Q-FuzzyNet: A Quantum Inspired QIF-RNN and SA-FPA Optimizer for Intrusion Detection and Mitigation in Intelligent Connected Vehicles

Abdullah Alenizi
Department of Information Technology-College of Computer and Information Sciences,
Majmaah University, Al-Majmaah 11952, Saudi Arabia

***Abstract*—In the evolving landscape of Intelligent Connected Vehicles (ICVs), ensuring cybersecurity is crucial due to the increasing number of cyber threats. Besides, challenges like data breaches, unauthorized access, and hacking attempts are prevalent due to the interconnected nature of ICVs. Several methods have been proposed to secure ICVs; however, accurate intrusion detection remains a challenging task yet to be fully achieved. For this reason, this paper proposes a comprehensive intrusion detection scheme denoted a Q-FuzzyNet, which is specifically tailored to safeguard ICV networks using Deep Learning (DL) approaches. This Q-FuzzyNet approach consists of five phases: (i) Data Collection (ii) Data Pre-processing (iii) Feature extraction (iv) Dimensionality Reduction and (v) Intrusion Detection and Mitigation. Initially, the raw data are gathered from the CICIoV2024 dataset. The collected data are pre-processed via Mean Imputation (MI) for data cleaning. Then, significant features are extracted through higher-order statistical features, Proposed Improved Mutual Information (IMI), Correlation, and Entropy approaches. Subsequently, the dimensionality is reduced via new Improved Linear Discriminant Analysis (ILDA). Ultimately, the data are classified (attacker/Normal) via the Meta-Heuristic Quantum-Inspired Fuzzy-Recursive Neural Network (QIF-RNN) model by combining the Quantum Neural Network (QNN), Recurrent Neural Network (RNN), and Fuzzy logic. The membership function of fuzzy logic is optimized via the new Self Adaptive-Flower Pollination Algorithm (SA-FPA). The identified attackers are mitigated from the network using the Policy Gradient Method. The acquired outcomes from Q-FuzzyNet are validated in terms of Accuracy, Precision, Sensitivity, and F1-score, as well. The highest accuracy of 98.6% has been recorded by the proposed model.**

Keywords*—Cybersecurity; intelligent connected vehicles; artificial intelligence; quantum neural network; recurrent neural network; flower pollination algorithm

I. INTRODUCTION

The automotive industry has greatly changed since the gasoline-fueled automobile was first created in the late 19th century [1]. At first, the trade was more interested in straightforward advancements in machines and mass production strategies illustrated by Henry Ford's assembly line [2]. Over time, improvements in safety, fuel economy and design transformed it into better, dependable vehicles. The incorporation of electrification, automation and connectivity into the industry has provided the era of ICVs over the past few years [3]. This change is not just altering how people drive but is also giving rise to new concepts in transportation and mobility [4].

ICVs are developing fast with the help of automation and connectivity, but these are cybersecurity threats as well [5]. ICVs are susceptible to different types of cyber-attacks such as in-vehicle attacks where hackers intrude into the vehicle's systems like the CAN bus to gain control of sensitive operations like brakes and doors [6]. V2X communication systems which are very vital for vehicle safety and efficiency are vulnerable to attacks such as replay, Sybil, and DoS which can compromise the exchange of important information between vehicles and other structures [7]. Besides, viruses and scams are capable of corrupting vehicle software, thus eradicating core functions and granting unauthorized access to information. Another issue is data privacy, which is an issue since people in ICVs are constantly sharing information with each other and personal information such as location data could easily be leaked in the process [8] [9]. Moreover, other parts of a vehicle, like TPMS and smart keys, which are sensor-based, are also vulnerable to the attack, which can result in vehicle tracking or unauthorized access. However, due to the constant development of ICVs, new risks arise and therefore, the need for strong and dynamic security measures [10].

Intelligent connected vehicles (ICVs) rely on advanced technologies that could be at risk of cyber threats, making cybersecurity critical [11]. Critical vehicle systems could be hacked to produce unsafe conditions in the car which would cause accidents if there were no strong cybersecurity measures to protect them. Moreover, strong cybersecurity measures also protect individual privacy by safeguarding their data against breaches and help to build public confidence in ICVs [12] [13]. This is of utmost importance if we are to have large-scale adoption of these driving machines. In addition, cyber security prevents big money loss and protects national interests by securing important transport facilities. Thus, for ICVs to be deployed safely and successfully, cyber safety has to be considered important [13].

Intrusion detection in intelligent connected vehicles involves signature-based, anomaly-based, behaviour-based, hybrid, Machine Learning (ML)-based, network-based, and hardware-based systems. All of these have several merits but also some remarkable demerits. Signature-based IDS works quite effectively against known threats, which mostly suffer

from novel ones and require a frequent signature update [14]. The problems in anomaly-based IDS are high false positives and adaptation. Behavioural-based IDSs are complex, and are not scale; hybrid systems are balanced yet resource-intensive, and hard to integrate. In ML-based IDSs, volumes of data are needed, and it is susceptible to model drift. In general, network-based IDS suffers from difficulties related to encrypted traffic and impacts on performance. Hardware-based IDSs are expensive and challenging to integrate [15]. Traditional Intrusion Detection Systems (IDS) suffer from to evolving attack patterns, limitations in terms of real-time detection, scalability, and ease of adaptation. Most proposed models suffer from excessive false positives, computational intensiveness, and poor feature selection that further degrades performance in dynamic ICV environments. There is a need for efficient intrusion mitigation mechanisms, which are often lacking in such approaches. Most of the existing traditional systems primarily concentrate on detection alone without having many opportunities to respond or mitigate attacks in real-time. Moreover, most of the mitigation techniques are dependent upon the static rule-based approach, which proves to be ineffectual enough for adaptive and evolving threats in the connected vehicle networks. To cope with these challenges, this paper has introduced Q-FuzzyNet, a comprehensive deep learning-based framework specifically designed for intrusion detection and mitigation in ICV networks. The novelty proposal within Q-FuzzyNet comes from the novel integration of Quantum-Inspired Neural Networks (QNN), Fuzzy Logic, and the Self Adaptive-Flower Pollination Algorithm (SA-FPA) in order to optimize membership functions with improved boosting of detection accuracy.

This paper introduced a novel IDS to tackle the previous challenge by attaining enhanced accuracy. The key contributions are:

- To propose a specialized IDS referred to as Q-FuzzyNet tailored for ICVs to enhance network cybersecurity.
- To introduce higher-order statistical features, IMI, correlation, and entropy for significant feature extraction from the CICIoV2024 dataset.
- To use ILDA to reduce data dimensionality while retaining essential information.
- To combine QNN, RNN, and fuzzy logic into a novel QIF-RNN, for efficient.
- To optimize the fuzzy logic membership functions using the SA-FPA to enhance classification performance.
- To utilize the Policy Gradient Method to mitigate the attacker from the ICV network.

This article is structured as a recent literature on IDS in Section II. Section III explains the proposed architecture. Experimentation and results are given in Section IV. Discussion is given in Section V and finally, Section VI concludes the paper.

II. Literature Study

A. Recent Research

In 2022, Cheng et al. [16] presented a new model for detecting automotive intrusion based on the STC features of the in-vehicle communication traffic. This model was based on encoding-detection architecture, in which spatial and temporal relations were encoded at the same time. The model employed the spatial and channel features through an attention-based convolutional network and the temporal features through an attention short-term memory network.

In 2021, Alladi et al. [17] have put forward an AI-driven intrusion detection model for IoV. This architecture also entailed DL Engines (DLEs) that were aimed at detecting and categorizing vehicular traffic into possible cyber threats. To support the dynamism of vehicles and the time-sensitive nature of IoV networks, these DLEs were hosted on MEC servers rather than cloud computing.

In 2022, Yu et al. [18] proposed a federated LSTM neural network-based intrusion detection approach to IVNs in ICVs. This method involved the development of an LSTM neural network model to determine the periodicity of the ID sequence of IVN messages for the prediction of the incoming message IDs. A Network IDS (NIDS) based on ID prediction was then proposed.

In 2021, Pascale et al. [19] developed an IDS that was integrated into the automotive industry, which employed a two-step algorithm to identify potential cyber threats. In the first step, the system first screened the messages in the Controller Area Network (CAN-Bus) using spatial and temporal analysis. When messages were detected as potentially malicious, a Bayesian network was then used to calculate the likelihood that an event was an attack.

In 2022, Ge et al. [20] presented an approach to a distributed longitudinal platooning control of Connected Automated Vehicles (CAVs) that improved robustness and safety under DoS attacks on V2V communications. They came up with a model that was capable of handling such factors as variable mass of the vehicle, delays in the engine and non-linear forces of resistance.

In 2022, Park and Park [21] proposed the PIER method that was used to evaluate cybersecurity threats in CAVs. This method improved on conventional risk analysis by including new factors such as exposure and recovery factors in addition to probability and impact factors. The PIER method was tested with regards to software updates over the air and collision avoidance capabilities and it was shown that it was indeed capable of reducing risk indices.

