Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 45 No. 04 (2024)

Attack Detection and enhanced Data Security Using Quantile Regressive Extreme Learning Machine and Contextual Cryptosystem in Wireless Networks

[1]Dhivya. R, [2]Dr. B. Srinivasan
[1]PHD PART TIME,
DEPARTMENT OF COMPUTER SCIENCE,
GOBI ARTS & SCIENCE COLLEGE, KARATTATIPALAYAM, GOBICHETTIPALAYM, ERODE(DT).
[2]ASSOCIATE PROFESSOR,
DEPARTMENT OF COMPUTER SCIENCE,
GOBI ARTS & SCIENCE COLLEGE ,.KARATTATIPALAYAM,
GOBICHETTIPALAYM,
ERODE(DT).

Abstract

Wireless networks enable devices to communicate and share data without the need for physical connections, such as cables or wires. The increasing usage of computer networks raises additional cybersecurity concerns, necessitating the implementation of preventive measures to protect valuable data. Intrusion Detection Systems (IDS) are essential components of network security, designed to monitor computer networks and systems for suspicious activities, unauthorized access, or potential attacks. The key functions of IDS include collecting, analyzing, and identifying abnormal behavior within the system, as well as responding to potential threats. Secure data transmission in wireless networks is a vital aspect for cryptographic techniques-based intrusion detection systems (IDS). To enhance attack detection accuracy, a novel method called the Quantile Regressive Extreme Learning Machine based Contextual Naccache–Stern (QRELM-CNSC) has been developed for wireless networks. QRELM-CNSC includes two major processes such as classification and secure data transmission within the wireless network. First, the Quantile Regressive Sequential Extreme Learning Machine classifier is employed for efficient attack detection in wireless networks and achieving higher accuracy. In the Extreme Learning Machine classifier, a number of data samples and their features are considered as input at the input layer. In Hidden Layer 1, Camargo's Index Targeted Projection Pursuit model is applied to select significant features from the dataset. With the selected features, Quantile Regression is applied in Hidden Layer 2 to analyze the data samples. Finally, the data samples are classified as normal or attack nodes (i.e., Fuzzers, Analysis nodes, Backdoors, DoS nodes, and Exploit nodes) in the output layer. Subsequently, sensitive normal data samples are transmitted securely using the Pseudo Randomized Contextual Naccache–Stern Cryptosystem. The proposed cryptosystem consists of three processes namely contextual key generation, encryption, and decryption. In the key generation process, both contextual public and private keys are generated. After key generation, the sender encrypts the data using the receiver's public key and transmits it to the receiver. The authorized receiver then decrypts the ciphertext to obtain the original data. This process ensures secure data transmission, enhancing data confidentiality in wireless networks. Experimental evaluations are conducted on various factors, such as attack detection accuracy, precision, recall, F-measure, data confidentiality rate, and attack detection time, concerning different numbers of data samples. The performance analysis results indicate that the proposed QRELM-CNSC method achieves better attack detection accuracy, precision, recall, and data confidentiality while minimizing time consumption

Keywords: Wireless network, Attack Detection**,** Data Security**,** Sequential Extreme Learning Machine classifier, Quantile Regression, Pseudo Randomized Contextual Naccache–Stern Cryptosystem.

1. Introduction

Intrusion detection in wireless network communication is a critical aspect of maintaining network security. Due to the open and dynamic nature of wireless networks, they are particularly vulnerable to various types of attacks, such as eavesdropping, spoofing, Denial of Service (DoS), and man-in-the-middle attacks. Intrusion Detection Systems (IDS) are designed to monitor network traffic and detect abnormal activities that indicate a security violation.

A Blockchain-based African Buffalo with Recurrent Neural Network (BbAB-RNN) model was developed in [1] with the aim of detecting intrusions and enhancing security. The model improves accuracy, precision, recall, F1-score, and detection rate. However, it also faces challenges related to higher time complexity, which impact security performance. The Whale with Cuckoo Search Optimization-based Quantum Neural Network (WCSO-QNN) combined with Elliptic Curve Cryptography (ECC) was developed in [2] to accurately detect attacks and ensure data protection by selecting significant features. However, the processing time of the QNN was higher.

A Random Forest model was designed in [3] with differential privacy to detect network attacks and perform classification. But, it failed to enhance the framework's applicability across different feature spaces and entities. A robust learning approach was developed in [4] for predicting and detecting hybrid attacks in IoT networks by integrating deep neural networks and ensemble techniques to improve the detection accuracy of hybrid attack patterns. But, a cryptographic technique was not employed to enhance data confidentiality. A hierarchical machine learning-based hyperparameter optimization algorithm was designed in [5] for classifying intrusions through the feature selection. But it failed to apply the deep learning models to improve attack detection accuracy. A novel defense system was designed in [6] to protect attacks by utilizing diverse set of classifiers to identify intrusions. But, it failed to provide robust security protection during data transmission. A novel deep learning model called the Cybernet model was designed in [7] to detect the behaviors of cyber attacks with high accuracy. But, it failed to detect different types of attacks in minimal time. A distributed framework was developed in [8] based on deep learning (DL) to detect various types of cyber attacks. However, attack detection complexity posed a significant challenge. An Adaptive Federated Learning Approach was introduced in [9] to detect DDoS attacks, significantly reducing convergence time and enhancing classification accuracy. But, the feature selection process in attack detection remained unaddressed.

An encrypted two-tier control model was developed in [10] that combine machine learning (ML) for cyberattack detection to enhance operational safety and cybersecurity. However, it did not apply deep learning models to further improve attack detection. To enhance attack detection accuracy, a Deep Reinforcement Learning (DRL) model was designed in [11]. However, it failed to facilitate collaborative efforts between cybersecurity experts and the machine learning model to address the multifaceted challenges at the integration of DRL and cybersecurity. A new collaborative learning approach was designed in [12] using a blockchain network for cyberattack detection while also mitigating the risk of exposing local data privacy. But, it did not utilize more effective methods to enhance the protection of local data privacy. A correlation-aware architecture with a neural network model was designed in [13] for DDoS attack detection. But, it failed to implement complex detection architectures using a collaborative method for dynamically training and updating the system for detecting DDoS attacks over time. A new two-stage deep learning model was designed in [14] by integrating Long Short-Term Memory (LSTM) and Autoencoders (AE) for detecting cyber attacks. However, it failed to select essential features while ignoring irrelevant ones which limiting the performance of attack detection. An intelligent hybrid model was designed in [15] that integrate machine learning and artificial intelligence to enhance network security by identifying

and preventing cyberattacks. The model utilizes feature reduction techniques to improve performance and minimize time complexity. But, the scalability of the algorithm for larger wireless sensor networks (WSNs) was not addressed.

1.1 contributions

The new contributions of the QRELM-CNSC is summarized as follows,

- To enhance attack detection accuracy, the QRELM-CNSC has been developed, incorporating Quantile Regressive Sequential Extreme Learning Machine classifier. The Quantile regression analyzes the data samples and provides the normal or different kinds of attack samples.
- To minimize the attack detection time, Camargo's Index Targeted Projection Pursuit model is employed in Extreme Learning Machine classifier for selecting the significant features and removing the others.
- To enhance data confidentiality, a Pseudo Randomized Contextual Naccache–Stern Cryptosystem has been designed for secure data transmission and to protect sensitive data.
- Finally, an experimental assessment is conducted to evaluate the performance of the QRELM-CNSC using various metrics and comparing it to other methods.

1.1 paper organization

The paper is organized as follows: Section 2 reviews related works, Section 3 describes the QRELM-CNSC in detail, Section 4 outlines the experimental setup and dataset description, Section 5 provides a comparative analysis of various metrics using different methods, and finally, Section 6 presents the overall conclusion of the work.

2. Related works

An enhanced approach was designed in [16] for detecting DDoS attacks using an ensemble-based Random Forest classifier and feature selection. But, the approach did not effectively address significantly higher and rapidly changing network conditions**.** A Fully Streaming Big Data Framework was developed in [17] using optimized deep learning for cybersecurity to enhance efficiency and stability. But, it failed to improve accuracy and information security, particularly in protecting sensitive customer information also critical. A Secure Federated Intrusion Detection Model was designed in [18] to classify attacks as either normal or an attack type with high precision. However, it failed to address a novel and greater number of network attack classes. A deep learning-based novel method was developed in [19] to detect cybersecurity vulnerabilities and enhance the confidentiality and integrity of users and systems sensitive information. However, the designed system failed to detect internal and external intruders and their malicious behaviors. An Improved Mayfly Optimization combined with a Hybrid Deep Learning model was designed in [20] to detect intrusions. But, it failed to maintain high accuracy in identifying cyberattacks under varying conditions and data distributions.

