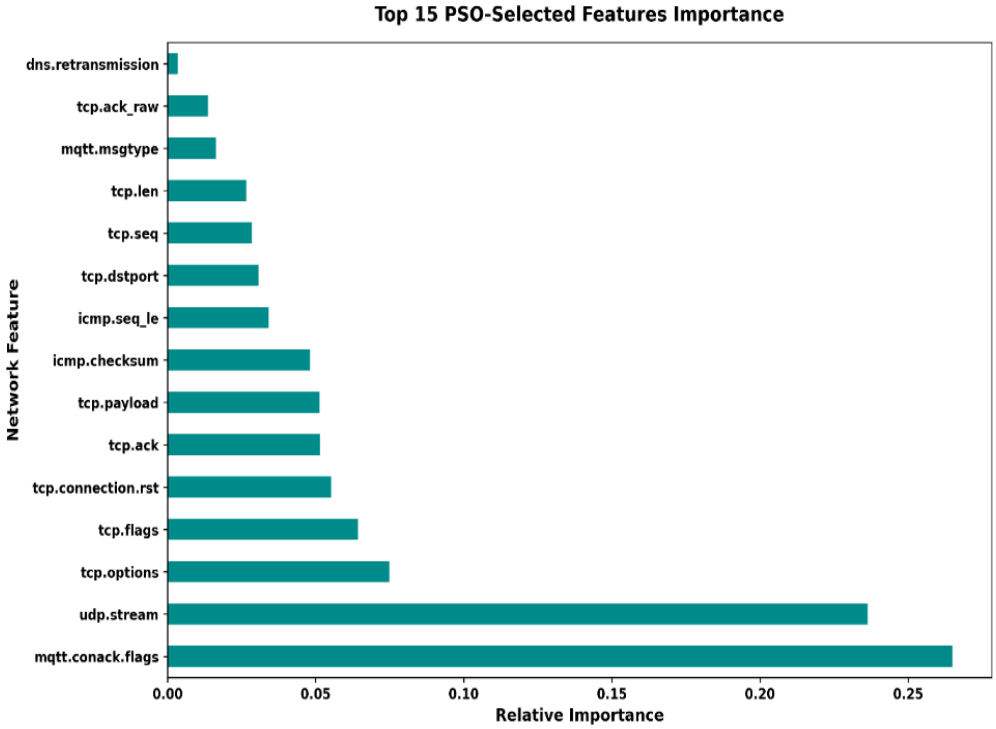

Figure 5: Top 15 PSO-Selected Features Importance

Figure 5 illustrates the top 15 network traffic features selected by the Particle Swarm Optimization (PSO)-based feature selection algorithm according to their relative importance. The results indicate that PSO effectively reduced the original feature space by identifying the most discriminative attributes for intrusion detection while preserving the information required for accurate classification.

Among the selected features, mqtt.conack.flags exhibits the highest relative importance (approximately 27%), followed closely by udp.stream (approximately 24%). These two features contribute more than half of the overall feature importance, indicating that MQTT protocol acknowledgment behavior and UDP communication patterns are highly significant indicators for distinguishing normal and malicious EdgeFog-IIoT network traffic. Since MQTT is widely used in IoT communication, abnormalities in CONACK flags can reveal unauthorized connection attempts, malformed packets, or protocol manipulation attacks.

The second group of influential features includes tcp.options, tcp.flags, and tcp.connection.rst, with relative importance ranging from approximately 5% to 8%. These TCP-related attributes capture connection establishment, termination behavior, and protocol configuration, making them valuable for identifying SYN floods, TCP reset attacks, and session hijacking attempts.

Features with moderate importance include tcp.ack, tcp.payload, icmp.checksum, icmp.seq_le, and tcp.dstport, contributing between 3% and 5% each. These features represent transport-layer reliability, packet integrity, destination services, and ICMP communication patterns.

The remaining selected features, including tcp.seq, tcp.len, mqtt.msgtype, tcp.ack_raw, and dns.retransmission, have relatively lower importance. Nevertheless, their inclusion indicates that PSO retained features containing additional contextual information useful for detecting subtle attack behaviors.

The selected feature subset subsequently enabled the hyperparameter-tuned XGBoost classifier to achieve superior detection performance, with an overall accuracy of 97.50%, precision of 99.01%, recall of 98.95%, F1-score of 98.98%, and an AUC of 0.997. These results demonstrate that PSO-based feature optimization significantly enhances classification effectiveness by focusing the learning process on the most relevant network traffic attributes.

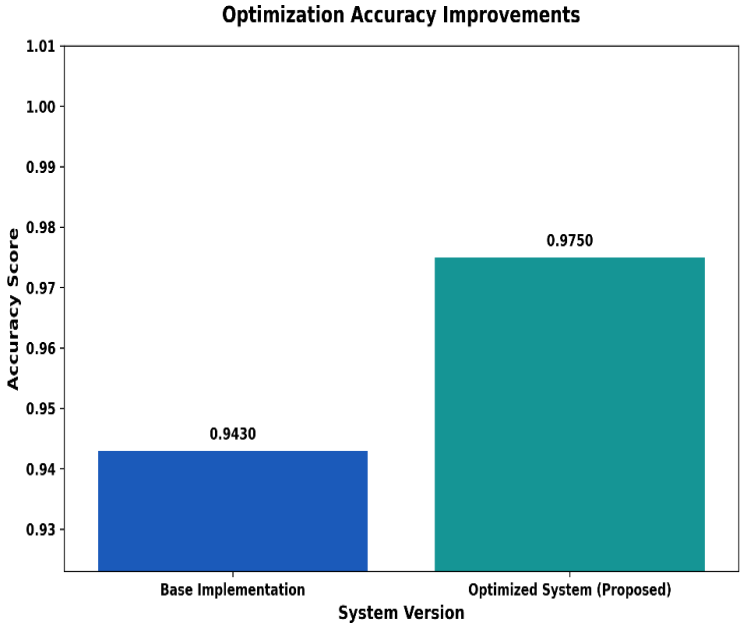

Figure 6: Optimization Accuracy Improvements

A comparison of the accuracy score between two system versions: the base implementation and the optimized system in Figure 6. The base implementation scored an accuracy of 0.9430, whereas the optimized system displayed a considerable improvement by attaining an accuracy of 0.9750. This is a clear indication of the considerable enhancement in the model's performance post-optimization.