In 2021, Ahmed et al. [22] developed a solution for DL-based IDS to improve security for CAN in vehicles. Based on the VGG structure, the system is capable of learning multiple network intrusion patterns and recognizing different types of attacks including DoS and fuzzy attacks. The proposed system was tested with the CAN-intrusion dataset to obtain an accuracy of 96% and a low FPR of 0. 6 % accuracy in comparison with more conventional ML approaches.

In 2021, Li et al. [23] presented two model update schemes for ML-based intrusion detection in the IoV. The first scheme, the cloud-assisted update, used a small set of labelled data for new attacks from the IoV cloud. The second scheme which was the local update comes into play when the cloud cannot afford to provide labeled data in time by using pseudo-labels of the pre-classified unlabeled data.

In 2021, Yang et al. [24] proposed a three-layered hierarchical IDS for protecting both the intravehicle and external vehicular networks. This IDS used both the signature-based approach and the anomaly-based approach as a way of detecting both known and unknown attacks. The experimental results show that the proposed system attains a recognition rate of 99. 9% accuracy for known attacks on the CAN-intrusion dataset and 99. The proposed model achieved a CICIDS2017 dataset accuracy of 88%.

In 2023, Alladi et al. [25] presented three DL-based misbehavior classification schemes for intrusion detection in IoV networks. DCLEs were developed for single or multi-step classification on vehicular edge servers using LSTM and Convolutional Neural Networks (CNNs). The schemes include preprocessing vehicular data collected by Road Side Units (RSUs) and forwarding the data to edge servers for classification.

B. Problem Statement

Table I defines the advantages and challenges of recent IDS using various methods. As ICVs become increasingly integrated into modern transportation systems, they are vulnerable to a myriad of cyber threats that can compromise their functionality and safety. The complexity of ICV networks, characterized by dynamic data flows and diverse communication protocols, necessitates robust IDS to identify and mitigate potential attacks in real-time. Traditional IDS methods often struggle to adapt to the evolving nature of threats, making it imperative to develop advanced solutions using ML and DL techniques to enhance detection accuracy and responsiveness. Utilizing ML and DL for IDS provides several advantages, including improved accuracy in detecting anomalies and previously unseen attacks due to their ability to learn from vast amounts of data and recognize complex patterns. These approaches can also adapt to changing environments, making them suitable for the dynamic nature of ICV networks. However, challenges remain, such as the need for high-quality labeled data for training, which is often scarce in cybersecurity contexts. Additionally, the computational requirements of ML/DL models can be significant, potentially leading to delays in real-time detection. Balancing model complexity with efficiency while ensuring robustness against adversarial attacks poses further hurdles that must be addressed in the development of effective IDS for ICVs.

TABLE I. ADVANTAGES AND CHALLENGES OF RECENT IDS USING VARIOUS METHODS

Authors/Year	Methods	Database	Advantages	Challenge	Achievements
Cheng *et al*, 2022	STC features, attention-based convolutional network, attention-short-term memory network	real-world vehicle attack dataset	Encodes spatial and temporal features simultaneously, and achieves strong anomaly classification with spatial-temporal attention features.	Model complexity due to dual-frame approaches, dependent on hyperparameter tuning.	Accuracy = 97% Precision = 93%
Alladi *et al*, 2021	DLEs	IoV Network Traffic Dataset	Uses MEC servers for real-time data processing, suitable for dynamic and time-sensitive IoV networks.	Limited details on specific datasets used, and potential scalability issues with MEC servers.	Accuracy = 95% Precision = 92% Recall = 90%
Yu *et al*, 2022	Federated LSTM neural network	IVN Attack Dataset	Federated learning framework for privacy-preserving model training, LSTM for ID sequence prediction.	Reliance on timely data from the IoV cloud is less effective if cloud data is not available.	Precision = 92% Recall = 91%
Pascale *et al*, 2021	Two-step algorithm: spatial-temporal analysis and Bayesian network	CAN-Bus Cyber-Attack Dataset	Integrates spatial and temporal analysis with Bayesian network for attack probability calculation, good accuracy on common attacks.	Reduced performance on Free State Attacks; limited to specific types of attacks.	Accuracy = 95%
Ge *et al*, 2022	Distributed longitudinal platooning control, resilient control law, design algorithm for DoS resilience	CAV-Platoon-Resilience Dataset	Handles diverse vehicle dynamics and DoS attacks, designed for stability, resilience, and scalability.	Focused on platooning control, may not address other types of attacks beyond DoS.	Accuracy = 93%
Park and Park, 2022	PIER method: exposure, recovery, probability, and impact factors for risk assessment	CAV-Cybersecurity-Risk Assessment Dataset	Enhances traditional risk assessment by including new factors, and improves risk determination efficiency and coverage.	Limited application scope, and effectiveness dependent on the implementation of security measures.	Accuracy = 92% Precision = 88%
Ahmed *et al*, 2021	DL-based IDS with VGG architecture	CAN-intrusion dataset	High accuracy in detecting various attacks, significantly lower false positive rate compared to conventional methods.	Focused primarily on the CAN network, may need further validation on other network types.	Accuracy = 96% FPR = 0.6%
Li *et al*, 2021	Two model update schemes: cloud-assisted and local update with pseudo-labels	AWID Dataset	Increases detection accuracy by 23%, local update scheme enables updates without cloud-provided labelled data.	Potential dependence on the availability of labelled data, local schemes may be complex.	Accuracy = 92% FNR = 13%

Yang *et al*, 2021	Three-layered hierarchical IDS combining signature-based and anomaly-based approaches	CAN-intrusion dataset, CICIDS2017	High accuracy in detecting known attacks, effective zero-day attack detection with fast processing times.	May need to optimize for specific types of zero-day attacks and large data processing requirements.	Accuracy = 99% F1 score = 80%
Alladi *et al*, 2023	DL-based misbehavior classification using LSTM and CNNs	VeReMi Extension datas et	Identifies 18 types of vehicular behavior; high F1-scores and fast processing times.	May require extensive computational resources for deep learning models.	F1 score = 95.58%

III. A Novel IDS Model

A. Proposed Architecture

This paper presents an advanced IDS designed to secure ICV networks through DL techniques. The framework is divided into five key phases: (i) Data Collection, (ii) Data Pre-processing, (iii) Feature Extraction, (iv) Dimensionality Reduction, and (v) Intrusion detection and mitigation. Initially, raw data from the CIC IoV dataset 2024 are pre-processed using MI for data cleaning. Significant features are then extracted using higher-order statistical features, Proposed IMI, Correlation, and Entropy methods. Dimensionality reduction is performed via ILDA. Finally, the intrusion classification is achieved using the Meta-Heuristic QIF-RNN, which integrates QNN, RNN, and Fuzzy Logic. Membership function optimization of fuzzy logic (decision maker) is carried out using the SA-FPA, and the outcome is obtained by fusing QNN, RNN, and optimized fuzzy logic. The identified attackers are mitigated via the Policy Gradient Method. Fig. 1 shows the overview of the proposed model.

B. Data Collection

Raw data are first obtained from the CIC IoV 2024 dataset (https://www.unb.ca/cic/datasets/iov-dataset-2024.html). The topmost CICIoV2024 dataset directory contains four subdirectories pertaining to three different files named as follows:

- Hexadecimal: Data captured in hexadecimal mode (benign, DoS, spoofing-GAS, spoofing-RPM, spoofing-SPEED, and spoofing-STEERING_WHEEL).
- Decimal: Data captured in decimal mode (benign, DoS, spoofing-GAS, spoofing-RPM, spoofing-SPEED, and spoofing-STEERING_WHEEL).
- Binary: Data captured in binary mode (benign, DoS, spoofing-GAS, spoofing-RPM, spoofing-SPEED, and spoofing-STEERING_WHEEL).

C. Data Pre-Processing

It plays a crucial role in enhancing data quality by cleaning and normalizing the raw input, which helps eliminate noise and irrelevant information.

1) MI: It is a simple technique used to handle missing data by replacing missing values with the mean of the available data for a particular feature. This method is commonly used to maintain the dataset's size and ensure continuity in the analysis without distorting the data [26]. Eq. (1) shows the MI procedure. For a feature X, with N observed values, $\hat{X}$ points to the observed value's mean, and X_i signifies non-missing values.

$$\hat{X} = \frac{1}{N}\sum_{i=1}^{N} X_i \quad (1)$$

D. Feature Extraction

Feature extraction includes selecting or transforming relevant features from the CICIoV2024 dataset. It helps in improving the efficiency of the subsequent classification process. From the pre-processed data, features like proposed higher orders statistical features, IMI, Correlation, and Entropy are extracted.