An Artificial Orca Algorithm with Ensemble Learning model was designed in [21] for cyberattack detection and classification with higher accuracy. However, it failed to ensure the protection of data exchanges and the development of privacy-preserving systems. A lightweight machine learning detection method based on a Decision Tree (DT) algorithm was developed in [22], utilizing the Gini method to select significant features. However, this method did not significantly improve attack detection accuracy. In [23], Machine Learning algorithms were designed to detect the network attack and cyber-security attacks with low false alarm rates. Numerous deep learning models were developed in [24] to detect cyberattacks on a collection of network traffic streams. However, high time complexity of attack detection remains a significant challenge. To minimize time complexity, a reliable feature selection model was designed in [25]. But, deep learning models were not implemented for multi-class classification in cyber attack detection. A Hybrid Convolutional Neural Network was developed in [26] to identify IoT attacks through feature selection and classification. But, it did not focus on analyzing unsupervised machine learning models to examine unidentified traffic

A blockchain-assisted hybrid metaheuristic model combined with machine learning was designed in [27] for cyber attack detection and classification, aiming to achieve better accuracy. However, privacy-preserving

methods were not implemented to protect sensitive information during cyber attack detection. To enhance data security, an Improved Elliptic Curve Cryptography algorithm combined with deep LSTM was designed in [28] for attack detection during data transfer. Hybrid deep learning models were designed in [29] to detect all types of DDoS attacks with high accuracy. However, it failed to incorporate feature selection to further enhance attack detection. An integration of two convolutional neural networks (CNN-CNN) was developed in [30] for detecting attacks on IoT networks by selecting significant features. However, these methods also pose challenges, including increased complexity and resource requirements.

3. Proposal methodology

Cybersecurity in wireless networks is a significant aspect of modern communication systems and are more susceptible to security threats due to their open and easily accessible nature. As computer networks continue to expand in size and complexity, the need for robust security measures becomes increasingly vital. Intrusion Detection Systems (IDS) have been designed to tackle this challenge by monitoring network and identifying potential security threats. These systems are capable of analyzing traffic to detect risks such as malware, network intrusions, and denial of service attacks. However, the growing complexity and variety of network traffic have made it challenging for traditional intrusion detection system. In this paper, a novel method called a novel RELM-CNSC Method is developed for enhancing the cyber attack detection.

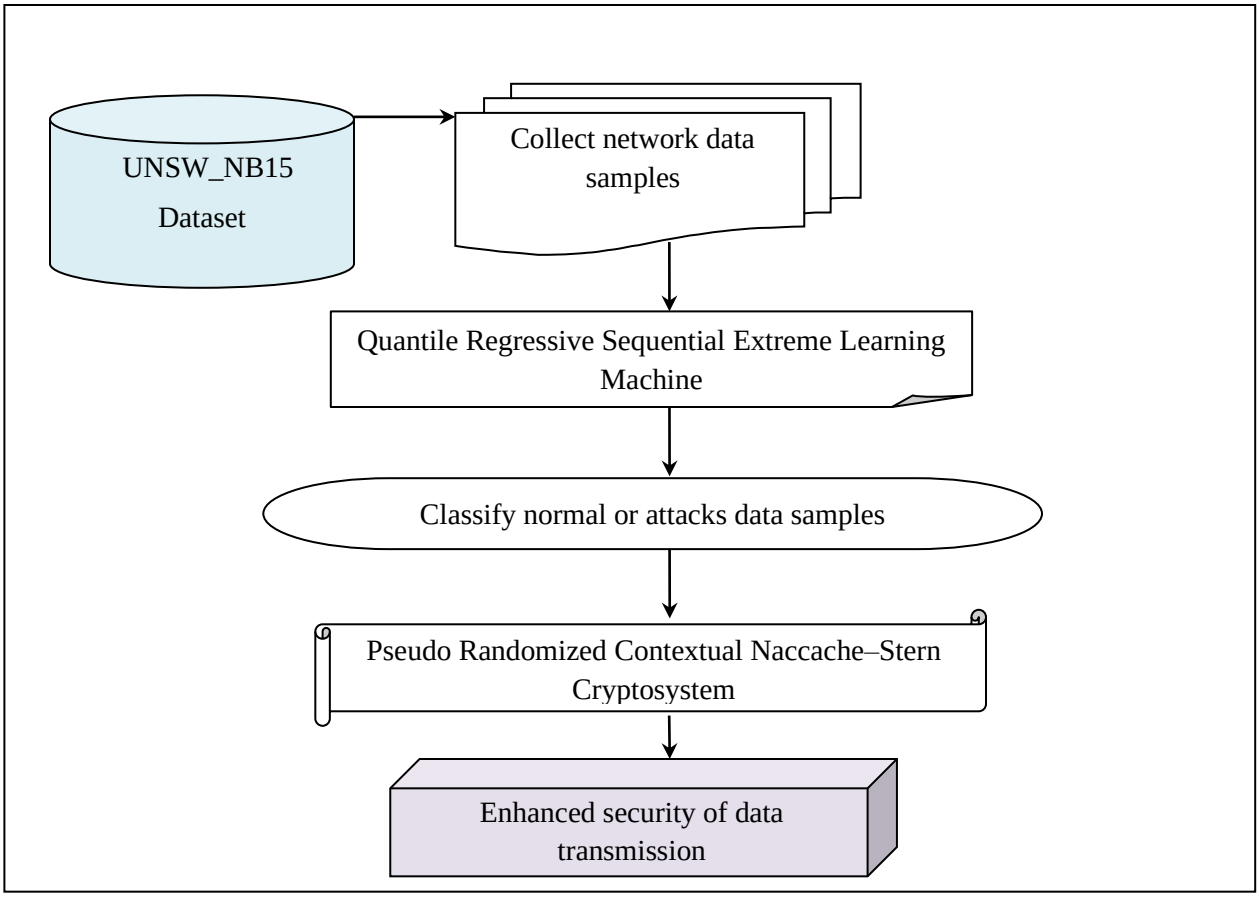

Figure 1 architecture of proposed QRELM-CNSC

Figure 1 given above illustrates the architecture diagram of the proposed QRELM-CNSC for accurate classification of attack and secure data transmission in wireless network. The proposed QRELM-CNSC includes a different processes namely data acquisition, classification and secure data communication. These three different processes of the proposed QRELM-CNSC are described in the following sections.

3.1 Data acquisition

Data acquisition refers to the process of collecting the information from various sources dataset for further analysis, processing, and storage. In order to collect the data samples for secure data transmission, the proposed method utilizes the UNSW_NB15 Dataset taken from Kaggle https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15. This UNSW_NB15 Dataset is employed for classifying the normal and potential attacks within the network. The dataset contains 175,341 data samples with 45 features or attributes. The final two columns indicate the attack category and label for each sample. Each record is classified as either normal or indicative of an attack.

3.2 Quantile regressive sequential Extreme learing machine classifier

After the data acquisition, the attack detection process is carried out in the proposed QRELM-CNSC in the wireless network using Quantile regressive sequential Extreme learing machine. The Extreme Learning Machine (ELM) is a type of feed-forward neural network prominent for its extremely fast learning speed and better generalization ability. This ELM leads to faster training and improved performance. The Sequential Extreme Learning Machine (SELM) offers significant benefits, particularly in real-time learning and managing large-scale data streams, as it processes incoming data sequentially. Therefore, the proposed approach employs the Extreme learing machine classifier to enhance classification accuracy of normal or attack.