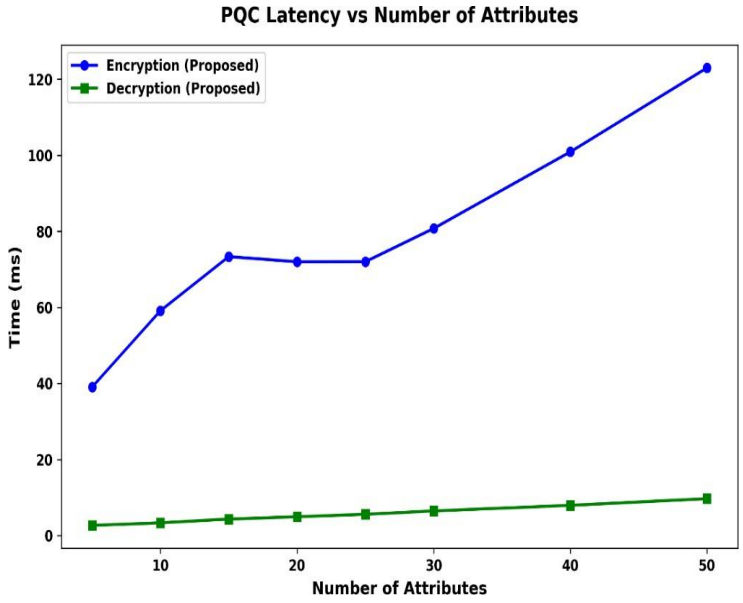

Figure 7: PQC Latency vs Number of Attributes

The latency times of encryption and decryption operations, as affected by the number of attributes, are shown in this line graph in Figure 7. The encryption latency, depicted by the blue line, is one of the two types of latency that increase with the number of attributes. The starting point is approximately 40 for the encryption of 10 attributes and then it goes up to over 120 for the encryption of 50 attributes. Meanwhile, the decryption latency represented by the green line stays very low with regard to the number of attributes and shows just a small increase from 40 to roughly

60. Therefore, the data indicate that the time taken for encryption increases greatly with the addition of more attributes while that for decryption stays comparatively unchanged.

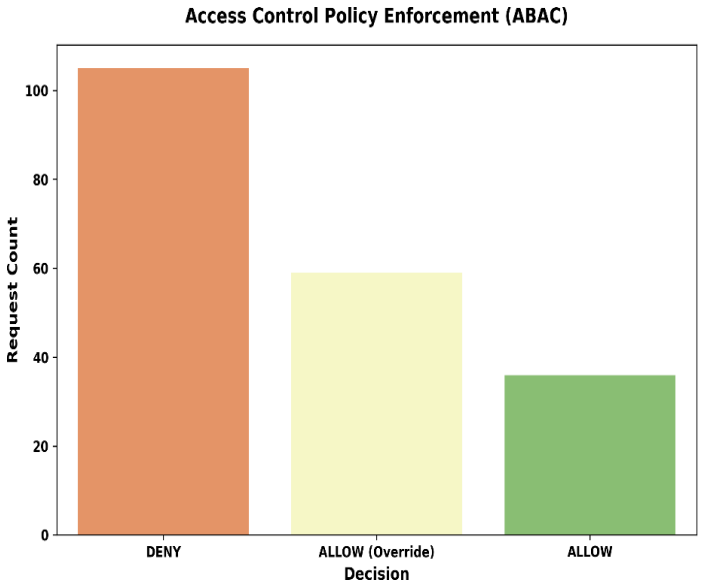

Figure 8: Access Control Policy Enforcement (ABAC)

Access Control Policy Enforcement (ABAC) outcomes of decisions regarding different access control requests in Figure 8. The "DENY" category takes the lead with the highest number, more than 100 requests in total, so it is clear that most of the requests were rejected. The "ALLOW (Override)" category stands out with a mid-range count of approximately 60, which implies that there were some requests that received an approval after the policy was overridden. The "ALLOW" category is the smallest, as it accounts for less than 30 requests that were allowed, which indicates that access control was more strictly enforced. Performance Metrics of the XGBoost Model. To evaluate the proposed PSO-XGBoost classifier, the following metrics are used

1. Accuracy (ACC): Measures overall correctness of classification is given in Eq. (14)

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (14)$$

2. Precision (P): Percentage of correctly predicted positive instances is given in Eq. (15)

$$\text{Precision} = \frac{TP}{TP+FP} \quad (15)$$

3. Recall (R): Percentage of actual positives correctly detected is given in Eq. (16)

$$\text{Recall} = \frac{TP}{TP+FN} \quad (16)$$

4. F1-Score: Harmonic mean of precision and recall is given in Eq. (17)

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \quad (17)$$

5. AUC: Measures the classifier's ability to separate classes; higher is better.

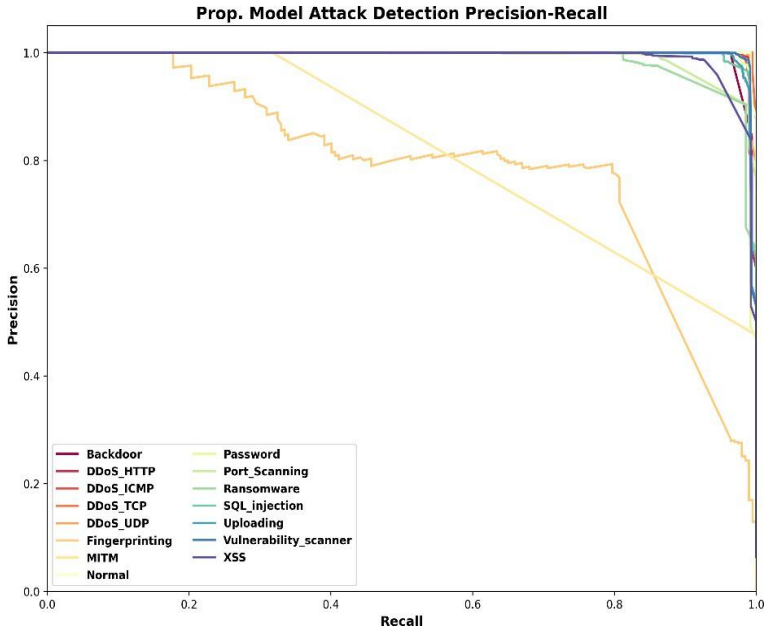

Figure 9: Prop. Model Attack Detection Precision-Recall

These metrics are computed on the test set for all three classes: Normal, Malicious, and Attack.