1) Higher-order statistical features: It is used to capture non-linear dependencies and subtle statistical properties in data that are not evident through basic statistical measures like mean or variance. These features are often derived from moments and cumulants, which describe the shape and characteristics of data distributions beyond first and second-order statistics. Table II shows the Higher-order Statistical features and their mathematical expressions [27].

TABLE II. Higher-Order Statistical Features and their Equations

Features	Formula	Description
Skewness V_z	$V_z = \frac{1}{Q}\sum_{l=1}^{q}\left(\frac{a_l-\mu}{\sigma}\right)^3$	Q is total number of values, q is number of values ranging from 1 to Q, a_l be the individual values in the set, μ means the mean value, σ be the standard deviation, $\sum_{l=1}^{q}\left(\frac{a_l-\mu}{\sigma}\right)^3$ be the values deviate from the mean in terms of the cube.
Kurtosis N	$N = \frac{1}{Q}\sum_{l=1}^{q}\left(\frac{a_l-\mu}{\sigma}\right)^4$	$\sum_{l=1}^{q}\left(\frac{a_l-\mu}{\sigma}\right)^4$ be the Sum of the fourth power differences.
Higher-Order Moments M_h	$M_h = \frac{1}{Q}\sum_{l=1}^{q}(a_l-\mu)^h$	h indicates the order of the moment, with $h \geq 3$ representing higher-order moments beyond variance (second-order)

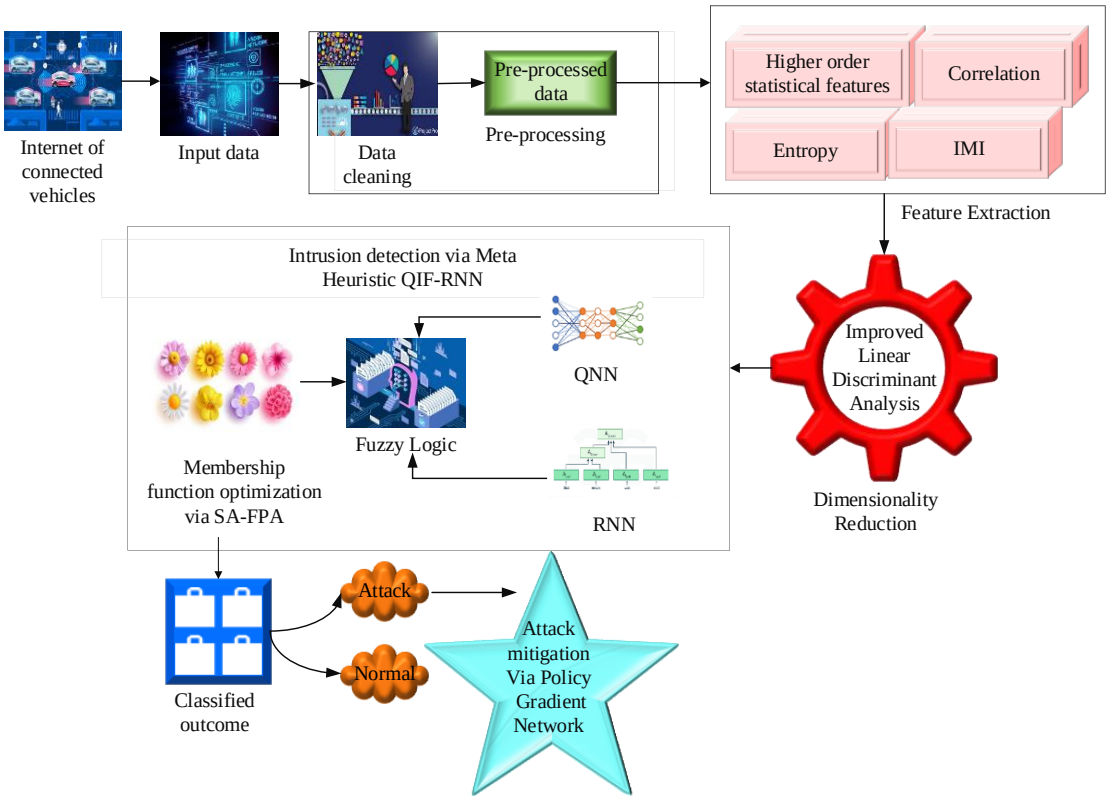


Fig. 1. Overview of the proposed model.

2) Entropy: In the context of an IDS, entropy is used to measure the distribution of different types of network packets, protocols, or system events. A significant deviation in entropy indicates unusual behavior, like a Distributed Denial of Service (DDoS) attack, where packet distributions change unexpectedly. Eq. (2) describes the entropy feature $E(X)$ extraction for IDS, in which $\rho(x_i)$ specifies the probability of occurrence of i^{th} event or value in the dataset, and n refers to total number of unique events or values.

$$E(X) = -\sum_{l=1}^{N} \rho(x_i)\rho(x_i) \quad (2)$$

3) IMI: An intuitive method for measuring the uncertainty of random variables and the information they share is provided by information theory, where two key ideas are mutual information and entropy [28]. A measure of the uncertainty of random variables is the entropy K. Assuming A to be a discrete random variable with alphabet χ and a probability mass function of $s(a) = Su\{A = a\}\, a\epsilon A$, the entropy of A is expressed as shown in Eq. (3).

$$K(A) = -\sum_{a\epsilon A} s(a)log(s(a)) \quad (3)$$

Although two random variables communicate information through a metric known as mutual information, which is shown in Eq. (4).

$$K(B;A) = \sum_{a\epsilon A} \sum_{b\epsilon B} s(b,a)log\frac{s(a,b)}{s(a)s(b)} = K(B) - K(\frac{B}{A}) \quad (4)$$

Where $K(\frac{B}{A})$ is the conditional entropy of B in the case of A is known, and can be represented as in Eq. (5).

$$K(\frac{B}{A}) = -\sum_{a\epsilon A} \sum_{b\epsilon B} s(b,a)log\left(s\left(\frac{b}{a}\right)\right) \quad (5)$$

The IMI and entropy for continuous random variables are defined in Eq. (6) – Eq. (8), respectively.

$$K(B) = -\int_a s(a)\ log\ log\left(s(a)\right) da \quad (6)$$

$$K(\frac{B}{A}) = -\int_{a,b} s(b,a)\ log\ log\left(s\left(\frac{b}{a}\right)\right) da\ db \quad (7)$$

$$K(B;A) = \int_{a,b} s(b,a)\ log\ log\ \frac{s(a,b)}{s(a)s(b)}\ da\ db \quad (8)$$

TABLE III. COMPARATIVE ANALYSIS: PROPOSED AND EXISTING FEATURE EXTRACTION APPROACHES

Metric	IMI	Entropy	Mutual Information
Accuracy	92%	85%	90%
Computational Time	12 seconds	20 seconds	15 seconds
F1-Score	0.88	0.8	0.86
Precision	0.89	0.81	0.87
Recall	0.88	0.79	0.85
Variance Explained	97%	93%	95%

Table III denotes comparative analysis of proposed and existing feature extraction approaches. The accuracy values reflect the fact that IMI substantially enhances the classifier's performance compared to traditional entropy and mutual information measures. The improvement from 85% to 92% shows the capture power of IMI for complex relations between variables. Furthermore, the relative computational time for the IMI measure is relatively low, which is only 12 seconds, while for entropy it took 20 seconds and for mutual information 15 seconds. This efficiency becomes highly valuable in those areas where large datasets are involved, or applications that require prompt outputs.

4) Correlation: A linear relationship among two variables is measured for both its strength and direction using correlation. Correlation is a technique used to determine the relationship between features in the context of feature extraction. A low correlation suggests independence, while a high correlation might point to redundancy.

E. Dimensionality Reduction

From the feature-extracted data, the dimensionality of the extracted features is reduced by utilizing ILDA.

1) ILDA: Statistical methods such as LDA [29] are now commonly employed as ML models for pattern recognition. The method involves projecting data into lower dimensional spaces in order to maximize class separability. Using Fisher's criteria, the optimal strategy for class separation is to maximize the ratio of the average difference to the total number of variables in the projection space for the two groups. The eigenvalue and eigenvector of the ideal projection transformation matrix $T_X^{-1}T_C$, where T_X and T_C are respectively the within-class and between-class scatter matrices, are the outcomes of the maximum ratio. More precisely, ILDA resolves the subsequent optimal problem utilizing Eq. (9).

$$K(x) = \frac{|\tilde{\mu}_1 - \tilde{\mu}_2|^2}{\tilde{T}_1^2 \tilde{T}_2^2} = \frac{x^{U}T_C x}{x^{U}T_C x} \quad (9)$$

where $\tilde{T}_1$ and $\tilde{T}_2$ are respective distribution matrices for classes 1 and 2. Consequently, $K(x)$ represents a measure of the within-class scatter matrix adjusted by a measure of the class mean difference. To determine $K(x)$'s maximum, differentiate and equal to zero and their mathematical expression is shown in Eq. (10) and Eq. (11).

$$\frac{d}{dx}K(u) = \frac{d}{dx}\left(\frac{x^{U}T_C x}{x^{U}T_C x}\right) = 0 \quad (10)$$

$$T_X^{-1}T_C - K(x)x = 0 \quad (11)$$

Resolving the problem of generalized eigenvalues is presented in Eq. (12).

$$T_X^{-1}T_C x = \lambda x \; where \; \lambda = K(x) = Scalar \quad (12)$$

Yield, the mathematical expression of x^* is shown in Eq. (13) and Eq. (14), respectively.

$$x^* = arg\ arg\ Max\ x\ K(x) = arg\ arg\ Max\ x\ \frac{x^{U}T_C x}{x^{U}T_C x} \quad (13)$$

$$x^* = T_X^{-1}(\mu_1 - \mu_2) \quad (14)$$

The mathematical expression of z is presented in Eq. (15).

$$z = x^{U}y, \quad (15)$$

where, y is a variable input, x vector projection, and z is a new feature in projection space used to find the projection space.

