Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Developing an intelligent model for accurate detection of cyber threats in smart logistics networks

Mashael M. Khayyat [1, 2, *], Araek Tashkandi [2], Amjad Qashlan [3], Ghada A. Gashgari [3], Manal M. Khayyat [4], Shashi Kant Gupta [1, 5]

[1]*Lincoln University College, Petaling Jaya, Malaysia*
[2]*Department of Information Systems and Technology, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia*
[3]*Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia*
[4]*Department of Computer Science and Artificial Intelligence, College of Computing, Umm Al-Qura University, Makkah, Saudi Arabia*
[5]*Center for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, Punjab 140401, India*

ARTICLE INFO

Article history:
Received 1 July 2025
Received in revised form
4 November 2025
Accepted 19 November 2025

Keywords:
Supply chain management
Smart logistics
Cyber threats
Feature selection
Grey recurrence neuro net

ABSTRACT

Supply Chain Management in the logistics sector involves coordinating processes, resources, and information to ensure the smooth flow of goods and services from suppliers to end customers. However, smart logistics networks are increasingly exposed to cyber threats such as data breaches, ransomware, and unauthorized access to IoT devices, which can disrupt operations and compromise sensitive data. In this study, the BoT-IoT dataset from the Kaggle platform is used. Data preprocessing is performed using Z-score normalization to standardize the data. Principal Component Analysis (PCA) is applied to reduce dimensionality, while Recursive Feature Elimination (RFE) is used to select the most relevant features. For classification, a novel Optimized Grey Recurrence Neuro Net Classifier is developed, which combines the global search capability of the Grey Wolf Optimizer (GWO) with Recurrent Neural Networks (RNNs) to improve detection performance. The model is implemented using Python tools and libraries. Experimental results show that the proposed method outperforms existing approaches, achieving 99.99% accuracy, 99.99% precision, 100% recall, and a 99.99% F1 score, demonstrating its high effectiveness and efficiency.

1. Introduction

Intelligent logistics networks have revolutionized global supply chains by utilizing cutting-edge technology like blockchain, cloud computing, artificial intelligence (AI), and IoT. These technologies enable real-time monitoring, automated management of the inventory, route optimization, and smooth communication among logistics stakeholders (Bhargava et al., 2022). Digitalization and network connections to logistics networks are causing increased vulnerability to cyberattacks since this development poses disruptions in the operations and exposure of personal information, resulting in huge financial losses. The potential targets of cyber safety threats are the accessibility, privacy, and safety of the logistics systems, such as phishing correspondence, ransomware, and distributed denial-of-service (DDoS) attacks (Ansari and Ujjan, 2024). Even Signature-based threat detection combined with rule-based intrusion detection systems (IDS) is not sufficiently effective and can fail to detect cyber threats quickly in modern times. Such practices ultimately result in a high number of false positives and missed security vulnerabilities since they do not adequately respond to the new threats. Since the possession of such features is essential in mitigating such constraints, ingenious threat detection models require artificial intelligence and machine learning (ML) techniques that can be used to observe the network activity and detect abnormal operations, including predicting instantaneous cyber-attacks (Singh et al., 2025). By using deep learning methods

* Corresponding Author.
Email Address: mkhayyat@uj.edu.sa (M. M. Khayyat)
https://doi.org/10.21833/ijaas.2025.12.010
Corresponding author's ORCID profile:
https://orcid.org/0000-0003-3770-432X

to identify complex attack signatures and reduce false positives, the detection accuracy improves (Manoharan and Sarker, 2022). Deep learning technologies, e.g., Convolutional Neural Networks (CNN) or Long Short-Term Memory (LSTM) networks, and ML technologies like random forest and Support Vector Machines (SVM), are applied by the log monitoring system to detect cyber threats and yield a reliable security architecture for contemporary logistics (Fatorachian and Kazemi, 2024; Udurume et al., 2024).