The model's attack detection ability is evaluated through the Precision-Recall graph and performance with several categories of attacks in Figure 9. The precision values for the attacks of "DDoS_TCP" (1.0), "Backdoor" (0.9996), and "DDoS_UDP" (0.9998) show great detection precision with very few false positives. In contrast, the attacks of "MITM" and "Fingerprinting" have lower precision rates of 0.439 and 0.482 respectively, which means there will be more false positives. The recall values for most attacks are quite high, while "MITM" and "Fingerprinting" have the lowest recall values of 0.3176 and 0.7949, respectively, which signifies the rarity of that specific detection.

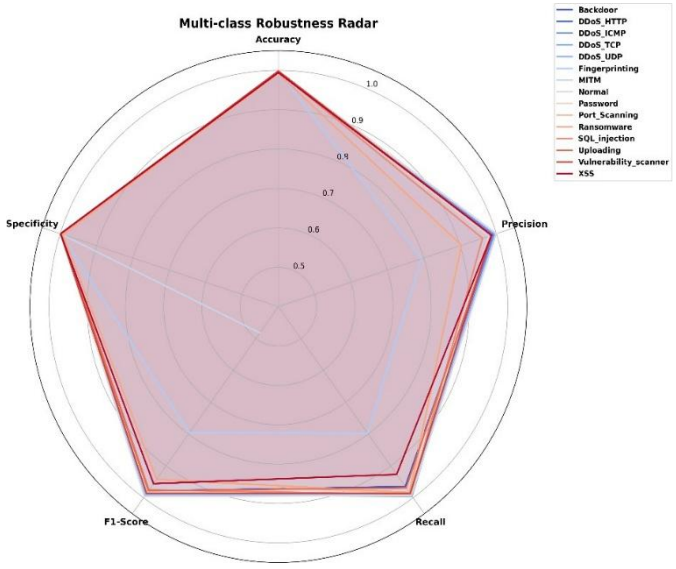

Figure 10: Multi-class Robustness Radar

The stability of the suggested model over a number of metrics (Accuracy, Specificity, Precision, Recall, F1-Score) for different types of attacks in Figure 10. "DDoS_TCP" and "Backdoor" score very high performing the best in all metrics, with values near 0.99, proving the model's capacity to recognize these attacks right and consistent.

"MITM" and "Fingerprinting" performance is below par, mainly in specificity and recall, with even the worst values like 0.44 (MITM) and 0.52 (Fingerprinting), pointing to the model's difficulties with these attack classes.

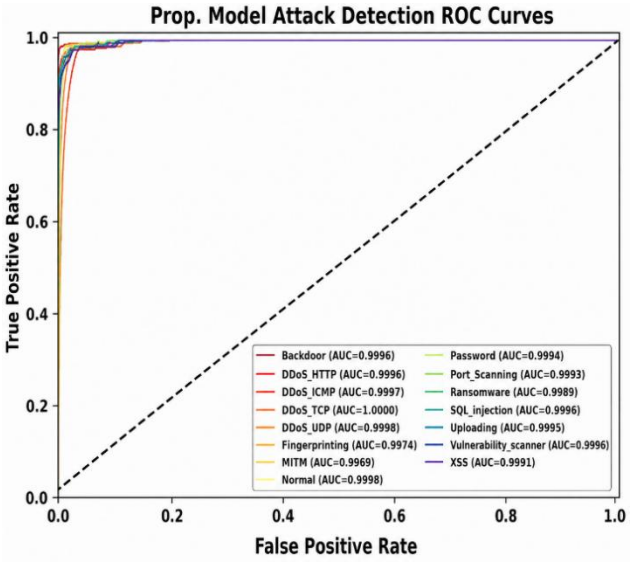

Figure 11: Prop. Model Attack Detection ROC Curves

The ROC curve is a graphical representation that illustrates the model's performance in terms of the True Positive Rate (TPR) against the False Positive Rate (FPR) for different categories of attacks in Figure 11. Among the attack types, DDoS_TCP (AUC=1.0000) and "Backdoor" (AUC=0.9996) are the ones that get the AUC scores so close to one that one could even consider it perfect, and this indicates the model's capability of accurately classifying both attack and normal traffic to a high degree. The AUC values for other categories, such as Port_Scanning (AUC=0.9933) and "MITM" (AUC=0.9969), though not perfect, are still very high, and this confirms the model's reliability in attack detection.