TABLE IV. COMPARATIVE ANALYSIS: LDA VS. ILDA

Metric	LDA	ILDA
Accuracy	85% (170/200)	90% (180/200)
Recall	0.8	0.85
F1-Score	0.81	0.86
Precision	0.82	0.88
Variance Explained (%)	95%	96%
Dimensionality Reduced (D)	10 to 2	10 to 2
Computational Time (s)	25	15

A comparison of the ILDA (Incremental Linear Discriminant Analysis) with the classic LDA (Linear Discriminant Analysis) highlights very important advantages of ILDA over a dynamic and evolving dataset, as depicted in Table IV, that the accuracy of ILDA is superior compared to LDA, where there is a great improvement from 85% to 90%. This indicates that ILDA could classify instances more effectively as the dataset grows or changes. It can be noticed from precision and recall values that it has resulted in increased accuracy. ILDA reflected a much greater precision at 0.88 compared with that of LDA, which was only 0.82. The same thing happened with recall: ILDA at 0.85 versus 0.80 with LDA. These improvements, therefore, say ILDA to be more effective in true positive identification, minimizing false positives as well as false negatives.

F. Classification

Using the dimensionality-reduced features, the data is classified via a Meta-Heuristic QIF-RNN. The suggested model is a combination of the QNN, RNN, and Fuzzy logic. The membership function optimization is acquired via the SA-FPA. Then the QNN, RNN, and membership function optimization are fused in the fuzzy logic to acquire an outcome.

1) QNN: A Neural Network (NN) inspired by quantum computing principles that helps in capturing complex relationships within the data, providing more powerful learning capabilities than traditional neural networks [30]. The QNN functions as a quantum circuit by acting on quantum input data through a series of parameter-dependent quantum gates, also known as unitary operators. Typically, a QNN is displayed in Eq. (16).

$$V(\theta) = \prod_{m=1}^{O} W_m V_m(\theta_m) \quad (16)$$

Eq. (16) results from O quantum layers. The product of parametric quantum gates $V_m(\theta_m)$ and non-parametric quantum gates V_m, where θ_m are variational parameters, that make up the l^{th} quantum layer. The parametric quantum gates $V_m(\theta_m)$ in the m^{th} layer is expressed as the generation of T parametric quantum gates and its mathematical expression is shown in Eq.

(17), in which Euler's formula is used to translate each parametric quantum gate $V_{m,k}(\theta_{m,k})$ as shown in Eq. (18).

$$V_m(\theta_m) \equiv T \otimes k = 1\, V_{m,k}(\theta_{m,k}) \quad (17)$$

$$exp\left(-j\theta_{m,k}Q\right) = J\, cos(\theta_{m,k}) - j\, sin(\theta_{m,k})Q \quad (18)$$

where Q is a Pauli operator functioning on qubits from the set $\{Y, Z, A\}$, $J\ is\ a\ 2 \times 2$ identity matrix, and j is the imaginary integer. The measurement result based on the readout qubits' computational basis is the QNN's output. Given that a qubit's measurement result is probabilistic, the measurement findings' expectation value, or E, is the QNN output. The expression of F is shown in Eq. (19).

$$F = \langle \Psi_y | V^{\dagger}(\theta) N V(\theta) | \Psi_y \rangle \quad (19)$$

where $|\Psi_y\rangle$ is represented as the QNN's input quantum state, and N is a linear amalgamation of Pauli operators that act as readout qubit observables. In a hybrid quantum-classical model, the loss M of a training example is computed conventionally on a classical device. An objective function $m(.)$ of the task is used to determine the loss L for the given training sample based on the actual output F and the expected output z. expression of the M is presented in Eq. (20).

$$M = m(F, z) \quad (20)$$

In the model optimization stage, the QNN update its variational parameters via back-propagation and gradient descent, just like a standard NN. It computes the gradient of a variational parameter θ_l in the $l-th$ quantum layer with respect to loss M using the following Eq. (21).

$$\frac{\partial M}{\partial \theta_l} = \frac{\partial M}{\partial F}\frac{\partial F}{\partial \theta_l} \quad (21)$$

$\partial M/\partial F$ is easily obtained using the objective function $m(.)$. $\partial F/\partial \theta_l$ is computed using Eq. (22).

$$\frac{\partial F}{\partial \theta_l} = j\langle \Psi_y | V_{-}^{\dagger}\left[Q_l,\, V_{+}^{\dagger} I V_{+}\right] V_{-} | \Psi_y \rangle \quad (22)$$

where, the Eq. (23) is represented as,

$$V_{+} = \prod_{m=l+1}^{o} W_m V(\theta_l)\ \ and\ V_{-} = \prod_{m=1}^{m=l} W_m V(\theta_l) \quad (23)$$

2) RNN [31]: It serves as a pivotal component, contributing to the model's efficacy in processing sequential data and capturing hierarchical dependencies within the input features. The proposed QIF-RNN excels in identifying complex patterns and relationships within the input features, ultimately enhancing its performance in data classification tasks by utilizing the inherent ability of RNNs to capture dependencies in sequential data. Fig. 2 shows the Structure of the QIF-RNN.

3) Fuzzy logic: It is a mathematical framework that deals with uncertainty and imprecision, where traditional binary logic fails. It helps to capture the vagueness in data, making the system more flexible and robust [32].

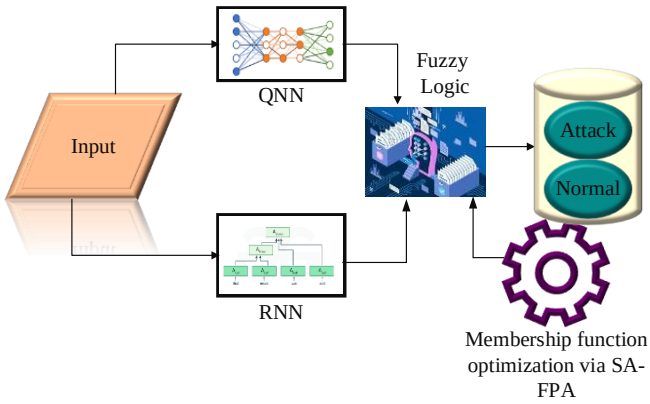


Fig. 2. Architecture of QIF-RNN.

a) Fuzzy sets: Crisp sets that have had their characteristic function changed to the membership function A: X →[0,1] are known as fuzzy sets.

b) Properties of fuzzy sets: Various properties of Fuzzy sets is presented in Table V. Algorithm 1 shows the pseudocode of Fuzzy decision-making.

TABLE V. PROPERTIES OF FUZZY SETS

Operation	Crisp	Fuzzy
Addition	$J + V$	$\tilde{J} + \tilde{V} = [J_1^{(\propto)} + V_1^{(\propto)}, J_3^{(\propto)} + V_3^{(\propto)}]$
Subtraction	$J - V$	$\tilde{J} - \tilde{V} = [J_1^{(\propto)} - V_3^{(\propto)}, J_3^{(\propto)} - V_1^{(\propto)}]$
Multiplication	$J \cdot V$	$\tilde{J} \cdot \tilde{V} = [J_1^{(\propto)} \cdot V_1^{(\propto)}, J_3^{(\propto)} \cdot V_3^{(\propto)}]$
Division	$J \div V$	$\tilde{J} + \tilde{V} = [J_1^{(\propto)} \div V_3^{(\propto)}, J_3^{(\propto)} \div V_1^{(\propto)}], if\ 0 \notin [V_1^{(\propto)}, V_3^{(\propto)}]$

4) Membership function optimization: It is acquired via the SA-FPA.