Data integrity, together with transparency and safe authentication in logistics networks, receives additional security enhancement through blockchain integration (Shkarupylo et al., 2024). The defense against cyberattacks might be improved through hybrid AI-blockchain models. The implementation of security adaptive to the changes in the form of a solution is possible as a way to improve the protection of smart logistics networks in dealing with cyber threats and maintaining safe operations in the system (Aljabhan, 2023). Thanks to these advancements, logistics networks will be able to identify and prevent cyber threats prior to their occurrence and this should minimize operational downtimes (Alrumaih et al., 2023). Also, the increased application of IoT in smart logistics introduces additional risks (Cheung et al., 2021). They are the kind of devices used in warehouses, trucks in delivery, and inventory systems, among others, which, unless properly secured, become a place of entry for attackers (Odimarha et al., 2024). Unauthorized access to the network is possible through vulnerability of software or hardware and can even compromise the entire logistics chain (Junejo et al., 2023). Furthermore, data processing and storing via cloud services contribute to the situation of increased security risks since companies are forced to depend on third-party vendors to secure confidential data (Szymonik et al., 2024). A large number of false positives, the inability to detect new threats, reliance on predefined rules, and limited adaptability are major weaknesses of traditional long-term cybersecurity strategies in smart logistics networks. Modern cyberattacks, the demand for real-time threat detection, and the integration of artificial intelligence into security systems create challenges that conventional methods are unable to meet. This study aims to develop an intelligent cyber-threat detection system for smart logistics networks using an optimized Grey Recurrence Neuro Net classifier, which is a deep learning method, combined with advanced feature-selection techniques to improve security, efficiency, and accuracy.

The proposed model is developed using data from the Bot-IoT 2018 dataset. It applies Z-score normalization and Principal Component Analysis to enhance data quality and operational efficiency. In addition, the model uses the Recursive Feature Elimination procedure to identify the most important features and improve prediction accuracy. The study introduces an enhanced version of the Grey Recurrence Neuro Net classifier that incorporates the Grey Wolf Optimizer to achieve higher accuracy in detecting cyber threats. The results show improved cybersecurity resilience in smart logistics networks, demonstrating higher detection accuracy and efficiency than current methods.

The remainder of this paper is organized as follows: Section 2 presents related work, Section 3 describes the methodology, Section 4 discusses the findings, and Section 5 concludes the study.

2. Literature review

Due to the imminent explosion of 5G IoT connections in industrial settings, Deep learning (DL)-based anomaly detection (AD) as a function of the 3GPP mobile cellular IoT design was investigated (Savic et al., 2021). By integrating autoencoder-based anomaly recognition modules into the mobile core network and IoT devices, the suggested design strikes a balance between accuracy and network efficiency. Cybersecurity threats in logistics were brought by cloud computing, big data, 5G, and IoT. It used scientific analysis to investigate mitigation options suggested in the approach examined in Enache (2023). To create a bi-directional CNN and blockchain-enabled IoT-based logistics and theft control solution. It performs exceptionally well via real-time analysis of transmission patterns and vulnerabilities. Limitations include significant computing complexity and difficulties integrating with current systems (Alanazi et al., 2024). In light of evolving cyber threats, the findings highlight the need for a virtual Chief Information Security Officer (vCISO) to enhance cybersecurity and ensure Agriculture 4.0's sustainability and resilience, as evaluated in VanYe et al. (2021). The Internet of Things technologies (Zhan et al., 2022) are used to create a monitoring system for financial logistics. The approach incorporates logistical applications to improve security and efficiency. The outcomes show improved network security, accuracy, forecasting, and delivery. High expenses and insufficient use of integrated systems are among the drawbacks.