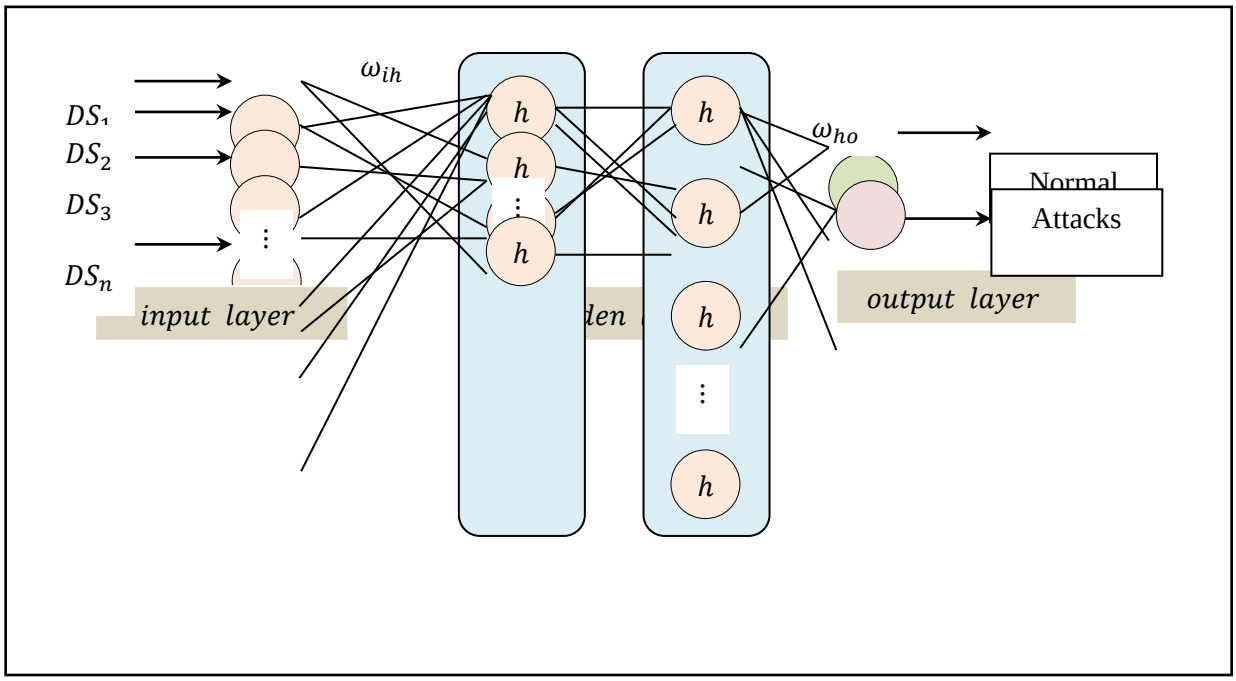

Figure 2 structural design of Sequential Extreme Learning Machine

neural network for classifying the data samples with multiple layers of hidden nodes 'h'. The proposed classifier included the three different layers such as input layer, hidden layers and output layer. As shown in the above figure 2, let us consider that the training set $\{DS, Y\}$ where 'DS' denotes a training data samples $\{DS_1, DS_2, DS_3, \ldots., DS_n\}$ and an output 'Y' representing classification output $Y_k \in Y_1$,. The input layer collects the

data samples and transmits it to the hidden layer. Finally, the output layer provides the better classification results. Three layers in the structure are connected in a feed-forward manner with variable weights. The computation process is performed in hidden layer. Each layer comprised the artificial neurons to transfer the input training data samples from one layer to the neurons in next consecutive layer.

The input weights are fixed with straightforward solution that not requires different iteration process. It is expressed as follows,

$$X(t) = \sum_{i=1}^{n} [DS_i(t) * w_i] + B \quad (1)$$

Where, '$X(t)$' represents the input layer 'w' symbolizes the weight between input layer neuron and hidden layer neuron and bias function 'B', 'DS' symbolizes the training data samples. The input data samples sent into hidden layer where feature selection and classification process is carried out.

In the hidden layer 1, Feature selection is a fundamental step aimed at selecting the most relevant and informative features from a dataset using Camargo's index Targeted Projection Pursuit. Its main objective is to improve model performance while reducing the dimensionality of the data.

Targeted Projection Pursuit is statistical technique mainly used for data analysis, and feature selection in high-dimensional datasets. It allows analysts to extract meaningful features and patterns from dataset with numerous attributes, facilitating interpretation and decision-making. In Targeted Projection Pursuit (TPP), the main aim is to find a projection from a high-dimensional space to a lower-dimensional space that maximizes an objective function to a specific target. The Camargo's index is a statistical method to measure the dependency between features formulated as follows,

$$C = 1 - \sum_{j=1}^{m} \frac{|NF_j - NF_k|}{m} \quad (2)$$

Where, C indicates an output of Camargo's index', NF_j and NF_k denotes a features in the dataset, m indicates a number of features. The Camargo's index function outputs values ranging from 0 to 1. The objective is to maximize this index to find projections or feature pairs that are highly dependent or similar. This is expressed as follows,

$$Z = arg\ max\ C \quad (3)$$

Where, Z denotes a targeted projection function between two feature vectors NF_j and NF_k , $arg\ max$ indicates a argument of maximum faction. This method aims to project the significant relevant target feature sets with maximum Camargo's index function contribute to specific patterns or dependencies in the dataset.

These target feature set are given as input to the next hidden layer for classifying the normal or attack samples such as Fuzzers node, Analysis nodes, Backdoors, DoS nodes and Exploit nodes.

The Quantile regression is employed for analyzing the extracted samples with selected features. The Quantile regression is a machine learning technique used for analyzing the relationship between the dependent variable (outcome) and independent variables (data samples). The relationship between the outcome and the data samples are formulated as follows,

$$Q(DS|Y) = \beta_0 + \beta_1\, DS_1 + \beta_2\, DS_2 + \cdots .. + \beta_n\, DS_n \ (4)$$

Where, $Q(DS|Y)$ denotes a Quantile regression, DS denotes a data samples, $\beta_0, \beta_1, \beta_2 \ldots \beta_n$ denotes a regression coefficient. Followed by, the objective function of the regression coefficient is formulated as follows,

$$\beta_Q = \arg\min[Y - Q(DS|Y)] (5)$$

Where, the coefficient of Quantile regression 'β_Q' minimizes the loss function Y denotes a actual output, $Q(DS|Y)$ denotes a observed output. The hidden layer output is expressed as follows,

$$H(t) = \sum_{i=1}^{n} w_{ij}\ \ \sigma\,(w_{jk}\ \ Q(DS|Y) + \ B_h) \qquad (6)$$

From (2), '$H(t)$' symbolizes the output result of the hidden layer, 'σ' indicates the sigmoid activation function, 'w_{jk}' indicates the weight between'j^{th}' hidden layer neuron and 'k^{th}' output layer neuron, 'w_{ij}' denotes

'i^{th}' input layer neuron and 'j^{th}' hidden layer neuron, $Q(DS|Y)$ Quantile regression outcomes, B_h denotes a bias at hidden layer. The output of the hidden layer is fed into the final output layer, where the sigmoid activation function is applied to provide the binary classification results.

$$Z = \sigma(w_k * H(t)) \quad (7)$$

Where 'Z' indicates the final classification result, σ indicates a sigmoid activation function, 'w_k' denotes the weight of the output layer, $H(t)$ denotes output of the hidden layer.

$$\sigma = \begin{cases} 1 & ; \quad attack \\ 0 ; & \quad normal \end{cases} \quad (8)$$

The sigmoid activation function returns '1' when the data samples are classified as attacks and '0' when the data samples are classified as normal. Finally, accurate data classification results are achieved at the output layer with minimal time complexity. Quantile regressive sequential Extreme learning machine classifier algorithm is explained below

Algorithm1: Quantile regressive sequential Extreme learning machine classifier

Input: Dataset 'D', network features $NF_1, NF_2, NF_3, \dots NF_n$, Number of samples $Ds_1, Ds_2, Ds_3, \dots Ds_m$
Output: increase attack detection accuracy

Begin
Collect the number of data samples $Ds_1, Ds_2, Ds_3, \dots Ds_m$ at an input layer
For each data Ds_i
Randomly assign weight and bias using (1)
End for
For each network features NF -- **hidden layer 1**
Measure the Camargo's index similarity 'C' using (2)
End for
End for
If $(arg\ max\ C)$ **then**
Features are selected as relevant
else
Features are selected as irrelevant
End if
For each selected feature with data samples Ds
Perform regression analysis using (4)
End for
Apply the sigmoid activation function
if $(\sigma = +1)$ **then**
Data samples is classified as 'attack'
else
Data samples is classified as 'normal'
End if
Return (classifications results)-- **output layer**
End for
End

Algorithm 1 outlines the process of the Quantile Regressive Sequential Extreme Learning Machine classifier, which is designed to achieve higher classification accuracy with lower time complexity. Initially, the algorithm collects the training data samples and transfers them into the input layer. Weights and biases are assigned

randomly. The data samples are then transferred to the hidden layer, where feature selection is applied to measure the similarity between features. Based on Camargo's Index similarity, relevant sets of features are extracted from the dataset. The selected features, along with the data samples, are then provided to the next hidden layer, where classification is performed by applying the regression function. The sigmoid activation function is used to classify the data samples as attacks or normal. Finally, accurate classification is achieved with minimal time consumption.