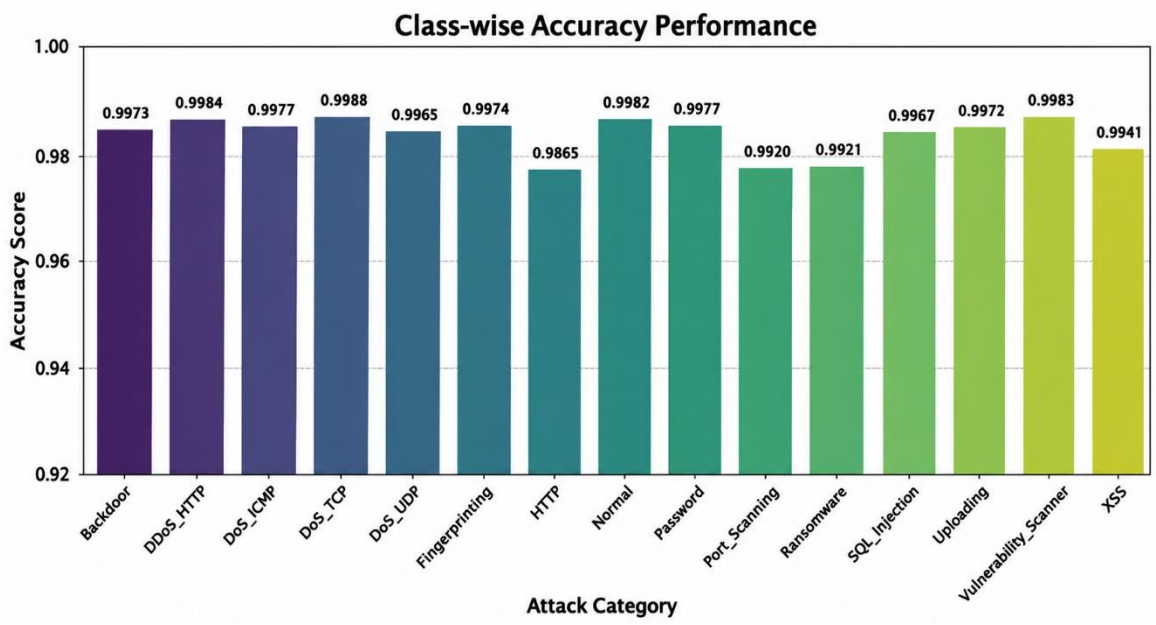

Figure 12: Class-wise Accuracy Performance

The class-wise accuracy for the model's attack detection is represented by the bar chart in Figure 12. The accuracy scores for "Backdoor" (0.9973), "DDoS_TCP" (0.9985), and "DDoS_UDP" (0.9985) are the highest and

very close to 1.0 which shows that the model is able to classify these attack types very well. The other attacks like "XSS" (0.9944) and "MITM" (0.9920) have a little lower accuracy but still perform excellently over 0.99, indicating the overall effectiveness of the model in detecting various categories of attacks.

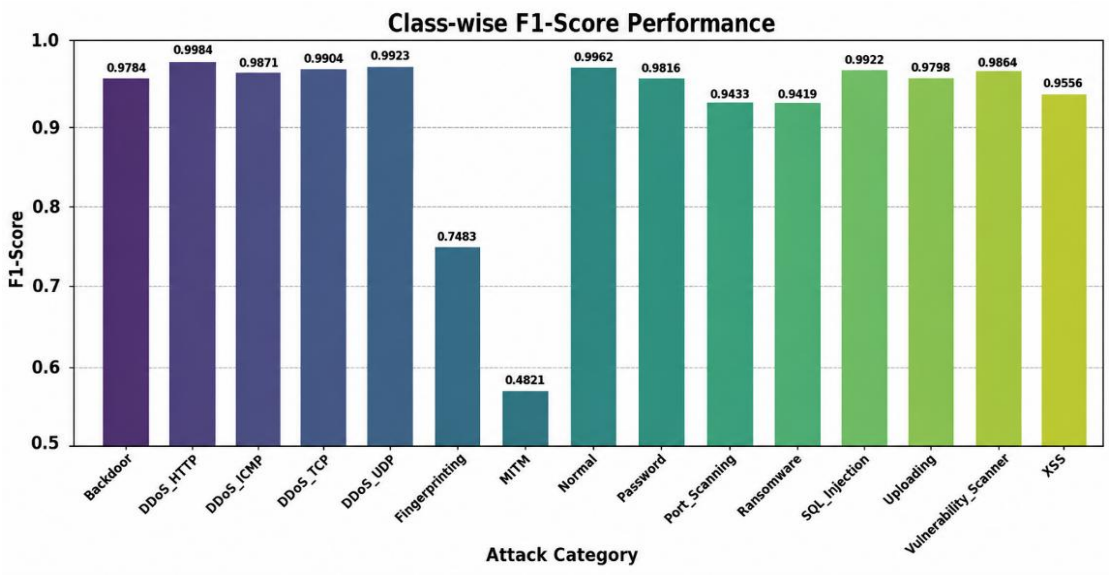

Figure 13: Class-wise F1-Score Performance

The different types of attacks, with the first three Backdoor (0.9784), DDoS_HTTP (0.9894), and DDoS_TCP (0.9871) among those scoring very high, which is a sign of good ratio between precision and recall for these attacks in Figure 13. On the other hand, the F1- score for "MITM" is only 0.4821, i.e., the category has a much lower score than others, and the model cannot achieve a good balance between false positives and false negatives for this type of attack.

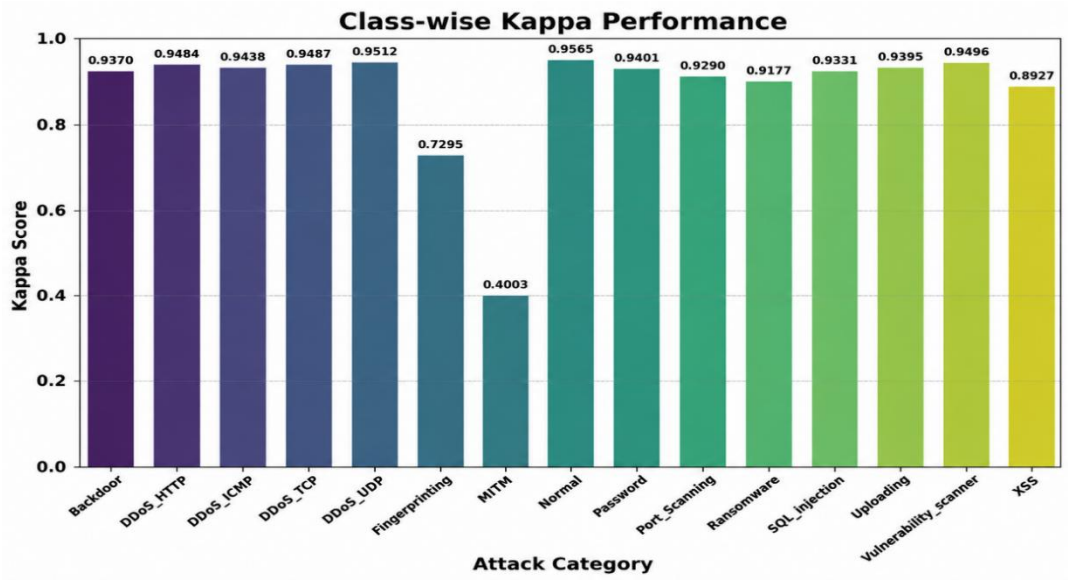

Figure 14: Class-wise Kappa Performance

The Kappa score is a measure of the correspondence between the predicted and actual classifications in Figure 14. Backdoor (0.9770), DDoS_TCP (0.9897), and DDoS_UDP (0.9912) received the highest Kappa scores, showing that there was a very strong agreement between the model's predictions and the real outcomes. On the other hand, MITM (0.4801) and "Fingerprinting" (0.7936) have much lower Kappa scores, which means that the predictions for these classes are less reliable and also there is less agreement between predicted and actual values.