Cyberwarfare threats against smart cities using intellectual analysis and a foresight scenario were presented in Nuseir et al. (2024). The results of an analysis of technological, social, and governance vulnerabilities show that to reduce cyber risks, enhanced safety measures, stronger local governance, and the integration of smart city security with national security policies were all necessary to be discussed in Soare and Burton (2020). The suggested approach tracks the development of IoT in logistics and supply chain management by using bibliometric analysis of 2,680 Scopus-indexed articles in Bravos et al. (2022). The influence of IoT, including AI, blockchain, and 5G, was highlighted in the results, which also point to new research areas and suggest future paths for technological developments and security improvements in SCM. Zrelli and Rejeb (2024)

examined real data and Internet of Things devices, presenting an architecture that supports reliable, monitored, and efficient industrial communication with improved protection against cyber threats. Their study proposed a hybrid feature-reduction approach for intelligent detection of IoT cyberattacks, where features are combined and ranked before applying machine-learning classifiers. This approach improved precision and detection rates. Kumar et al. (2021) reported a limitation related to handling changing attack patterns and computational demands. They developed and validated a data-driven model with an advanced engine manufacturer, showing reductions in production time and energy consumption while keeping computation time at a reasonable level.

Cyberattacks in smart logistics networks create opportunities for attackers to access critical information and disrupt supply-chain operations. Traditional security measures struggle to detect such attacks because the data are high-dimensional and the attack patterns change frequently. Existing classification systems designed for sequential logistics data are often ineffective and cannot achieve accurate threat detection. Therefore, detecting cyber threats in intelligent logistics networks requires an advanced framework that improves data preprocessing and selects the most relevant features before applying an optimized classification model to achieve more accurate identification results.

3. Methodology

The proposed method establishes an organized process to detect cyber threats within smart logistics networks effectively. The dataset from Bot-IoT 2018 on Kaggle is pre-processed using Z-score normalization, feature extraction using PCA, and RFE for feature selection. The model employs an Optimized Grey Recurrence Neuro Net Classifier, fine-tuned with Grey Wolf Optimization, outperforming existing methods in accuracy and efficiency. Fig. 1 shows the overview of the methodology.

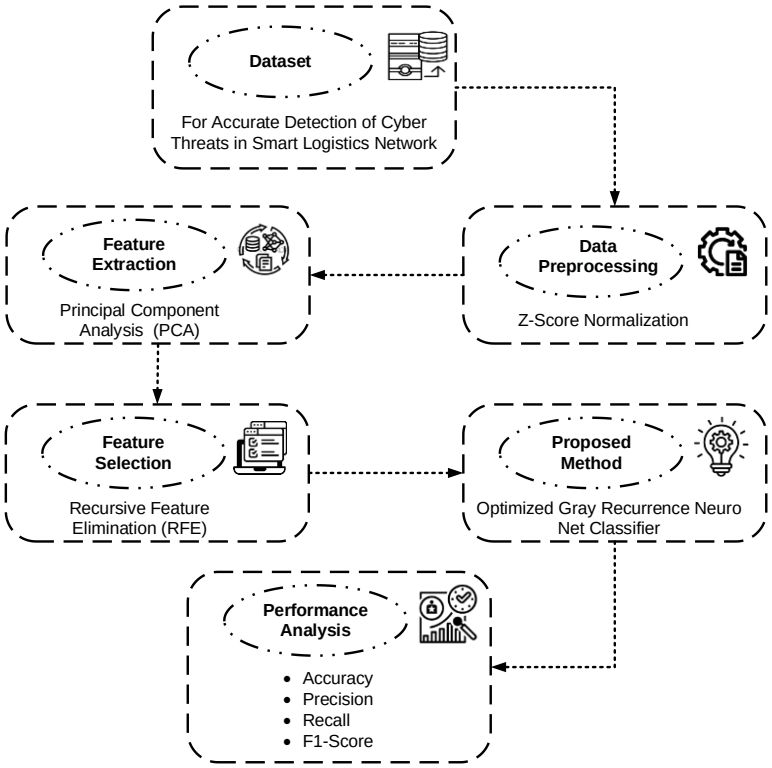

Fig. 1: Overview of framework

3.1. Dataset

The Bot-IoT 2018 dataset was obtained from the open-source Kaggle platform to support accurate cyber-threat detection in smart logistics networks. The dataset includes a combination of cybersecurity-related features relevant to smart logistics environments, such as network traffic logs, authentication records, IoT device events, and system access attempts. It contains examples of both normal operations and various cyberattacks, including unauthorized access, malware intrusions, and data breaches. To maintain the original class distribution and achieve balanced representation for reliable performance evaluation, the dataset (www.kaggle.com/datasets/liuwoo/botiot-2018) was split into 80% for training and 20% for testing using class-conscious sampling.