3.3 Pseudo Randomized Contextual Naccache–Stern Cryptosystem

For data samples classified as normal, the proposed QRELM-CNSC performs secured data transmission using Pseudo Randomized Contextual Naccache–Stern Cryptosystem. Since the data is legitimate, encryption methods is employed to ensure efficient and secure transmission. The Naccache–Stern cryptosystem is a homomorphic public-key cryptosystem also known as asymmetric cryptography that utilizes a pair of keys such as private and public key for secure communication. The private key is kept secret by the owner and is used to decrypt data, while the public key is shared openly and it used by everyone to encrypt data. This enhances the confidentiality of data transmission from sender to receiver by The Naccache–Stern Cryptosystem includes three processes, namely key generation, encryption, and decryption.

3.3.1 Contextual keys generation

Key generation is a crucial process in cryptography that involves creating cryptographic keys for use in encryption and decryption. During the key generation process, Blum Blum Shub pseudorandom number generator is generated for Contextual keys such as private and public key for encrypting all messages in one communication session. If the session is finished, it automatically disabled to ensure security. Contextual key generation suggests a method of generating cryptographic keys based on specific contextual information such as session-specific data.

Let us consider a set of distinct prime numbers $p_1, p_2, p_3, \dots p_k$ and it divides into two groups

$$a = \prod_{i=1}^{k/2} p_i \quad (9)$$

$$b = \prod_{k/2+1}^{k} p_i \quad (10)$$

Compute the τ which is the product of the a and b

$$\tau = a * b \quad (11)$$

Followed by selecting the two large prim numbers x and y calculate the followings,

$$u = 1 + 2xa \ (12)$$

$$v = 1 + 2yb (13)$$

Therefore, the private key is generated as follows,

$$K_r = (u, v) \quad (14)$$

$$K_b = (\tau, N, G) \quad (15)$$

$$N = u * v \quad (16)$$

Where, K_b denotes a public key, G denotes a random number generated using Blum Blum Shub pseudorandom number generator. Consider two distinct prime integers c and d, the random number is generated as follows,

$$G = {x_0}^2 \ mod \ P \ (17)$$

$$P = c \ d (18)$$

Where, x_0 denotes an initial value that starts the process of generating random numbers. In this way, the keys are generated for secure data transmission.

3.3.2 Data encryption

Upon successful key generation, the sender proceeds with data encryption, a process used to transform the original data (plaintext) into an unreadable format known as ciphertext. This ensures that the sensitive information within the data is hidden, making it unintelligible to unauthorized entities thus ensuring the confidentiality and integrity of the data.

Let us consider the random number 'R' and perform the encryption as given below,

$$En(Ds) = R^{\tau} G^{Ds} \, mod \, N \quad (19)$$

Where, $E(Dp)$ denotes an encrypted data packet (i.e. ciphertext), τ is the product of a and b, G denotes a random generator, Ds denotes a data samples, M denotes a product two large prime numbers $u \, and \, v$. Finally, the sender node sends the encrypted data samples to the receiver in the form of ciphertext to avoid unauthorized access.

3.3.3 Data decryption

In cryptographic system, the decryption process is the reverse of encryption. The main aim is to convert the ciphertext (the encrypted data) back into its original form, known as plaintext.

$$Ds_i = Ds \, mod \, p_i \quad (20)$$

From (13), the original data sample 'Ds_i' is obtained at the receiver end. Finally, the plain text is received in a secure manner. In this way, the secure data transmission from sender to receiver is effectively performed to enhance the data confidentiality. The algorithmic process of Pseudo Randomized Contextual Naccache–Stern Cryptosystem is clearly described as given below,

// Algorithm 2: Pseudo Randomized Contextual Naccache–Stern Cryptosystem

Input: Number of normal data samples $Ds_1, Ds_2, Ds_3 \ldots Ds_k$,
Output: Increase the data confidentiality

Begin
// key generation
For each Ds_i transmission
Generate Contextual keys using (14) (15)
End for
// **Encryption**
Sender transmit Ds to receiver
Sender Encrypt the data '$En(Ds)$' using (19)
Obtain the ciphertext
Send to receiver 'R'
// **Decryption**
If the receiver is an authentic node **then**
Decrypt the data with the private key using (20)
Obtain the original 'Ds'
End if
End

Algorithm 2 describes a Pseudo Randomized Contextual Naccache–Stern Cryptosystem designed to enhance secure data transmission from the sender to the receiver in wireless networks. First, the Pseudo Randomized Contextual key generation process is employed to generate the private and public keys for secure data transmission. Following this, the sender performs encryption using the receiver's public key and sends the data samples in the form of ciphertext. The authorized receiver then performs decryption to obtain the original text. This process achieves a higher level of security in wireless networks during data transmission.

4. Experimental setup

Experimental evaluations of the proposed QRELM-CNSC method and existing methods, namely BbAB-RNN [1] and WCSO-QNN and ECC [2] are implemented using python language and UNSW_NB15 Dataset from Kaggle https://www.kaggle.com/datasets/mrwellsdavid/unsw-nb15. To conduct the experiment, the UNSW_NB15 dataset is utilized to distinguish between normal activities and potential attacks. This dataset comprises various CSV

files, with the training.csv files selected for experimentation. The CSV files contain 175,341 records or data samples, encompassing 45 features or attributes. The last two columns in the dataset denote the attack category and label for each data sample. Each row is categorized and labeled as either a normal record or indicative of an attack. Before proceeding with data classification, significant features are selected to reduce complexity..

5. Performance Results and Comparisons

In this section, performance analysis of the proposed QRELM-CNSC method and existing methods, namely BbAB-RNN [1] and WCSO-QNN and ECC [2] are analyzed using various parameters, including attack detection accuracy, precision, recall, measure, data confidentiality rate and attack detection time. The performance results are presented through tabular data and graphical representations for comparison.

Attack detection accuracy: It is referred to as ratio of the number of data samples that are correctly classified as attacks or normal to the total number of data samples. It is measured as follows,

$$ADA = \left(\frac{T_p + T_n}{T_p + F_p + T_n + F_n}\right) * 100 \qquad (21)$$

Where ADA denotes a attack detection accuracy, T_p indicates a true positive, F_p denotes a false positive, T_n indicates the true negative, F_n represents the false negative. The accuracy is measured in terms of percentage (%).

Precision: it is a metric used to evaluate the performance of a attack detection in binary classification tasks. It is mathematically computed as follows,

$$PC = \left(\frac{T_p}{T_p + F_p}\right) \qquad (22)$$

Where PC denotes a precision, T_p indicates a true positive, F_p denotes a false positive.

Recall, also known as sensitivity, is used to assess the performance of a classification model. It measures the proportion of true positive predictions out of all actual true positives and false negatives.

$$RL = \left(\frac{T_p}{T_p + F_n}\right) \qquad (23)$$

Where RL denotes a recall, T_p indicates a true positive, F_n denotes a false negative

F- measure: It is also called as F1 score that combines precision and recall into a single value to provide a balanced evaluation of a model's performance. It is the harmonic mean of precision and recall.

$$F\ M = 2 * \left(\frac{PC * RL}{PC + RL}\right) \quad (24)$$

Where, $F\ M$ denotes a F- measure, PC denotes a precision, RL denotes a recall

Attack detection time: It is measured as the amount of time taken by algorithm for attack detection. It is calculated as follows,

$$ADT = \sum_{i=1}^{n} Ds_i * TM\ [CDs] \qquad (25)$$

Where, ADT indicates the attack detection time, $TM\ [CDS]$ indicates a time for classifying single data samples 'Ds'. The overall time is measured in terms of milliseconds (ms).