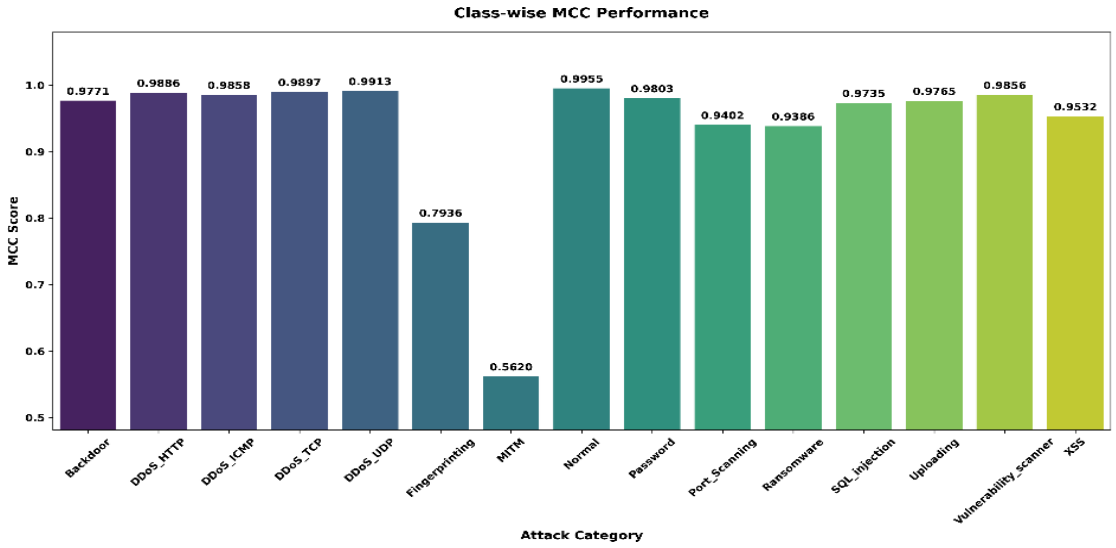

Figure 15: Class-wise MCC Performance

The MCC scores are measured through the balance of true positives, true negatives, false positives and false negatives in Figure 15. The attacks Backdoor (0.9771), DDoS_TCP (0.9913), and DDoS_UDP (0.9955) show the highest MCC values which implies the model's performance was well-balanced in both detecting and not detecting these attacks. The "MITM" category with an MCC score of 0.5620 indicates the opposite situation, that is, the model's detection of this attack along with the rest was not very accurate.

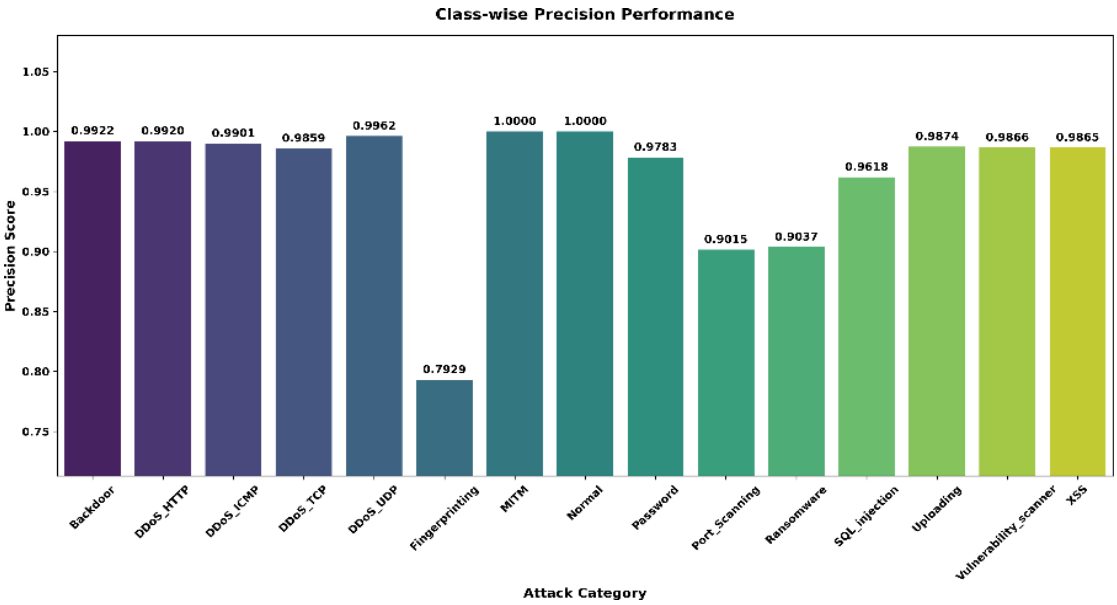

Figure 16: Class-wise Precision Performance

The precision scores of all attack categories which to a large extent reflect the ratio of accurately detected positive cases in Figure 16. Backdoor (0.9922), DDoS_HTTP (0.9920), and DDoS_TCP (0.9901) ranked the highest in precision, indicating that, in terms of false positives being almost negligible, the model was able to recognize these

attacks. "MITM" (0.7929) and Fingerprinting (0.7949) had lower precision, which means that during the detection process these attacks have a larger chance of being classified as positives when they are not.