Algorithm 1: Pseudocode for Fuzzy Decision Making
Using fuzzy decision-making entails the subsequent actions:
Step 1: The identification of variables and the completion of the alternatives is the first phase.
Step 2: The linguistic parameters are transformed from real variables throughout the fuzzification process.
Step 3: The user chooses the variables that must be entered into the knowledge base.
Step 4: A membership function is the expression of a membership function in a mathematical function.
Step 5: Giving the if-then condition rule is the next step. One rule is represented by each variable.
Step 6: Converting the fuzzy value to an output variable is the next step.
Step 7: Practical implementation of the alternative is the final stage of the fuzzy process. If the implementation is successful, the system's performance will improve concerning the process's goal.

a) Proposed SA-FPA: Flowering plants reproduce, and FPA mimics this process [33]. The proposed SA-FPA is used for optimizing the fuzzy membership functions. Membership functions define how each data point belongs to a fuzzy set (e.g., low, medium, high). SA-FPA adapts these membership functions for optimal performance, ensuring that the fuzzy logic system can accurately represent the underlying uncertainties in the data. Algorithm 2 defines the FPA procedure.

Algorithm 2: SA-FPA Procedure
Step 1: The process of biotic pollination is regarded as worldwide, with pollinators carrying out Levy flights.
Step 2: The process of abiotic pollination is seen as a local one.
Step 3: Flower constancy is examined using the hypothesis that the degree of similarities between the flowers in question and the likelihood of reproduction are inversely connected.
Step 4: Whether a pollination technique is local or global is determined by a switching probability p in the interval [0, 1].

A flower m represents a solution vector b_m in FPA. Two distinct search techniques are used by the algorithm: local and global pollination. Utilizing the following Eq. (24), the first and third FPA criteria could be used to numerically express the global pollination procedure.

$$b_m^{x+1} = b_m^x + \gamma \cdot P(\lambda) \cdot (k^* - b_m^x) \quad (24)$$

where $k^*$is the finest flower in the populace of flowers at iteration x, b_m^x represents flower m at iteration x, λ is a constant, γ is a constant scaling aspect to control the step size and $P(\lambda) > 0$ is the Le´vy flight step size, which is drawn from a Le´vy distribution and characterizes the strength of the pollination; $\Gamma(\lambda)$ is the usual gamma function and $w > 0$. The mathematical expression of p is presented in Eq. (25).

$$P \sim \frac{\lambda \Gamma(\lambda) sin sin\left(\frac{\pi\lambda}{2}\right)}{\pi} \cdot \frac{1}{w^{1+\lambda}}, (w > 0), \quad (25)$$

Conversely, the following Eq. (26) represents the local pollination rule (second rule) and floral dependability (third rule), where e is taken from a uniform distribution in [0, 1] and b_n^x and b_o^x are distinct flowers of the same population.

$$b_m^{x+1} = b_m^x + \varepsilon \cdot (b_n^x - b_o^x) \quad (26)$$

As per the fourth rule, a switch probability t in [0, 1] determines the kind of flower pollination (local or global). Reiterating the earlier data. Eq. (27) expresses the fitness estimation of proposed SA-FPA, in which ρ_i refers to prediction error for each fuzzy set, c_i indicates complexity of the membership function, $s(M)$ signifies constraint function ensuring feasible membership function structures, and γ addresses regularization parameter balancing error minimization and function complexity.

$$f_{opt} = \left(\sum_{i=1}^{N} \left(\frac{\rho_i}{c_i}\right) + \gamma s(M) \right) \quad (27)$$

Fig. 3 displays the FPA flowchart, where r is the population size of flowers and h is the number of problem dimensions. Once the QNN and RNN have processed the data, the outputs are fused with the optimized fuzzy logic system. The fusion helps in incorporating both the sequential information (handled by RNN) and the non-binary decision-making capacity (handled by fuzzy logic).

The final classification output O is derived by combining the outputs from QNN, RNN, and the fuzzy system. Let O_{qnn} and O_{rnn} be the outputs from the QNN and RNN, and O_{fuzzy} be the fuzzy logic decision, Eq. (28) states the overall classification output, in which α, β, and γ means for weighting factors to balance the contributions from each component.

$$O = \alpha \cdot O_{qnn} + \beta \cdot O_{rnn} + \gamma \cdot O_{fuzzy} \quad (28)$$

This combined approach allows the QIF-RNN model to utilize the strengths of quantum-inspired learning, sequence prediction, and handling of uncertainty to achieve a highly accurate classification.

G. Attack Mitigation via Policy Gradient Method

The Policy Gradient method is one such technique in reinforcement learning, which achieves those situations where the number of possible actions is high dimensional or continuous is practical for Q-learning. Unlike Q-learning, which emphasizes verdict optimal actions, policy gradient seeks optimal parameters θ for a policy π_θ which would maximize the total reward. The chief aim of the policy gradient is to maximize the expectation of return or collected reward starting from a given initial state. That is, it is apprehended by Eq. (29).

$$J(\pi_\theta) = E_{\tau \sim \pi_\theta}[r(\tau)] = \int \pi_\theta(\tau) r(\tau) d\tau \quad (29)$$

Here, $\pi_\theta(\tau)$ indicates the probability of observant trajectory τ. The method learns the optimal parameter θ by calculating the gradient $\nabla_\theta J(\pi_\theta)$ as per the Eq. (30).

$$\nabla_\theta J(\pi_\theta) = E_{\tau \sim d_{\pi_\theta}}[\sum_{t=1}^{T} r(s_t, a_t) \sum_{t=1}^{T} \nabla_\theta log\ log\ \pi_\theta(s_t, a_t)] \quad (30)$$

In the above equation, d_{π_θ} is the distribution of trajectories produced by policy π_θ . The derivation encompasses the substitution in the Eq. (31).

$$\pi_\theta(\tau) = p(s_1) \prod_{t=1}^{T} \pi_\theta(s_t, a_t) p(s_{t+1} | s_t, a_t) \quad (31)$$

Here, $p(\cdot)$ is independent of the policy parameter θ, and for simplicity, it's not explicitly encompassed in the derivation.

TABLE VI. ATTACK MITIGATION APPROACH: A COMPARATIVE ANALYSIS OF POLICY GRADIENT APPROACH AND Q-LEARNING

Method	Convergence Speed	Average Total Reward	Sample Efficiency	Robustness
Policy Gradient	Fast	High (85)	Moderate	High (10% drop)
Q-Learning	Moderate	Moderate (70)	Low	Low (30% drop)

As indicated in Table VI, we compare the two leading reinforcement learning methods, Policy Gradient and Q-Learning, with a focus solely on attack mitigation. In these dimensions—convergence speed, average total reward, and robustness—the Policy Gradient approach performs better than the Q-Learning method. Hence, this makes policy gradient more viable for dynamic and complex environments.

IV. SIMULATION RESULTS

A. Simulation Setup

The proposed IDS model via suggested QIF-RNN was developed via Python on an Intel core® i5 processor @2.6GHz, 16 GB RAM, 64-bit OS. Here, CICIoV2024 dataset was utilized for detection which is accessible via (https://www.kaggle.com/datasets/hassan06/nslkdd) [Accessed

Date: 24-09-2024]. 70% of the collected data has been used for training and 30% for testing. This assessment considered various metrics like sensitivity, specificity, accuracy, precision, False Positive Rate (FPR), False Negative Rate (FNR), NPV, F1-score, Matthews Correlation Coefficient (MCC), and Recall.