Data confidentiality rate: It is measured as the ratio of the number of data samples are preserved from the unauthorized access during the data transmission.

$$DCR = \sum_{i=1}^{n} \left(\frac{Preserved\ Ds_i}{Ds_i}\right) \quad (26)$$

Where, DCRdenotes a data confidentiality rate, $Preserved\ Ds_i$denotes a number of data samples preserved. Data confidentiality rate is measured in percentage (%).

Table 1 attack detection accuracy versus number of data samples

Number of data samples	Attack detection accuracy (%)		
	QRELM-CNSC	BbAB-RNN	WCSO-QNN and ECC
10000	95.5	91	89
20000	95.89	90.56	89.14
30000	96.56	91.05	88.05
40000	95.78	91.48	89.05
50000	95	91.89	89.45
60000	95.05	90.05	88.05
70000	96.45	91.36	89.74
80000	95.74	91.22	88.45
90000	96.78	90.45	89.05
100000	95.25	91.78	89.11

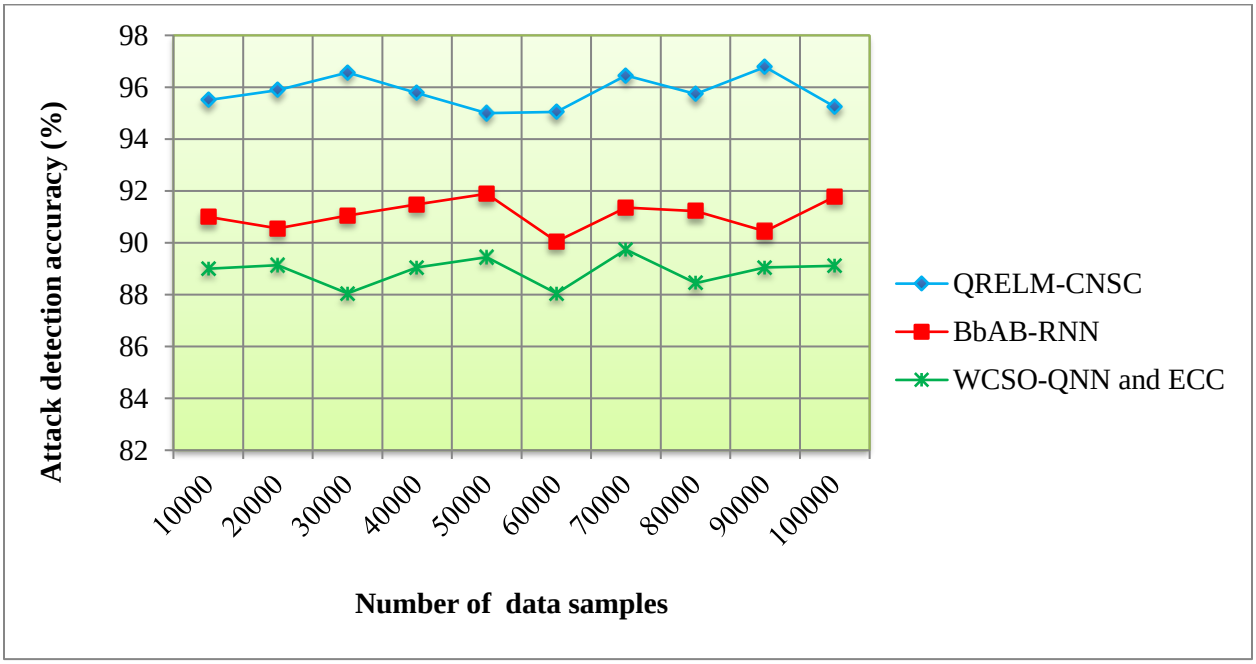

Figure 3 graphical results of attack detection accuracy

Figure 3 illustrates graphical results of attack detection accuracy versus the number of data samples, ranging from 10000 to 100000 collected from the dataset. The numbers of data samples are taken in horizontal axis and the accuracy was observed on the vertical axis. The graphically analyzed result illustrates that the accuracy of QRELM-CNSC was observed to be higher compared to existing methods BbAB-RNN [1] and WCSO-QNN and ECC [2]**.** Let us consider first iteration involving 10000 samples from dataset, the accuracy using the QRELM-CNSC model was found to be 95.5%. Subsequently, 91% and 89% of accuracy were observed by applying [1] and [2], respectively. Multiple runs were carried out for each method with various numbers of input data samples. The performance outcomes of QRELM-CNSC were compared to the results of existing methods. The overall comparison result indicates that the QRELM-CNSC model increased accuracy by 5% compared to [1] and 8% compared to [2]

by applying a respectively. This is due to the Quantile Regressive Sequential Extreme Learning Machine classifier, which aims to achieve higher classification accuracy. The Quantile Regression analyzes the data samples and applies the sigmoid activation function to classify them as either attacks or normal instances, resulting in enhanced accuracy.

Table 2 precision versus number of data samples

Number of data samples	Precision		
	QRELM-CNSC	BbAB-RNN	WCSO-QNN and ECC
10000	0.964	0.929	0.915
20000	0.963	0.925	0.907
30000	0.958	0.916	0.896
40000	0.948	0.928	0.905
50000	0.958	0.932	0.911
60000	0.957	0.922	0.905
70000	0.965	0.927	0.911
80000	0.955	0.915	0.906
90000	0.968	0.927	0.902
100000	0.961	0.924	0.911

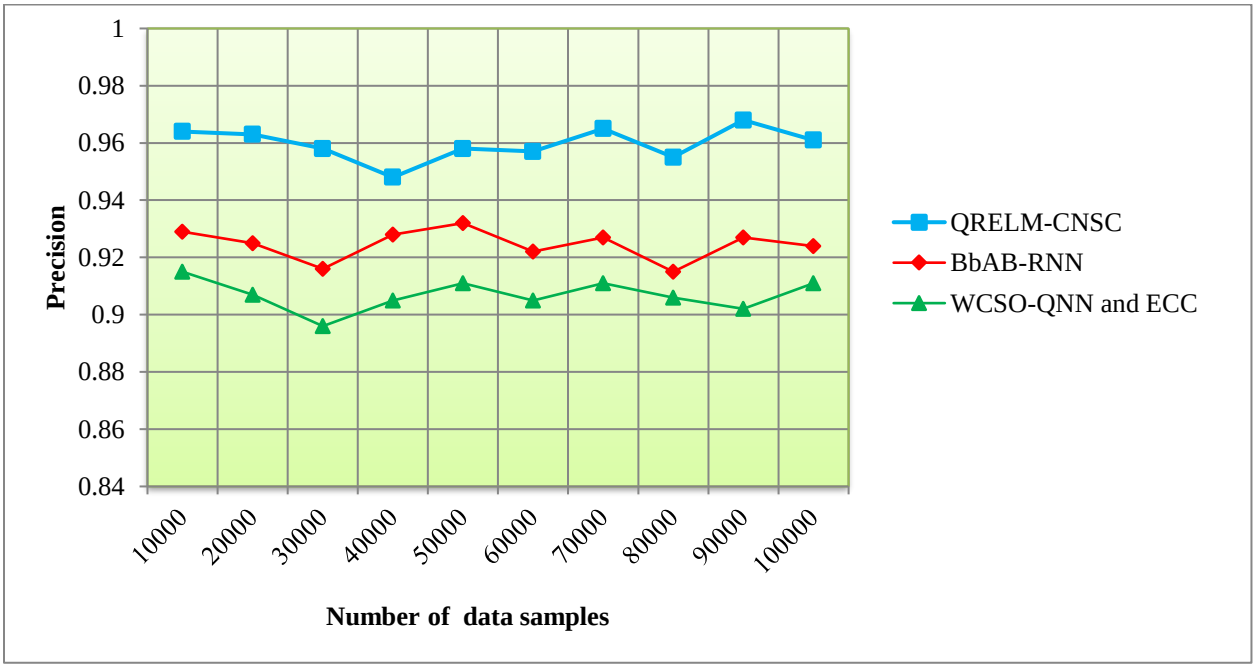

Figure 4 graphical results of precision

Figure 4 illustrates graphical results of precision in attack detection versus the number of data samples taken in the range from 10000 to 100000. The graph depicts the number of input samples on the 'x' axis and the precision performance observed on the 'y' axis. Among the three methods, QRELM-CNSC demonstrates the improved precision performance compared to the other two existing methods [1] [2]. This improvement is achieved due to the analysis of selected relevant features by applying the Quantile regression contribute to minimize false

positives and increase the true positives results. On average, the comparison of ten results reveals that the precision performance of QRELM-CNSC was increased by 4% compared to [1] and 6% compared to [2].