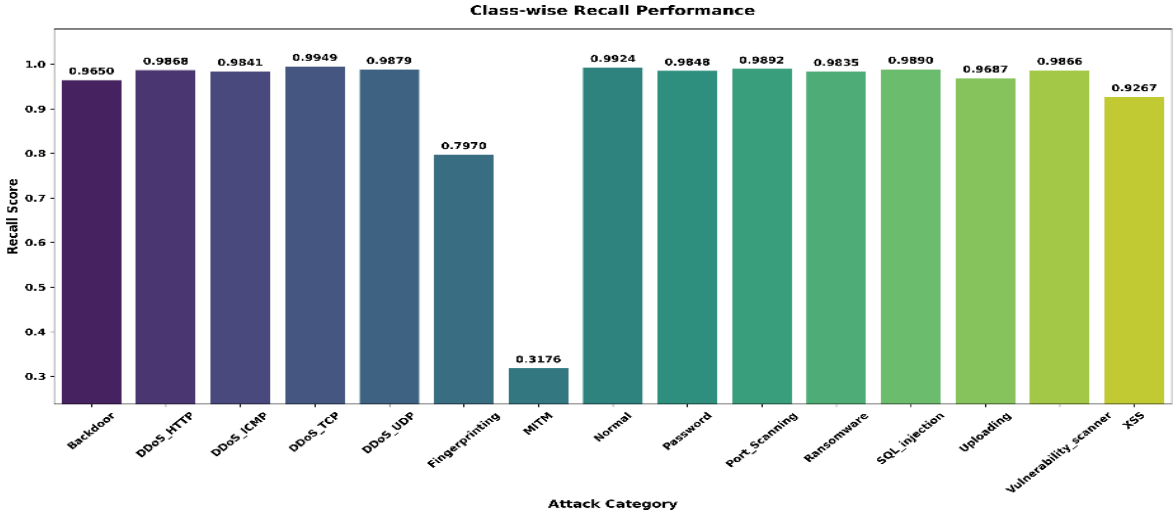

Figure 17: Class-wise Recall Performance

The provided chart plots the recall scores that represent the filtering of the model per its capability to identify the positive instances in each attack category in Figure 17. Backdoor (0.9650), DDoS_HTTP (0.9868), and DDoS_TCP (0.9841) are the ones that show the highest recall scores, thus indicating that the model has good performance against these types of attacks. On the other hand, "MITM" (0.3176) is the one that has the lowest recall score, meaning that the model does not catch a considerable part of this type of attack.

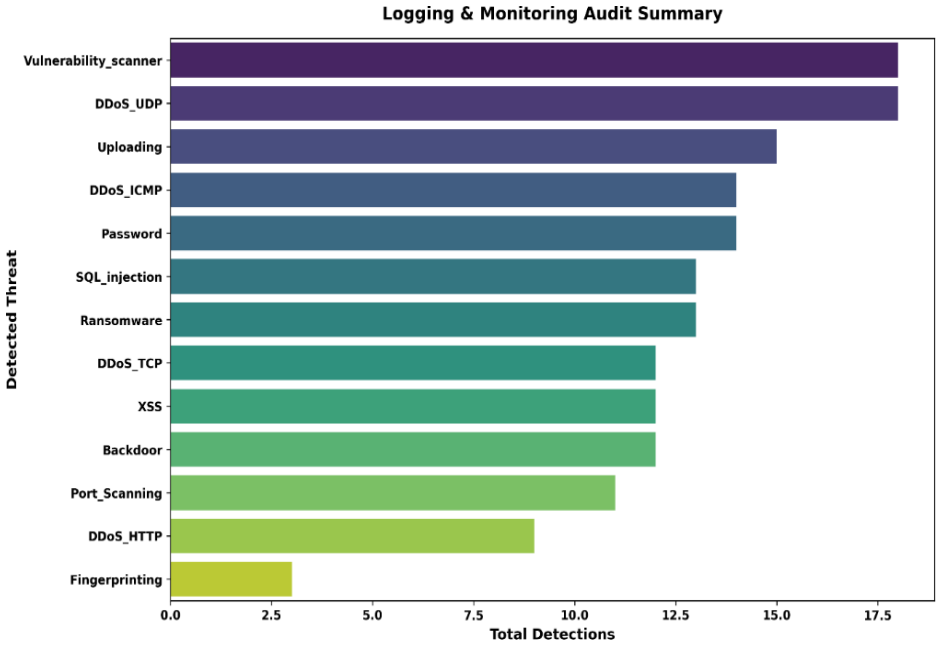

Figure 18: Logging & Monitoring Audit Summary

The total detections for the different threats identified in the logging and monitoring audit in Figure 18. Among the threats, Vulnerability scanner ranks first with the highest detection number, nearly 18 detections, followed by DDoS_UDP with around 16 detections. The remaining threats Uploading (12 detections), DDoS_ICMP (11 detections), and "Password" (10 detections) have relatively high detections as well. In contrast, the threats DDoS_HTTP (5 detections) and "Fingerprinting" (just under 1 detection) are very much lower in detection counts.