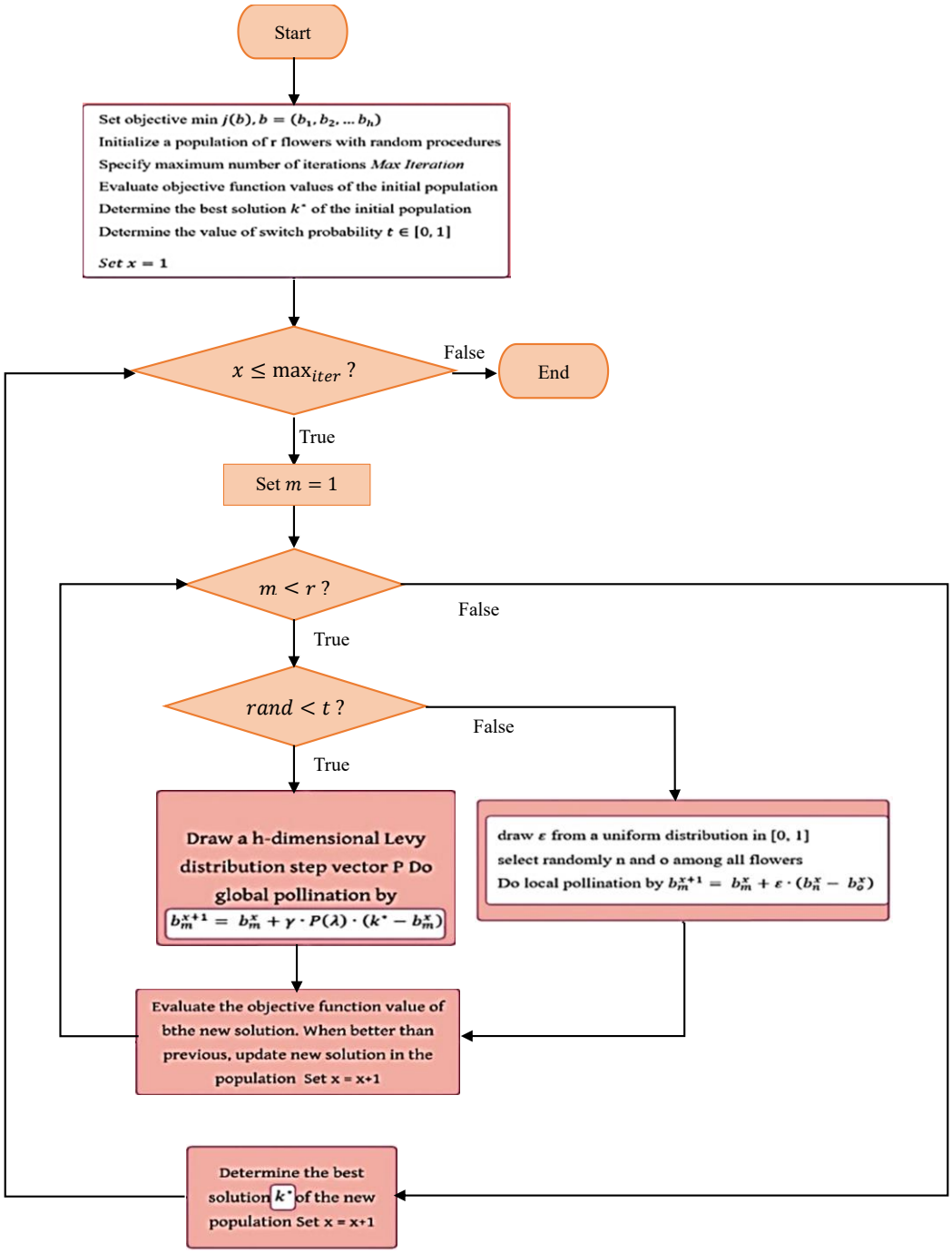


Fig. 3. Flow chart of proposed SA-FPA.

B. *Intrusion Detection Network: Performance Analysis for 70/30 Data Split*

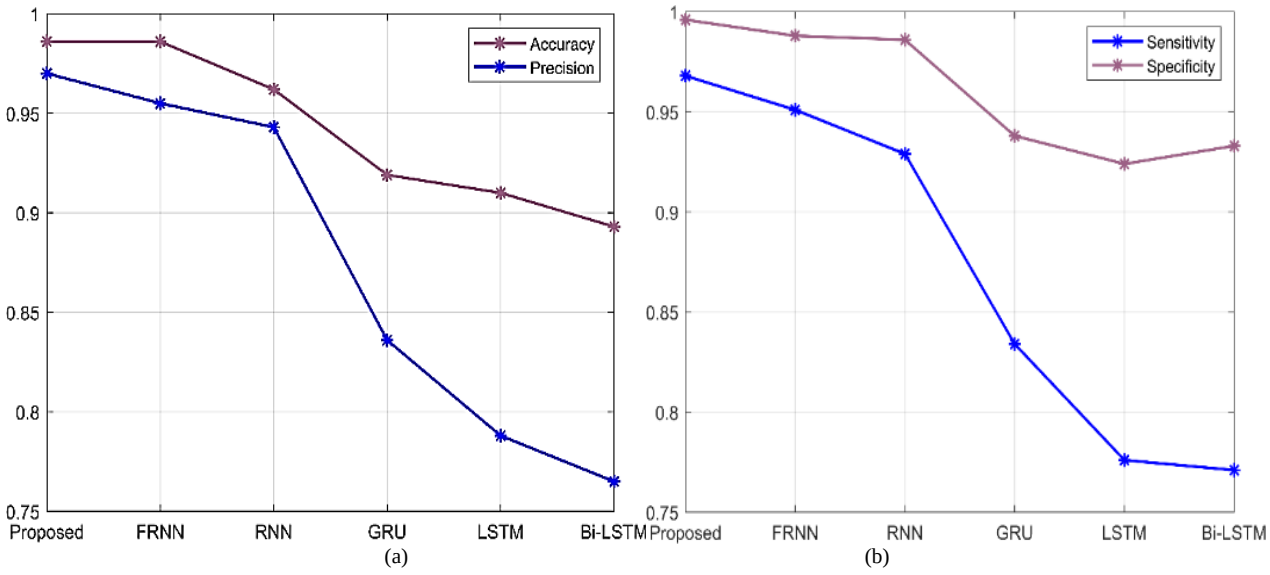
The comprehensive performance analysis demonstrates the superiority of the suggested ensemble framework with quantum learning over the other models already in use, such as Fuzzy RNN (FRNN) [34], RNN, GRU [35], LSTM [35], and Bi-LSTM [36], on a range of critical metrics in Fig. 4. With a sensitivity of 96.8%, the suggested model outperforms FRNN (95.1%), RNN (92.9%), GRU (83.4%), LSTM (77.6%), and Bi-LSTM (77.1%). This indicates the enhanced ability of the suggested model to precisely identify affirmative cases, which is essential for successful intrusion detection. The suggested model outperforms FRNN (98.8%), RNN (98.6%), GRU (93.8%), LSTM (92.4%), and Bi-LSTM (93.3%) in terms of

specificity, achieving a phenomenal 99.6%. The high specificity highlights how well the suggested model can identify negative instances and reduce false positives, which is an important consideration in real-world intrusion detection scenarios. The suggested model's total accuracy is 98.6%, which is higher than that of FRNN (98.6%), RNN (96.2%), GRU (91.9%), LSTM (91.0%), and Bi-LSTM (89.3%). This high accuracy illustrates how the suggested ensemble architecture is resilient in producing accurate and trustworthy classifications for both positive and negative examples. The suggested model's precision, a crucial parameter for assessing the model's capacity to reduce false positives, is reported to be 97%, surpassing that of FRNN (95.5%), RNN (94.3%), GRU (83.6%), LSTM (78.8%), and Bi-LSTM (76.5%). The accuracy with which the suggested model identifies intrusions is demonstrated by its precision.

The suggested model's F1-score, which weighs recall and precision, is stated as 96.4%, indicating that it can successfully strike an equilibrium between accuracy and completeness. This is superior to LSTM (79.7%), Bi-LSTM (77.3%), GRU (83.0%), RNN (94.5%), and FRNN (96.1%). The suggested model consistently outperforms other models in addition to maintaining a high Negative Predictive Value (NPV) of 99.2%. The remarkably low FPR and FNR, which stand at 2.9% and 7%, correspondingly, highlight the potential of the suggested approach to reduce misclassifications. The suggested model's overall Matthews Correlation Coefficient (MCC), which measures how well the model captures genuine correlations in the data, is stated as 94.6%. When compared to FRNN, RNN, GRU, LSTM, and Bi-LSTM, the suggested ensemble architecture consistently performs better across sensitivity, specificity, accuracy, precision, recall, F-measure, NPV, and Matthews Correlation Coefficient. The suggested model is shown by this thorough analysis as a cutting-edge and promising data categorization method, especially for data classification. Table VII shows the Comparative analysis of the suggested framework and existing model performance metrics.

TABLE VII. COMPARATIVE ANALYSIS OF PERFORMANCE METRICS WITH EXISTING MODELS

Metrics	Sensitivity	Specificity	Accuracy	Precision	F1-Score	NPV	FPR	FNR	MCC
Proposed	0.968	0.996	0.986	0.97	0.964	0.992	0.029	0.07	0.946
FRNN	0.951	0.988	0.986	0.955	0.961	0.992	0.036	0.072	0.921
NN	0.929	0.986	0.962	0.943	0.945	0.983	0.038	0.089	0.897
GRU	0.834	0.938	0.919	0.836	0.83	0.962	0.078	0.206	0.771
LSTM	0.776	0.924	0.91	0.788	0.797	0.947	0.099	0.259	0.707
Bi-LSTM	0.771	0.933	0.893	0.765	0.773	0.931	0.108	0.271	0.689