Table 3 recall versus number of data samples

Number of data samples	Recall		
	QRELM-CNSC	BbAB-RNN	WCSO-QNN and ECC
10000	0.971	0.942	0.928
20000	0.965	0.936	0.918
30000	0.974	0.933	0.914
40000	0.962	0.925	0.905
50000	0.957	0.928	0.907
60000	0.968	0.933	0.912
70000	0.963	0.924	0.907
80000	0.975	0.938	0.916
90000	0.978	0.941	0.924
100000	0.97	0.933	0.92

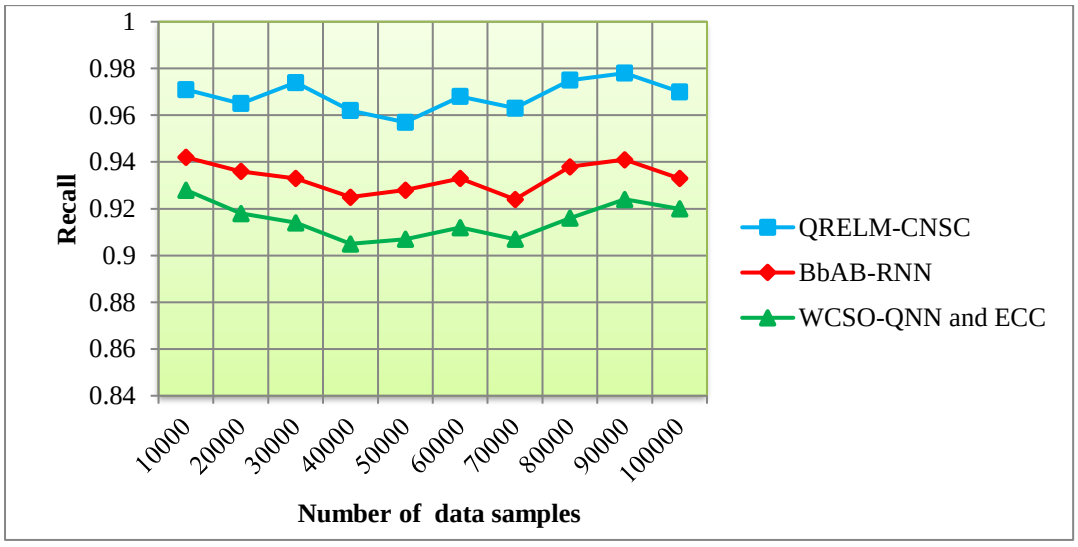

Figure 5 graphical results of recall

Figure 5 shows the graphical outcomes of recall against the number of data samples, ranging from 10000 to 100000 taken from two datasets. To calculate recall, three methods were employed namely QRELM-CNSC, the existing BbAB-RNN [1] and WCSO-QNN and ECC [2]. The horizontal axis indicates the number of data samples, while the vertical axis indicates recall. The experimental results demonstrate that the QRELM-CNSC achieved improved recall compared to the other two existing methods. For each method, a variety of results were observed with different counts of data samples. The observed results of the QRELM-CNSC were compared with the existing techniques. The overall comparison shows that the performance of recall using QRELM-CNSC in accurately predicting the attack detection is enhanced by 4% compared to [1] and 6% compared to [2] respectively. The extreme learning machine classifier employed in the QRELM-CNSC minimizes the false negative rates and increases true positive rate in classifying normal and attack.

Table 4 F measure versus number of data samples

Number of data samples	F measure		
	QRELM-CNSC	BbAB-RNN	WCSO-QNN and ECC
10000	0.967	0.935	0.921
20000	0.963	0.930	0.912
30000	0.965	0.924	0.904
40000	0.954	0.926	0.905
50000	0.957	0.93	0.909
60000	0.962	0.927	0.908
70000	0.963	0.925	0.909
80000	0.964	0.926	0.910
90000	0.972	0.933	0.912
100000	0.965	0.928	0.915

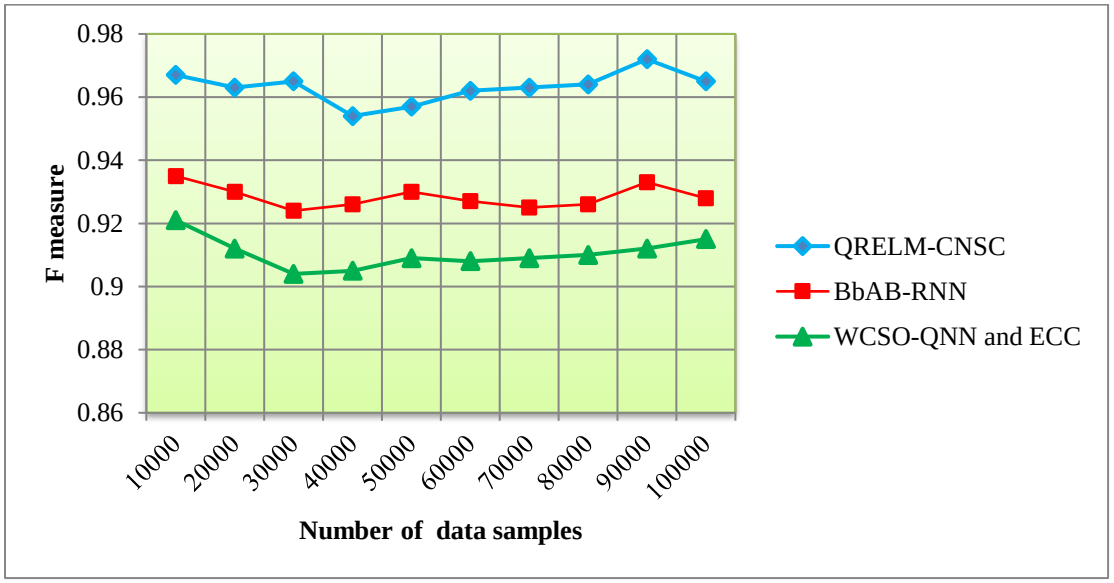

Figure 6 graphical results of F measure

Figures 6 demonstrate the performance outcomes of the F measure with respect to different number of data samples ranged from 10000 to 100000. According to the observed results, the proposed QRELM-CNSC demonstrated improved performance of F measure in attack detection compared to existing models. Ten outcomes were obtained for each method. The results of the QRELM-CNSC were then compared to existing methods. The average of the ten comparisons illustrates that the F measure using the QRELM-CNSC improved by 4% and 6% compared to [1] and [2], respectively. This is because of the QRELM-CNSC enhances the performance of the both precision and recall in the attack classification.

Table 5 attack detection time versus number of data samples

Number of data samples	Attack detection time (ms)		
	QRELM-CNSC	BbAB-RNN	WCSO-QNN and ECC
10000	36	48	57
20000	44	55.5	64.5
30000	56.9	66.5	72.4
40000	63	75.7	85.4
50000	75.8	88	93.6
60000	84	93.5	102
70000	95	107.3	118.6
80000	103.5	117.8	122.4
90000	117.5	125.6	130.5
100000	128.7	136.5	145.9