3.2. Data pre-processing

The Z-score normalization technique normalizes data by using attribute means to calculate the standard deviation reduction of outcomes. By

efficiently handling various sizes of data, this ensures that each point of data will have a mean of zero and a standard deviation of one, thus improving the performance of the model.

3.2.1. Z-score normalization

The normalization technique called Z-score creates equal scaling through the process of mean subtraction and standard deviation division. The process uses three benefits to boost model performance for accurate cyber threat detection in smart logistics networks, as described in Eq. 1.

$$u' = \frac{u-\mu}{\sigma} \quad (1)$$

The value of the feature standard deviation is σ, and the mean of the selected feature is expressed asμ. Values identical to the mean in Z-score normalization become zero, while those above the mean receive positive values and those below the mean receive negative values.

3.3. Feature extraction

Through the algorithmic method of PCA, data with many dimensions gets separated into a reduced number of independent, uncorrelated variables called principal components. PCA enhances computational performance while making the model concentrate on essential patterns in the data, while maintaining vital information.

3.3.1. Principal component analysis (PCA)

PCA and Z-score normalization are common methods that are used here specifically for the GRNN framework and the BoT-IoT dataset. While PCA eliminates multicollinearity and preserves important uncorrelated components, normalization standardizes a variety of feature scales. This improves the Grey Wolf-optimized GRNN's capacity to precisely identify cyberthreats in smart logistics while lowering computing costs and accelerating convergence.

The main patterns, along with uncorrelated variable reduction of high-dimensional data, can be achieved through PCA to enhance feature extraction. Its use of PCA in logistical networks simplifies computational operations, makes models operate faster, and improves the detection of cyber threats. A thorough description of the PCA methodology used in this training appears below. A unit-weighting vector (Y_j) and the original data matrix Z with $o \times m$ dimensions are used to express the ith PC matrix (Ej) as Eq. 2.

$$Ej = Y_j^S \mathrm{Z} = \sum_{i=1}^{m} y_{ji} z_i \quad (2)$$

where, the data vector of size m is denoted by z and the loading coefficient by z. Projecting Z to Y yields the variance matrix $Z(Var(\mathrm{Z}))$, which needs to be maximized in the manner described in Eqs. 3-4 below.

$$Var(\Upsilon) = \frac{1}{m}(YZ)(YZ)^S = \frac{1}{m}YZZ^SY \quad (3)$$

$$MaxVar(Z) = Max\left(\left(\frac{1}{m}\right)YZZ^SY\right) \quad (4)$$

Given that the covariance matrix of $Z(cov(Z))$ is equal to $\frac{1}{m}ZZ^S$, $Var(Z)$ can be written in this way, Eqs. 5-6.

$$Var(Z) = Y^s cov(Z)Y \quad (5)$$

$$K = Y^S cov(Z)Y - \delta(Y^SY - 1) \quad (6)$$

Since the weighting vector in Eq. 6 is a unit vector, the word $Y^SY - 1$ is regarded as 0.

Therefore, by equating the derivative of the Varangian function (K) concerning Y, the maximum value of $var(Z)$ can be determined by Eqs. 7-8.

$$\frac{dK}{dY} = 0 \quad (7)$$

$$cov(Z)Y - \delta Y = (cov(Z) - \delta J)Y = 0 \quad (8)$$

where, δ is the eigenvalue of $cov(Z)$ and Z is its eigenvector. The eigenvalue ratio of the Jth PC concerning the entire dataset can be used to determine the percentage of variance explained; this ratio shows the extent to which the PC (o) covers the entire dataset under investigation.