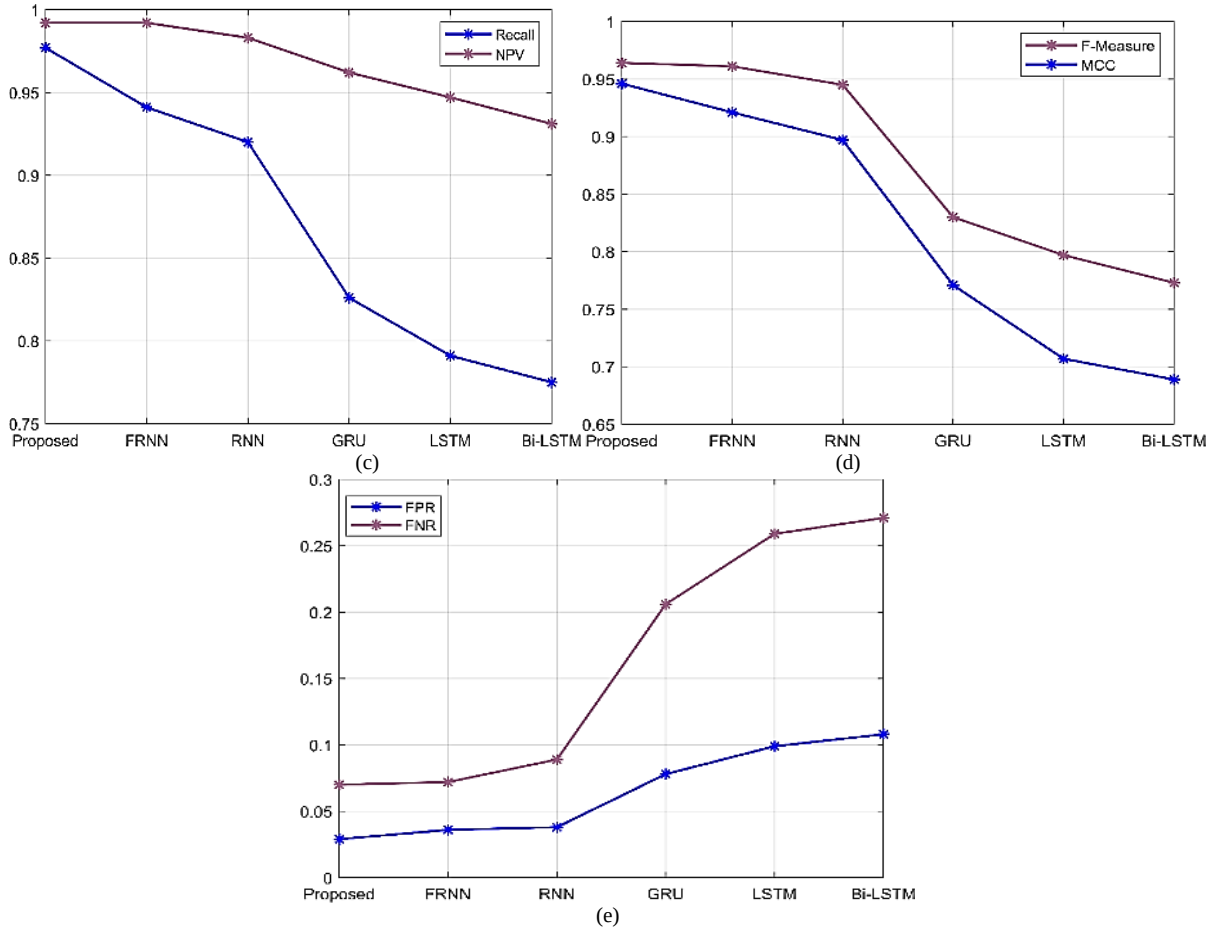


Fig. 4. Performance of proposed QIF-RNN over other algorithms for (a) Accuracy and precision, (b) Sensitivity and specificity, (c) Recall and NPV, (d) F1-Score and MCC, and (e) FPR and FNR.

C. Comparative Analysis of Proposed Intrusion Detector Model over SOTA Approaches for Varying Learning Rate

The research proposed a novel Meta-Heuristic QIF-RNN for IDS, structured into five phases: (i) Data Collection, (ii) Pre-processing, (iii) Feature Extraction, (iv) Dimensionality Reduction, and (v) Meta-Heuristic QIF-RNN-based Data Classification.

Table VIII shows the performance of the proposed model in comparison to the prevailing models in terms of Accuracy, Precision, Sensitivity, F-score, Specificity, MCC, FPR, and FNR. The proposed Model gives highest accuracy value of 98.261%, the precision of 98.095%, and F1-score of 97.549%, hence overall better performance due to higher values of correct classification. The Quantum network along with fuzzy and meta-heuristic optimization assisted in enhancing the classification accuracy of the model.

Table IX discusses the contrast of the performance of the proposed model with the existing models on metrics such as Accuracy, Precision, Sensitivity, F-score, Specificity, MCC, FPR, and FNR. The proposed Model reflects better performance on all these metrics with the highest value in accuracy of 99.755% and precision of 99.901%. Its high sensitivity of 98.655% and specificity of 99.075% show its higher classification accuracy in identifying the attacks. The fuzzy logic-based classification has enhanced the detection accuracy of the model. Thus, making it accurate in detecting the attacks.

TABLE VIII. COMPARATIVE ANALYSIS OF PERFORMANCE METRICS WITH EXISTING MODELS

Model	Accuracy	Precision	F-Score	Specificity	Sensitivity	MCC	FPR	FNR
Proposed	0.98261	0.98095	0.97549	0.98961	0.98108	0.98398	0.0263	0.0107
LSTM [18]	0.95429	0.95683	0.95927	0.95939	0.95892	0.95478	0.0571	0.0639
CNN [25]	0.96828	0.96545	0.96118	0.96321	0.96478	0.96828	0.0441	0.0512
MTH-IDS[24]	0.95105	0.95323	0.95124	0.95806	0.95308	0.95939	0.0501	0.0436
QNN [30]	0.94048	0.94685	0.95118	0.95621	0.94478	0.95828	0.0431	0.0312

TABLE IX. COMPARATIVE ANALYSIS OF PERFORMANCE METRICS WITH EXISTING MODELS

Model	Accuracy	Precision	F-Score	Specificity	Sensitivity	MCC	FPR	FNR
Proposed	0.99755	0.99901	0.98404	0.99075	0.98655	0.99765	0.0141	0.0092
LSTM [18]	0.96765	0.96909	0.96683	0.96333	0.96909	0.96675	0.0461	0.0553
CNN [25]	0.97081	0.97683	0.97771	0.97684	0.97308	0.97617	0.0361	0.0223
MTH-IDS[24]	0.96538	0.96323	0.96118	0.96286	0.96694	0.96828	0.0421	0.0323
QNN [30]	0.95833	0.95683	0.96393	0.96231	0.95254	0.96161	0.0391	0.0236

V. DISCUSSION

The proposed Meta-Heuristic QIF-RNN model for IDS brings several advantages. First, the structured approach involves multiple phases such as data preprocessing steps that ensure only relevant and clean data are used for classification. The use of higher-order statistical features, IMI, correlation, and entropy ensures that the model captures critical attributes of the data. These data helped in detecting intrusions more effectively. Furthermore, the integration of QNN, RNN, and Fuzzy Logic in the classification phase allows the model to handle both sequential and fuzzy data, leading to high classification accuracy of 98.6%. The SA-FPA optimization of the membership function enhances the precision of the decision-making process. Also, the Policy Gradient Method contributes to effective attack mitigation. These features make the model robust in detecting and mitigating cyber threats in ICVs.

Despite these advantages, the model also has limitations. While the use of dimensionality reduction (ILDA) helps minimize the computational load, the complexity introduced by combining multiple components (QNN, RNN, Fuzzy Logic, and SA-FPA) leads to increased computational overhead. This might limit its scalability in real-time environments, particularly when dealing with large-scale and high-speed networks like those in ICVs. Another potential limitation is the static nature of the dataset used (CICIoV2024). It may not represent real-time or evolving attack scenarios. As the research suggests, future improvements could focus on incorporating real-time data streams and advanced optimization techniques to address these limitations.

VI. CONCLUSION

The research proposed a novel Meta-Heuristic QIF-RNN for IDS, structured into five phases: (i) Data Collection, (ii) Pre-processing, (iii) Feature Extraction, (iv) Dimensionality Reduction, and (v) Meta-Heuristic QIF-RNN-based Data Classification. Initially, raw data were collected from the CICIoV2024 dataset, which then underwent preprocessing through a data-cleaning technique. From the pre-processed data, significant features including Higher-Order Statistical Features, IMI, Correlation, and Entropy were extracted. The dimensionality of these extracted features was subsequently reduced using ILDA. Finally, the data were classified using the dimensionality-reduced features in conjunction with the Meta-Heuristic QIF-RNN model, which integrated QNN, RNN, and Fuzzy Logic. The optimization of the membership function was achieved through SA-FPA. The attack mitigation is achieved via the Policy Gradient Method. The proposed model attained 98.6% accuracy and outran existing models. Integrating complex DL algorithms (QNN, and RNN) requires considerable computational time. Future work could focus on enhancing the Meta-Heuristic QIF-RNN model by incorporating real-time data streams for dynamic intrusion detection in ICVs. Additionally, exploring advanced optimization algorithms and integrating ensemble learning techniques improve classification accuracy and robustness. Investigating the model's adaptability to emerging cyber threats and conducting extensive performance evaluations in diverse network environments could further strengthen its applicability. Finally, expanding the feature extraction methods to include DL-based approaches yields richer insights and enhances the model's predictive capabilities.