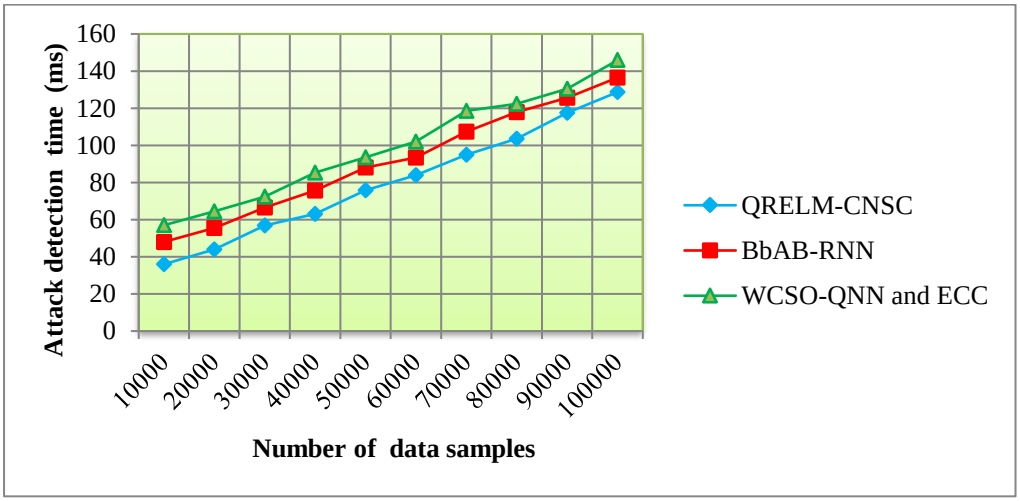

Figure 7 graphical results of attack detection time

Figure 7 depicts the performance of graphical illustration of attack detection time versus the number of data samples ranges from 10000 to 100000. The graphical results show that the attack detection time for all three methods gradually increases with the number of data samples. Specifically, the attack detection time for the QRELM-CNSC is considerably minimized compared to the existing methods [1] and [2]. In the first iteration with 10000 samples, the attack detection time for the QRELM-CNSC was found to be 36 ms, while the time consumption for [1] and [2] was 48 ms and 57 ms, respectively. The results obtained from the QRELM-CNSC were then compared to the existing methods. The average of ten comparison results shows that the attack detection time of the QRELM-CNSC is considerably minimized by 14% and 21% when compared to the existing methods [1] and [2]. This reduction is achieved through the application of Camargo's Index Targeted Projection Pursuit model, which selects significant features from the dataset. Using these selected features, attack detection is performed to minimize time consumption

Table 6 Data confidentiality rate versus number of data samples

Number of data samples	Data confidentiality rate (%)		
	QRELM-CNSC	BbAB-RNN	WCSO-QNN and ECC
10000	98.18	94.81	92.31
20000	97.89	94.56	91.05
30000	97.12	93.25	90.05
40000	98	93.45	91.65
50000	98.44	94.05	91.45
60000	97.32	93.23	91.06
70000	98.32	94.78	91.33
80000	97.05	93.65	91
90000	98.22	94.89	92.65
100000	97.56	93.56	91.47

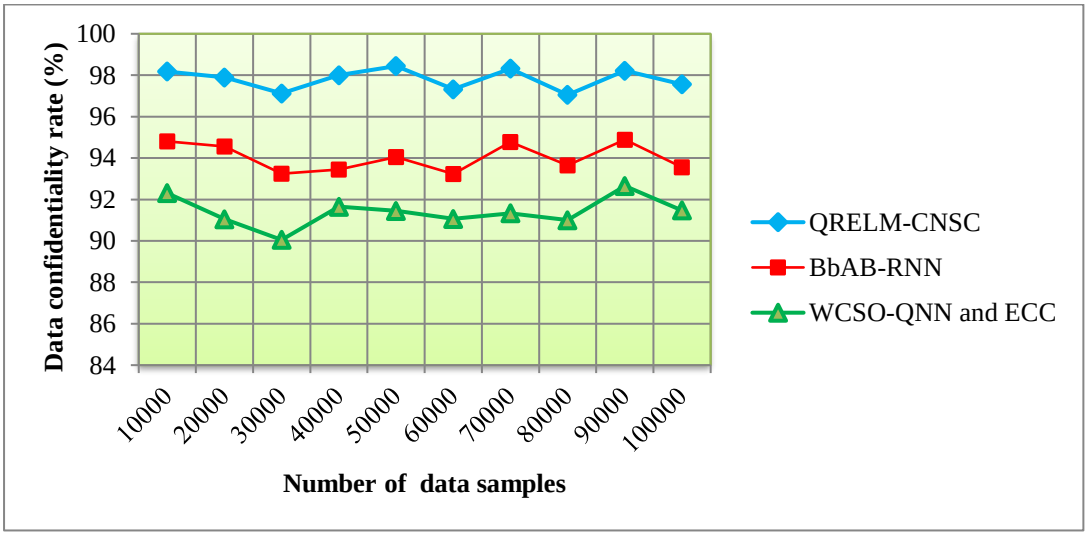

Figure 8 graphical results of data confidentiality rate

Figure 8 describe the results of the data confidentiality rate of three methods QRELM-CNSC, the existing BbAB-RNN [1] and WCSO-QNN and ECC [2] with respect to the number of data samples. In order to prove the efficiency of the proposed QRELM-CNSC, the comparison is performed with existing methods. During the experimental scenario, the number of data samples is considered in the ranges from 10000 to 100000. From the simulation conducted for 10000 samples and the data confidentiality rate of the QRELM-CNSC was found to be 98.18%. Similarly data confidentiality rate of existing [1] [2] was observed to be 94.81% and 92.31% using [1] [2] respectively. Ten results of data confidentiality rate are obtained and compared. The overall comparison result demonstrates that the accuracy of the QRELM-CNSC is higher than the other two related schemes. The average of ten results illustrates that the data confidentiality rate is increased by 4% and 7% using the QRELM-CNSC when compared to two related works [1] [2]. This statistical improvement is achieved by applying the Pseudo Randomized Contextual Naccache–Stern Cryptosystem to enhance secure data transmission in wireless networks. First, the Pseudo Randomized Contextual key generation process is employed to generate the private and public keys. Then, the encryption process is carried out, transmitting the data samples as ciphertext. The authorized entity

performs decryption to retrieve the original text. This process ensures a higher level of data confidentiality during transmission in wireless networks.

6. Conclusion

Secure data transfer is an essential requirement for Intrusion Detection Systems (IDS) in wireless networks due to their distributed and dynamic nature. Wireless networks rely on interconnected nodes to communicate, making them vulnerable to various security threats, including a variety of attacks. To address this issue, the proposed QRELM-CNSC model ensures accurate intrusion detection and data security in a wireless network environment. The Quantile Regressive Sequential Extreme Learning Machine classifier is employed for precise attack detection. The Camargo's Index Targeted Projection Pursuit model reduces attack detection time by selecting significant features from the dataset. Using these selected features, the Quantile Regression classifies data samples as either normal or attack. Sensitive normal data samples are then securely transmitted using the Pseudo Randomized Contextual Naccache–Stern Cryptosystem to achieve a higher data confidentiality rate. A comprehensive experimental assessment was conducted using various performance metrics, including attack detection accuracy, precision, recall, F-measure, attack detection time, and data confidentiality rate across different data samples. The results show that the proposed QRELM-CNSC significantly improves the accuracy of attack detection and data confidentiality rate, while reducing time consumption, compared to conventional methods.

References

[1] V. Saravanan, M Madiajagan, Shaik Mohammad Rafee, P Sanju, Tasneem Bano Rehman & Balachandra Pattanaik, “IoT-based blockchain intrusion detection using optimized recurrent neural network”, Multimedia Tools and Applications, Springer, Volume 83, 2024, Pages 31505–31526. https://doi.org/10.1007/s11042-023-16662-6

[2] Heba Kadry, Ahmed Farouk, Elnomery A. Zanaty, Omar Reyad, “Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security”, Alexandria Engineering Journal, Elsevier, Volume 71, 2023, Pages 491-500. https://doi.org/10.1016/j.aej.2023.03.072

[3] Tijana Markovic, Miguel Leon, David Buffoni, Sasikumar Punnekkat, “Random forest with differential privacy in federated learning framework for network attack detection and classification”, Applied Intelligence, Springer, Volume 54, 2024, Pages 8132–8153. https://doi.org/10.1007/s10489-024-05589-6

[4] D. Adhimuga Sivasakthi, A. Sathiyaraj, Ramkumar Devendiran, “HybridRobustNet: enhancing detection of hybrid attacks in IoT networks through advanced learning approach”, Cluster Computing, Springer, Volume 27, 2024, Pages 5005–5019. https://doi.org/10.1007/s10586-023-04248-8

[5] Sandeep Dasari and Rajesh Kaluri, “An Effective Classification of DDoS Attacks in a Distributed Network by Adopting Hierarchical Machine Learning and Hyperparameters Optimization Techniques”, IEEE Access, Volume 12, 2024, Pages 10834 – 10845. **DOI:** 10.1109/ACCESS.2024.3352281