3.4. Feature selection

A powerful feature selection method called Recursive Feature Elimination (RFE) iteratively eliminates the least significant features according to a prediction model's performance. RFE considers feature interdependence and connections within the dataset, in contrast to more basic methods like mutual information, which assess the significance of individual features separately. RFE refines the subset of characteristics to include the attributes that most effectively contribute to model correctness by continuously removing less important features. The model's capacity to generalize to new data is enhanced by this iterative process, which aids in finding the best, most condensed set of features. RFE is especially useful for high-dimensional, complicated datasets with potentially redundant or associated features. It produces more robust and dependable predictions by reducing noise and overfitting.

3.4.1. RFE

RFE enhances the performance and efficiency of cyber threat detection in the smart logistics network by recursively eliminating less significant features and picking up the most important features. Feature selection procedures are vital in the performance and effectiveness of an intelligent model employed during a cyber-threat detection process in smart logistics networks. The RFE algorithm executes three

parts to train its model on the data, and it decides significant features it leave out in each stage.

In logistic regression, the value of feature importance $I(fi)$ is shown either by model weights, which are expressed as wi.

$$I(fi) = | wi | \quad (9)$$

Through this method, the model supports improved efficiency and accurate predictions by remaining focused on the essential threat detection features. Using RFE ensures the model operates at its optimum level, thus enhancing its immediate ability to detect and respond to cyber threats.

3.5. Optimized grey recurrence neuro net classifier

The Optimized Grey Recurrence Neuro Net Classifier refers to the high-powered deep learning architecture, which enhances the SLN cybersecurity via the optimized detection and mitigation of the cyber threat. The frame has three techniques, which integrate the Grey System Theory (GST) to adapt to the uncertainty of network traffic, the Recurrence Analysis to detect cyber abnormalities, and Neural Networks to learn adjustment and classification. SLNs face cyberattacks, such as DDoS, and also intrusion of data and malware attacks, causing destruction to automated supply chains, IoT-based fleets, and cloud-managed logistics operations. Optimized Grey Recurrence Neuro Net Classifier makes use of Grey System Theory to process uncertain and incomplete data measurements to enhance threat detection in changing system environments. Recurrence analysis extracts temporal dependencies, helping detect subtle patterns of malicious activities. The Neural Network component optimizes feature learning and classification, ensuring high accuracy in identifying cyber threats. Algorithm 1 shows the pseudo-code of the Optimized Grey Recurrence Neuro Net Classifier.

Algorithm 1: Optimized Grey Recurrence Neuro Net Classifier

Input:

- Dataset D with 1000 samples, each with 20 features (X: 1000 x 20) and 3 classes (Y: 1000 x 1)
- Learning rate (lr) = 0.001
- Number of layers = 3
- Neurons per layer: 64 (Layer 1, Layer 2), 32 (Layer 3)
- Grey Recurrence Threshold (GRT) = 0.85
- Optimization Strictures:

$-\ Momentum = 0.9$

$-\ Weightdecay = 0.0001$

Output:

- Trained Optimized Grey Recurrence Neuro Net Classifier model
- Classification results (Accuracy, Precision, Recall)

Step 1: Data Preprocessing

1.1 Normalize the dataset (Min-Max Scaling)

- For each feature xi in X, normalize as: $xi = (xi - min(xi)) / (max(xi) - min(xi))$

1.2 Apply Grey Relational Analysis (GRA) to extract important features

- GRA value between features $X1, X2$: $GRA\ (X1, X2) = (min\ (|X1 - X2|)) / (max\ (|X1 - X2|))$

1.3 Compute the Grey Recurrence Matrix (GRM) based on feature similarity

- $GRM[i][j] = GRA(X[i], X[j])\ (Forallpairsofi, jinthedataset)$

1.4 Construct Grey Recurrence Graph (GRG) using GRT:

- $IfGRM[i][j] > 0.85, thenlinknodesiandj$ in the GRG

1.5 Convert GRG into feature embedding representation:

- GRFE = Eigenvalue Decomposition of GRM (dimensionality reduction)