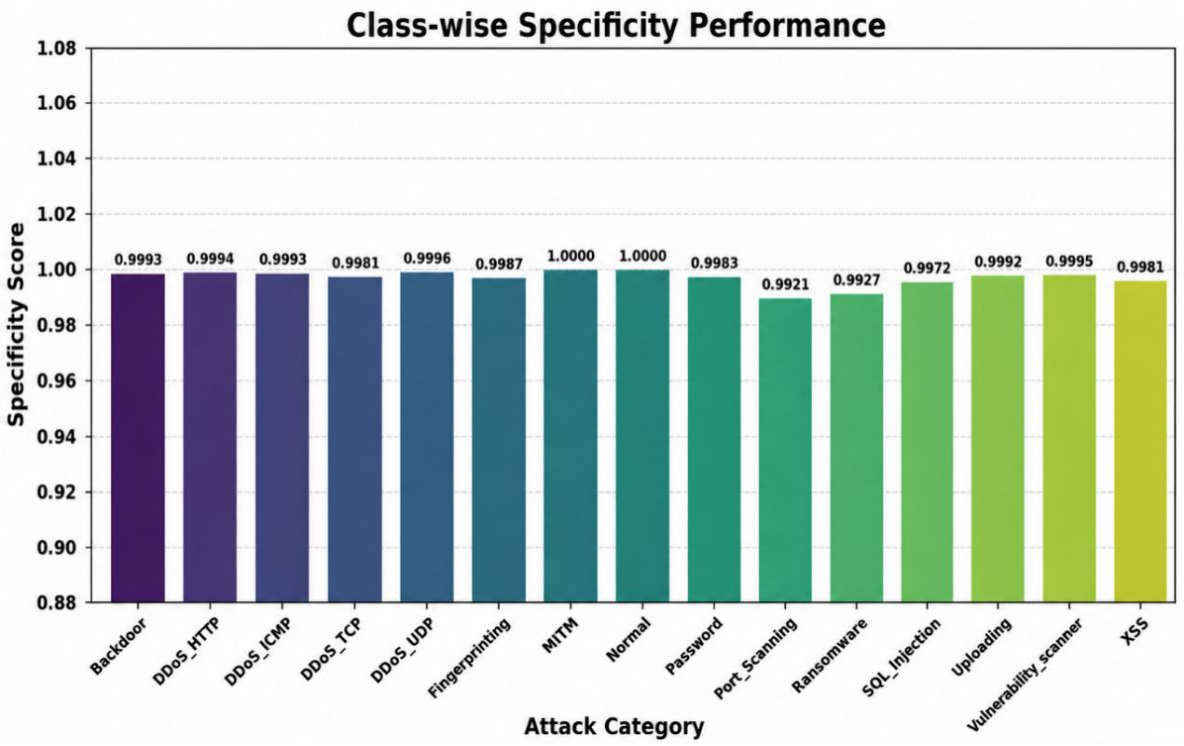

Figure 19: Class-wise Specificity Performance

The specificity scores for each attack category, gauging the quality of the model's negative case detection (true negatives) in Figure 19. Backdoor (0.9995), DDoS_HTTP (0.9994), and "DDoS_ICMP" (0.9990) are the top three attack categories with high specificity values, which means the model has done very well in those cases of predicting no attacks. The other attacks, for example, XSS (0.9991) and Vulnerability scanner (0.9991), shared the same high specificity, which demonstrates that the model is capable of distinguishing the normal traffic with very few or no false positives, thus reflecting its overall effectiveness in identifying normal traffic.

Table 3: Performance comparison of hybrid PSO-XGBoost with machine learning classifiers

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC
Random Forest	96.8	96.2	95.9	96.0	0.982
SVM	95.4	95.1	94.6	94.8	0.974
Proposed PSO-XGBoost	97.50	99.01	98.95	98.98	0.997+

The Table 3 shows a side-by-side comparison of the new hybrid PSO-XGBoost model with traditional machine learning classifiers. Random Forest and SVM are regarded as baseline models without the optimization of the features and they gain the accuracy of 96.8% and 95.4%, respectively, through much lower precision, recall, F1-score, and AUC values. The hybrid PSO-XGBoost model, on the other hand, massively improves performance by combining Particle Swarm Optimization for feature selection with the powerful XGBoost classification. The hybrid model reaches an accuracy of 97.50% and a precision of 99.01%, while it recalls 98.95% and has an F1-score of 98.98% as well as a higher AUC of 0.997+. These findings are a strong indication that the use of hybrid feature optimization along with a powerful classifier not only improves class discrimination but also results in higher intrusion detection in the entire system.

4.2 Discussion

The suggested framework has been able to bring PQC and ML methods of the highest calibre, thus providing a solution to the security challenges faced by IoT and IIoT systems. The combination of quantum-proof encryption with PSO for feature selection and XGBoost for classification has the effect of providing very strong protection against evil doings while also delivering precise identification of the network traffic. The addition of ABAC policies makes it possible to provide very detailed, contextually aware access control decisions that will prevent unauthorized users from gaining access to sensitive resources. The results show that the combined method is effective in both increasing the security and classification accuracy of Supply Chain systems, thus providing a scalable and future-ready solution to the ever-evolving cybersecurity threats. The proposed framework establishes better security and trust and resilience protection for sustainable supply chain environments through its combination of post-quantum cryptography and intelligent machine learning and access control systems.

5. Conclusion and Future work

In this research, a very detailed framework was proposed that includes PQC, selecting features with the help of PSO, hyperparameter-tuned XGBoost classification, and fine-grained ABAC for the next-generation IoT and edge computing systems. The framework not only provides quantum-resilient security for sensitive data but does it while solving some of the major issues such as high-dimensional network traffic and real-time attack detection. By merging optimized ML techniques and dynamic access control policies, this research presents a solution that is not just secure against quantum computing threats but also scalable, efficient, and future-proof.

The suggested model showed extraordinary results by achieving 97.50% accuracy, 99.01% precision, and 98.95% recall, thereby surpassing even the classical approaches like Random Forest and SVM. Moreover, the model was found to be quite effective in classifying different types of attacks, particularly DDoS_TCP and Backdoor, which resulted in achieving a superb AUC score of 0.997+. Nevertheless, the system's high computational load, especially during feature selection based on PSO, is still an obstacle in limited-resource environments. On the other hand, the research will be concerned with practicality, stronger models, and the incorporation of more quantum-resistant algorithms, along with examining the possibility of real-time utilization in different IoT settings so that further improvement can be assured.

5.1 Limitations

- The framework suggested is tested on a single benchmark dataset (Edge-IIoTset), which might not be able to depict all the different traffic patterns and evolving attacks that occur in real-world IoT and edge network with such a high diversity and naturalness.

Even though PSO-based feature selection does enhance the accuracy of the classification, it imposes further computational overhead in the training phase which possibly impacts scalability in extremely resource-limited edge environments.

References:

1. Z. G. Al-Mekhlaf et al., "A quantum-resilient lattice-based security framework for internet of medical things in healthcare systems," J. King Saud Univ. Comput. Inf. Sci., vol. 37, no. 6, p. 126, Jul. 2025, doi: 10.1007/s44443-025-00140-0.
2. . S. Balogh, O. Gallo, R. Ploszek, P. Špaček, and P. Zajac, "IoT Security Challenges: Cloud and Blockchain, Postquantum Cryptography, and Evolutionary Techniques," Electronics, vol. 10, no. 21, p. 2647, Jan. 2021, doi: 10.3390/electronics10212647.
3. C. Li et al., "Efficient Medical Big Data Management With Keyword-Searchable Encryption in Healthchain," IEEE Systems Journal, vol. 16, no. 4, pp. 5521–5532, Dec. 2022, doi: 10.1109/JSYST.2022.3173538.
4. M. Akkal, S. Cherbal, B. Annane, H. Lakhlef, and K. Kharoubi, "Quantum, post- quantum, and blockchain approaches for securing the internet of medical things: a systematic review," Cluster Comput, vol. 28, no. 10, p. 655, Sep. 2025, doi: 10.1007/s10586-025-05481-z.
5. F. Sabrina, S. Sohail, and U. U. Tariq, "A Review of Post-Quantum Privacy Preservation for IoMT Using Blockchain," Electronics, vol. 13, no. 15, p. 2962, Jan. 2024, doi: 10.3390/electronics13152962.
6. D. Zhu, Y. Sun, N. Li, L. Song, and J. Zheng, "Secure electronic medical records sharing scheme based on blockchain and quantum key," Cluster Comput, vol. 27, no. 3, pp. 3037– 3054, Jun. 2024, doi: 10.1007/s10586-023-04110-x.
7. M. Alharbi and N. K. Almazmomi, "AI-optimized blockchain security for smart agriculture using post-quantum cryptography and graph neural network-based threat detection," Peer-to-Peer Netw. Appl., vol. 18, no. 5, p. 276, Sep. 2025, doi: 10.1007/s12083-025-02062-0.