[6] Antonio Paya, Sergio Arroni, Vicente García-Día, Alberto Gómez, “Apollon: A robust defense system against Adversarial Machine Learning attacks in Intrusion Detection Systems”, Computers & Security, Elsevier, Volume 136, 2024, Pages 1-13. https://doi.org/10.1016/j.cose.2023.103546

[7] Azar Abid Salih and Maiwan Bahjat Abdulrazaq, “Cybernet Model: A New Deep Learning Model for Cyber DDoS Attacks Detection and Recognition”, Computers, Materials & Continua Volume 78, Issue 1, 2024, Pages 1275-1295. https://doi.org/10.32604/cmc.2023.046101

[8] Olivia Jullian, Beatriz Otero, Eva Rodriguez, Norma Gutierrez, Héctor Antona & Ramon Canal, “Deep-Learning Based Detection for Cyber-Attacks in IoT Networks: A Distributed Attack Detection Framework”, Journal of Network and Systems Management, Springer, Volume 31, 2023, Pages 1-24. https://doi.org/10.1007/s10922-023-09722-7

[9] Roberto Doriguzzi-Corin, Domenico Siracusa, "FLAD: Adaptive Federated Learning for DDoS Attack Detection", Computers & Security, Elsevier, Volume 137, 2024, Pages 1-16. https://doi.org/10.1016/j.cose.2023.103597
[10] Yash A. Kadakia, Atharva Suryavanshi, Aisha Alnajdi, Fahim Abdullah, Panagiotis D. Christofides, "Integrating machine learning detection and encrypted control for enhanced cybersecurity of nonlinear processes", Computers & Chemical Engineering, Elsevier, Volume 180, 2024, Pages 1-21. https://doi.org/10.1016/j.compchemeng.2023.108498
[11] Sang Ho Oh, Jeongyoon Kim, Jae Hoon Nah and Jongyoul Park, "Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity", Electronics , Volume 13, Issue 3, 2024, Pages 1-19. https://doi.org/10.3390/electronics13030555
[12] Tran Viet Khoa, Do Hai Son, Dinh Thai Hoang, Nguyen Linh Trung, Tran Thi Thuy Quynh, Diep N. Nguyen, "Collaborative Learning for Cyberattack Detection in Blockchain Networks", IEEE Transactions on Systems, Man, and Cybernetics: Systems, Volume 54, Issue 7, 2024, Pages 3920 – 3933. **DOI:** 10.1109/TSMC.2024.3374280
[13] Arvin Hekmati, Jiahe Zhang, Tamoghna Sarkar, Nishant Jethwa, Eugenio Grippo, Bhaskar Krishnamachari, "Correlation-Aware Neural Networks for DDoS Attack Detection in IoT Systems", IEEE/ACM Transactions on Networking, 2024, Pages 1 – 16. **DOI:** 10.1109/TNET.2024.3408675
[14] Vanlalruata Hnamte, Hong Nhung-Nguyen, Jamal Hussain, Yong Hwa-Kim, "A Novel Two-Stage Deep Learning Model for Network Intrusion Detection: LSTM-AE", IEEE Access, Volume 11, 2023, Pages 37131 – 37148. **DOI:** 10.1109/ACCESS.2023.3266979
[15] Mohamed H. Behiry and Mohammed Aly, "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods", Journal of Big Data, Springer, Volume 11, 2024, Pages 1-39. https://doi.org/10.1186/s40537-023-00870-w
[16] Md. Alamgir Hossain, "Enhanced Ensemble-Based Distributed Denial-of-Service (DDoS) Attack Detection with Novel Feature Selection: A Robust Cybersecurity Approach", Artificial Intelligence Evolution, Volume 4, Issue 2, 2023, Pages 165-186. https://doi.org/10.37256/aie.4220233337
[17] Noha Hussen, Sally M. Elghamrawy, Mofreh Salem, Ali I. El-Desouky, "A Fully Streaming Big Data Framework for Cyber Security Based on Optimized Deep Learning Algorithm", IEEE Access, Volume 11, 2023, Pages 65675 – 65688. **DOI:** 10.1109/ACCESS.2023.3281893
[18] Emmanuel Baldwin Mbaya, Emmanuel Adetiba, Joke A. Badejo, John Simon Wejin, Oluwadamilola Oshin, Olisaemeka Isife, "SecFedIDM-V1: A Secure Federated Intrusion Detection Model With Blockchain and Deep Bidirectional Long Short-Term Memory Network", IEEE Access, Volume 11, 2023, Pages 116011 – 116025. **DOI:** 10.1109/ACCESS.2023.3325992
[19] Irfan Ali Kandhro, Sultan M. Alanazi, Fayyaz Ali, Asadullah Kehar, Kanwal Fatima, Mueen Uddin, "Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures", IEEE Access, Volume 11, 2023, Pages 9136 – 9148. **DOI:** 10.1109/ACCESS.2023.3238664
[20] Salahaldeen Duraibi, Abdullah Mujawib Alashjaee, "Enhancing Cyberattack Detection Using Dimensionality Reduction With Hybrid Deep Learning on Internet of Things Environment", IEEE Access, Volume 12, 2024, Pages 84752 – 84762. **DOI:** 10.1109/ACCESS.2024.3411612
[21] Randa Allafi, Ibrahim R. Alzahrani, "Enhancing Cybersecurity in the Internet of Things Environment Using Artificial Orca Algorithm and Ensemble Learning Model", IEEE Access, Volume 12, Pages 63282 – 63291. **DOI:** 10.1109/ACCESS.2024.3390093
[22] Muawia A. Elsadig, "Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach", IEEE Access, Volume 11, August 2023, Pages 83537 – 83552. **DOI:** 10.1109/ACCESS.2023.3303113

[23] Farane Shradha, Gotane Rutuja, Chandanshive Sakshi, Agrawal Khushi and Khandekar Srushti , "Detection of cyber-attacks and network attacks using Machine Learning", World Journal of Advanced Engineering Technology and Sciences, Volume 12, Issue 01, 2024, Pages 128–132. https://doi.org/10.7717/peerj-cs.1793
[24] Sidra Abbas, Imen Bouazzi, Stephen Ojo, Abdullah Al Hejaili, Gabriel Avelino Sampedro5, Ahmad Almadhor, Michal Gregus, "Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks", PeerJ Computer Science, 2024, Pages 1-23. https://doi.org/10.7717/peerj-cs.1793
[25] João Vitorino, Miguel Silva, Eva Maia, Isabel Praça, "Reliable feature selection for adversarially robust cyber-attack detection", Annals of Telecommunications, Springer, 2024, Pages 1-15. https://doi.org/10.1007/s12243-024-01047-z
[26] Syed Shahul Hameed, V. Akshaya, Vishwanadham Mandala, Chunduru Anilkumar, P. VishnuRaja, R. Aarthi, "Security enhancement and attack detection using optimized hybrid deep learning and improved encryption algorithm over Internet of Things", Measurement: Sensors, Elsevier, Volume 30, 2023, Pages 1-8. https://doi.org/10.1016/j.measen.2023.100917
[27] Ashwag Albakri, Bayan Alabdullah and Fatimah Alhayan, "Blockchain-Assisted Machine Learning with Hybrid Metaheuristics-Empowered Cyber Attack Detection and Classification Model", Sustainability, Volume 15, Issue 18, 2023, Pages 1-22. https://doi.org/10.3390/su151813887
[28] R. Aiyshwariya Devi , A.R. Arunachalamm, "Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM", High-Confidence Computing, Springer, Volume 3, Issue 2, 2023, Pages 1-14. https://doi.org/10.1016/j.hcc.2023.100117
[29] Ahmed Ahmim, Faiz Maazouzi, Marwa Ahmim, Sarra Namane, Imed Ben Dhaou, "Distributed Denial of Service Attack Detection for the Internet of Things Using Hybrid Deep Learning Model", IEEE Access , Volume 11, 2023, Pages 119862 – 119875. **DOI:** 10.1109/ACCESS.2023.3327620
[30] Basim Ahmad Alabsi, Mohammed Anbar and Shaza Dawood Ahmed Rihan, "CNN-CNN: Dual Convolutional Neural Network Approach for Feature Selection and Attack Detection on Internet of Things Networks", Sensors, Volume 23, Issue 14, 2023, Pages 1-17. https://doi.org/10.3390/s23146507