Step 2: Neural Network Initialization

2.1 Define the architecture of the Recurrence Neuro Net with 3 layers:

- Layer 1: 20 input features → 64 neurons
- Layer 2: 64 neurons → 64 neurons
- Layer 3: 64 neurons → 32 neurons
- Output Layer (OL): 32 neurons → 3 classes (Softmax)

2.2 Initialize weights and biases:

- W1 (20x64), b1 (64)
- W2 (64x64), b2 (64)
- W3 (64x32), b3 (32)
- W4 (32x3), b4 (3)

2.3 Set up activation functions:

- Re LU for hidden layers (HL) (Layer 1, 2, 3)
- Softmax for OL

2.4 Define loss function: Cross-entropy loss for classification

Step 3: Forward Propagation

3.1 Compute feature transformation for the first HL:

H1 = Re LU ($W1 * X + b1$) (Shape: 1000 x 64)

3.2 Compute Grey Recurrence Feature Encoding (GRFE) using GRG:

GRFE = Eigenvalue Decomposition of GRM → Reduce dimensions from 64 to 32

3.3 Compute activations for Layer 2:

H2 = Re LU ($W2 * H1 + b2$) (Shape: 1000 x 64)

3.4 Compute activations for Layer 3:

H3 = Re LU ($W3 * H2 + b3$) (Shape: 1000 x 32)

3.5 Compute final OL (Softmax):

Output = Softmax ($W4 * H3 + b4$)($Shape$: 1000 x 3)

Step 4: Loss Computation and Backpropagation

4.1 Determine the losses L utilizing the anticipated (Output) and actual (Y) labels:

$L = -\Sigma Y$ * log (Output) for each sample

4.2 Compute gradients $\partial L/\partial Wi$ and $\partial L/\partial bi$ for each layer using backpropagation:

$-\ \partial L/\partial W4, \partial L/\partial b4$

$-\ \partial L/\partial W3, \partial L/\partial b3$

$-\ \partial L/\partial W2, \partial L/\partial b2$

$-\ \partial L/\partial W1, \partial L/\partial b1$

4.3 Update weights and biases using Adam optimizer:

- Update rule: $Wi = Wi - lr * \partial L/\partial W$i (with momentum)

Step 5: Model Optimization

5.1 Apply Dropout in Layers 2 and 3 (Dropout rate = 0.5)

5.2 Apply Batch Normalization after each HL

5.3 Apply Momentum-based Gradient Descent with momentum = 0.9 for stability

5.4 Fine-tune learning rate: $lr = lr * 0.99$ after every 100 epochs

Step 6: Model Evaluation

6.1 Evaluate model performance on test dataset:

- Test dataset size = 200 samples

6.2 Compute Accuracy, Precision, Recall, F1-score

- Accuracy = (Correct Predictions) / (Total Predictions)

6.3 Generate Confusion Matrix:

Confusion Matrix = [[TP, FP], [FN, TN]]

Step 7: Prediction and Deployment

7.1 Use a trained Optimized Grey Recurrence Neuro Net Classifier model to classify new instances
7.2 Optimize model deployment using ONNX/Tensor RT for real-time applications
End Algorithm

3.5.1. RNN

RNNs enhance cybersecurity in smart logistics by detecting anomalies in network traffic, identifying cyber threats, and predicting attacks. Their sequential processing capability enables real-time threat analysis, safeguarding IoT devices, supply chains, and data integrity in logistics systems. RNNs are not limited to processing input in a single direction, in contrast to fundamental neural networks, including Multilayer Perceptron (MLPs). RNNs can briefly memorize information for later use in addition to looping through many layers. A conventional neural network is shown by the symbol MM, where the input is represented by w_o and the output by g_o.