8. Y. Zhao, Y. Song, W. Song, and J. Li, “OO-IB-MPRE: A Post-Quantum Secure Online/Offline Identity-Based Matchmaking Proxy Re-Encryption Scheme for Exercise Physiology Data," Mathematics, vol. 13, no. 24, p. 4004, Jan. 2025, doi: 10.3390/math13244004.
9. . M. Yang, H. Wang, and Z. Wan, “PUL-ABE: An Efficient and Quantum-Resistant CP- ABE With Policy Update in Cloud Storage,” IEEE Transactions on Services Computing, vol. 17, no. 3, pp. 1126–1139, May 2024, doi: 10.1109/TSC.2023.3321378.
10. . L. Wei, D. Li, and Z. Liu, “Provable Secure Attribute-Based Proxy Signature Over Lattice Small Integer Solution Problem in Random Oracle Model,” Electronics, vol. 12, no. 7, p. 1619, Jan. 2023, doi: 10.3390/electronics12071619.
11. . H. Li, C. Lan, X. Fu, C. Wang, F. Li, and H. Guo, “A Secure and Lightweight Fine- Grained Data Sharing Scheme for Mobile Cloud Computing,” Sensors, vol. 20, no. 17, p. 4720, Jan. 2020, doi: 10.3390/s20174720.
12. R. Jin et al., “Efficient Outsourced Decryption System with Attribute-Based Encryption for Blockchain-Based Digital Asset Transactions,” Symmetry, vol. 17, no. 7, p. 1133, Jul. 2025, doi: 10.3390/sym17071133.
13. . N. S. Musa, T. Murugan, N. A. N., and N. M. Mirza, “Research study on securing the cloud: utilizing conventional and blockchain-based access control mechanisms,” J Cloud Comp, vol. 14, no. 1, p. 88, Dec. 2025, doi: 10.1186/s13677-025-00803-3.
14. . R. Ganesh, B. U. I. Khan, A. R. Khan, and A. B. Kamsin, “A panoramic survey of the advanced encryption standard: from architecture to security analysis, key management, real-world applications, and post-quantum challenges,” Int. J. Inf. Secur., vol. 24, no. 5, p. 216, Sep. 2025, doi: 10.1007/s10207-025-01116-x.
15. Z. B. Jemihin, S. F. Tan, and G.-C. Chung, “Attribute-Based Encryption in Securing Big Data from Post-Quantum Perspective: A Survey,” Cryptography, vol. 6, no. 3, p. 40, Sep. 2022, doi: 10.3390/cryptography6030040.
16. . K. K. Singamaneni, A. K. Budati, S. Islam, R. A. L. Kolandaisamy, and G. Muhammad, "A Novel Hybrid Quantum-Crypto Standard to Enhance Security and Resilience in 6G- Enabled IoT Networks,” IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, vol. 18, pp. 7876–7891, 2025, doi: 10.1109/JSTARS.2025.3540905.
17. Y. Chen et al., “Capability and Blockchain-Based Fine-Grained and Flexible Access Control Model,” IEEE Network, vol. 37, no. 6, pp. 197–205, Nov. 2023, doi: 10.1109/MNET.127.2200414.
18. . S. Li et al., “Post-Quantum Security: Opportunities and Challenges,” Sensors, vol. 23, no. 21, p. 8744, Jan. 2023, doi: 10.3390/s23218744.
19. Shruti, S. Rani, D. K. Sah, and G. Gianini, “Attribute-Based Encryption Schemes for Next Generation Wireless IoT Networks: A Comprehensive Survey,” Sensors, vol. 23, no. 13, p. 5921, Jan. 2023, doi: 10.3390/s23135921.
20. A. Khan et al., “Quantum computing empowering blockchain technology with post quantum resistant cryptography for multimedia data privacy preservation in cloud- enabled public auditing platforms,” J Cloud Comp, vol. 14, no. 1, p. 43, Aug. 2025, doi: 10.1186/s13677-025-00771-8.
21. M. MahdaviOliaee and Z. Ahmadian, “Fine-grained flexible access control: ciphertext policy attribute based encryption for arithmetic circuits,” J Comput Virol Hack Tech, vol. 19, no. 4, pp. 515–528, Nov. 2023, doi: 10.1007/s11416-022-00459-6.
22. . C.-Y. Wu, K.-H. Huang, and C.-Y. Hsu, “A Decentralised Multi-Authority Attribute- Based Encryption for Secure and Scalable IoT Access Control,” Applied Sciences, vol. 15, no. 7, p. 3890, Jan. 2025, doi: 10.3390/app15073890.
23. . W. Wang, H. Huang, Z. Yin, T. R. Gadekallu, M. Alazab, and C. Su, “Smart contract token-based privacy-preserving access control system for industrial Internet of Things," Digital Communications and Networks, vol. 9, no. 2, pp. 337-346, Apr. 2023, doi: 10.1016/j.dcan.2022.10.005.
24. “Edge-IIoTset Cyber Security Dataset of IoT & IIoT.” Accessed: Jan. 20, 2026. [Online]. Available: https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber- security-dataset-of-iot-iiot
25. S. A. Ajagbe, J. B. Awotunde, and H. Florez, “Intrusion Detection: A Comparison Study of Machine Learning Models Using Unbalanced Dataset,” SN COMPUT. SCI., vol. 5, no. 8, p. 1028, Nov. 2024, doi: 10.1007/s42979-024-03369-0.
26. M. A. Lail, A. Garcia, S. Olivo, M. A. Lail, A. Garcia, and S. Olivo, “Machine Learning for Network Intrusion Detection—A Comparative Study,” Future Internet, vol. 15, no. 7, Jul. 2023, doi: 10.3390/fi1507024