DATASET ACCESSIBILITY

The dataset used in your study, CICIoV2024, is referenced as accessible through the link to the Kaggle dataset (https://www.kaggle.com/datasets/pushpakattarde/ciciov2024decimalcsv), which is publicly available for download. This ensures reproducibility for anyone looking to replicate the results.

ACKNOWLEDGEMENT

The author extends the appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through the project number (R-2024-1153).

REFERENCES

[1] Hadjilambrinos, C. (2021). Reexamining the automobile's past: What were the critical factors that determined the emergence of the internal combustion engine as the dominant automotive technology?. Bulletin of Science, Technology & Society, 41(2-3), 58-71.

[2] Boysen, N., Schulze, P., & Scholl, A. (2022). Assembly line balancing: What happened in the last fifteen years?. European Journal of Operational Research, 301(3), 797-814.

[3] Cao, J., Lin, L., Zhang, J., Zhang, L., Wang, Y., & Wang, J. (2021). The development and validation of the perceived safety of intelligent connected vehicles scale. Accident Analysis & Prevention, 154, 106092.

[4] Campisi, T., Severino, A., Al-Rashid, M. A., & Pau, G. (2021). The development of the smart cities in the connected and autonomous vehicles (CAVs) era: From mobility patterns to scaling in cities. Infrastructures, 6(7), 100.

[5] Xie, Y., Zhou, Y., Xu, J., Zhou, J., Chen, X., & Xiao, F. (2021). Cybersecurity protection on in-vehicle networks for distributed automotive cyber-physical systems: state-of-the-art and future challenges. Software: Practice and Experience, 51(11), 2108-2127.

[6] Feng, Y., Huang, S. E., Wong, W., Chen, Q. A., Mao, Z. M., & Liu, H. X. (2022). On the cybersecurity of traffic signal control system with connected vehicles. IEEE Transactions on Intelligent Transportation Systems, 23(9), 16267-16279.

[7] Garcia, M. H. C., Molina-Galan, A., Boban, M., Gozalvez, J., Coll-Perales, B., Şahin, T., & Kousaridas, A. (2021). A tutorial on 5G NR V2X

communications. IEEE Communications Surveys & Tutorials, 23(3), 1972-2026.

[8] Rahman, M. A., Rahim, M. A., Rahman, M. M., Moustafa, N., Razzak, I., Ahmad, T., & Patwary, M. N. (2022). A secure and intelligent framework for vehicle health monitoring exploiting big-data analytics. IEEE Transactions on Intelligent Transportation Systems, 23(10), 19727-19742.

[9] Dakić, P. (2024). IMPORTANCE OF KNOWLEDGE MANAGEMENT FOR CI/CD AND SECURITY IN AUTONOMOUS VEHICLES SYSTEMS. Journal of Information Technology & Applications, 14(1).

[10] Zhi, P., Zhao, R., Zhou, H., Zhou, Y., Ling, N., & Zhou, Q. (2021). Analysis on the development status of intelligent and connected vehicle test site. Intelligent and Converged Networks, 2(4), 320-333.

[11] Guan, T., Han, Y., Kang, N., Tang, N., Chen, X., & Wang, S. (2022). An overview of vehicular cybersecurity for intelligent connected vehicles. Sustainability, 14(9), 5211.

[12] Khan, S. K., Shiwakoti, N., Stasinopoulos, P., & Warren, M. (2023). Modelling cybersecurity regulations for automated vehicles. Accident Analysis & Prevention, 186, 107054.

[13] Cao, J., Lin, L., Zhang, J., Zhang, L., Wang, Y., & Wang, J. (2021). The development and validation of the perceived safety of intelligent connected vehicles scale. Accident Analysis & Prevention, 154, 106092.

[14] Anbalagan, S., Raja, G., Gurumoorthy, S., Suresh, R. D., & Dev, K. (2023). IIDS: Intelligent intrusion detection system for sustainable development in autonomous vehicles. IEEE Transactions on Intelligent Transportation Systems, 24(12), 15866-15875.

[15] Sousa, B., Magaia, N., & Silva, S. (2023). An intelligent intrusion detection system for 5g-enabled internet of vehicles. Electronics, 12(8), 1757.

[16] Cheng, P., Han, M., Li, A., & Zhang, F. (2022). STC-IDS: Spatial–temporal correlation feature analyzing based intrusion detection system for intelligent connected vehicles. International Journal of Intelligent Systems, 37(11), 9532-9561.

[17] Alladi, T., Kohli, V., Chamola, V., Yu, F. R., & Guizani, M. (2021). Artificial intelligence (AI)-empowered intrusion detection architecture for the internet of vehicles. IEEE Wireless Communications, 28(3), 144-149.

[18] Yu, T., Hua, G., Wang, H., Yang, J., & Hu, J. (2022, May). Federated-lstm based network intrusion detection method for intelligent connected vehicles. In ICC 2022-IEEE International Conference on Communications (pp. 4324-4329). IEEE.

[19] Pascale, F., Adinolfi, E. A., Coppola, S., & Santonicola, E. (2021). Cybersecurity in automotive: An intrusion detection system in connected vehicles. Electronics, 10(15), 1765.

[20] Ge, X., Han, Q. L., Wu, Q., & Zhang, X. M. (2022). Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks. IEEE/CAA Journal of Automatica Sinica, 10(5), 1234-1251.

[21] Park, S., & Park, H. (2024). PIER: cyber-resilient risk assessment model for connected and autonomous vehicles. Wireless Networks, 30(5), 4591-4605.

[22] Ahmed, I., Jeon, G., & Ahmad, A. (2021). Deep learning-based intrusion detection system for internet of vehicles. IEEE Consumer Electronics Magazine, 12(1), 117-123.

[23] Li, X., Hu, Z., Xu, M., Wang, Y., & Ma, J. (2021). Transfer learning based intrusion detection scheme for Internet of vehicles. Information Sciences, 547, 119-135.

[24] Yang, L., Moubayed, A., & Shami, A. (2021). MTH-IDS: A multitiered hybrid intrusion detection system for internet of vehicles. IEEE Internet of Things Journal, 9(1), 616-632.

[25] Alladi, T., Kohli, V., Chamola, V., & Yu, F. R. (2023). A deep learning based misbehavior classification scheme for intrusion detection in cooperative intelligent transportation systems. Digital Communications and Networks, 9(5), 1113-1122.

[26] Madhu, G., Lalith Bharadwaj, B., Sai Vardhan, K., & Naga Chandrika, G. (2020). A normalized mean algorithm for imputation of missing data values in medical databases. In Innovations in Electronics and Communication Engineering: Proceedings of the 8th ICIECE 2019 (pp. 773-781). Springer Singapore.

[27] Dahiya, D. (2023). DDoS attacks detection in 5G networks: hybrid model with statistical and higher-order statistical features. Cybernetics and Systems, 54(6), 888-913.

[28] Piras, D., Peiris, H. V., Pontzen, A., Lucie-Smith, L., Guo, N., & Nord, B. (2023). A robust estimator of mutual information for deep learning interpretability. Machine Learning: Science and Technology, 4(2), 025006.

[29] Graf, R., Zeldovich, M., & Friedrich, S. (2024). Comparing linear discriminant analysis and supervised learning algorithms for binary classification—A method comparison study. Biometrical Journal, 66(1), 2200098.

[30] Park, S., Baek, H., Yoon, J. W., Lee, Y. K., & Kim, J. (2024). AQUA: Analytics-driven quantum neural network (QNN) user assistance for software validation. Future Generation Computer Systems.

[31] Donkol, A. A. E. B., Hafez, A. G., Hussein, A. I., & Mabrook, M. M. (2023). Optimization of intrusion detection using likely point PSO and enhanced LSTM-RNN hybrid technique in communication networks. IEEE Access, 11, 9469-9482.

[32] Alohali, M. A., Elsadig, M., Al-Wesabi, F. N., Al Duhayyim, M., Mustafa Hilal, A., & Motwakel, A. (2023). Enhanced chimp optimization-based feature selection with fuzzy logic-based intrusion detection system in cloud environment. Applied Sciences, 13(4), 2580.

[33] Yang, X. S., Karamanoglu, M., & He, X. (2014). Flower pollination algorithm: a novel approach for multiobjective optimization. Engineering optimization, 46(9), 1222-1237.

[34] Zhang, Z., He, H., & Deng, X. (2023). An FPGA-implemented antinoise fuzzy recurrent neural network for motion planning of redundant robot manipulators. IEEE transactions on neural networks and learning systems.

[35] Al-kahtani, M. S., Mehmood, Z., Sadad, T., Zada, I., Ali, G., & ElAffendi, M. (2023). Intrusion detection in the Internet of Things using fusion of GRU-LSTM deep learning model. Intelligent Automation & Soft Computing, 37(2).

[36] Zhang, J., Zhang, X., Liu, Z., Fu, F., Jiao, Y., & Xu, F. (2023). A Network Intrusion Detection Model Based on BiLSTM with Multi-Head Attention Mechanism. Electronics, 12(19), 4170.