Let w_o represent the standard RNN (sRNN) model's input. The symbol x_{gw} represents the weights of the association among the input w_o and the first HL. x_{gg} represents the weight of the link that connects the currently invisible level to the next concealed level. x_{gz} epitomizes the weight among the last HL and its corresponding OL. Let the output at time o be represented by g_o. The biases introduced to the connections from the final level and the concealed level are represented a_g and a_z, respectively. An SRNN is theoretically formed as follows in Eqs. 10-12.

$$g_o = h(g_{o-1}.w_o) \tag{10}$$
$$g_o = h\left(\left[x_{gw}.w_o + x_{gg}.w_{o-1}\right] + a_g\right) \tag{11}$$
$$\bar{z}_o = h\left(\left[x_{gw}.w_o + x_{gg}.w_{o-1}\right] + a_g\right) \tag{12}$$

where, $\bar{z}_o$ is the projected conclusion.

Sequential training is done on the RNN. Every step$o$ calculates the variance (F) between the actual (real) output values and the expected ones. In machine learning, F is referred to as Loss, K. The reduction of K is the ultimate goal of the training process. Put differently, a good model will have a low K.

$$K(\bar{z}_o, z) = \sum_{o=1}^{M} K(\bar{z}_o - z_o) \tag{13}$$

As the dataset size and M rise, the sRNN model is known to encounter gradient vanishing problems or explosions during development.

Let M be the E produced by a batch, A, over a maximum training duration, M. Finding the reduction's fractional derivatives about the associated weight,X, is indicated by Eq. 14.

$$\frac{\partial K}{\partial X} = \sum_{o=1}^{M} \frac{\partial K_o}{\partial X} \tag{14}$$

By rewriting the expression in Eq. 14 using the chain rule, $\frac{\partial K}{\partial X}$ becomes as follows in Eq. 15.

$$\frac{\partial K}{\partial X} = \sum_{o=1}^{M} \frac{\partial K_o}{\partial z_o}\frac{\partial z_o}{\partial g_o}\frac{\partial g_o}{\partial z_m}\frac{\partial z_m}{\partial X} \tag{15}$$

The derivative of a hidden state that retains data at time o that is directly related to the hidden state at time m, is derived from Eq. 15. Additionally, the Jacobian matrix $\frac{\partial g_o}{\partial g_m}$, about time o and m is contained in the expression 16.

$$\frac{\partial g_o}{\partial g_m} = \frac{\partial g_o}{\partial g_{o-1}}\frac{\partial g_{o-1}}{\partial g_{o-2}} \dots \frac{\partial g_{m+1}}{\partial g_m} = \prod_{j=m+1}^{o} \frac{\partial g_j}{\partial g_{j-1}} \tag{16}$$

The Eigen Decomposition Vector (EDV)produced by Eq. 17 is represented as follows.

$$EDV = X^S diag[h'(g_{o-1})] \tag{17}$$

These eigenvalues are produced by the EDV based on the following constraint: $\lambda_1, \lambda_2, \lambda_3, \dots \dots, \lambda_m$ $|\lambda_1| > |\lambda_2||\lambda_3| \cdots |\lambda_m|$. Every one of the following eigenvalues is associated with its matching eigenvector: $ev_1, ev_2, ev_3, \dots \dots, ev_m$.

When the biggest λ_j is less than 1, a vanishing gradient is present. It is when $\lambda_j > 1$ that the gradient explodes.

The information flow inside an LSTM and gated recurrent unit (GRU) is mathematically expressed by the formulas defined in 18 and 19, respectively.

$$LSTMFormulation: \begin{cases} h_o = \sigma(X_h.[u_{o-1}, w_o] + a_h) \\ l_o = \sigma(X_l.[u_{o-1}, w_o] + a_o) \\ T'_o = \tanh\left(X_t.[u_{o-1}, w_o] + a_t\right) \\ T_o = h_o * T_{o-1} + o_1 * T'_o \\ q_o = \sigma(X_q.[u_{o-1}, w_o] + a_q) \\ u_o = q_o * \tanh(T_o) \end{cases} \tag{18}$$

where, the cell state is indicated by T, the LSTM unit uses the following activating operations: The sigmoid, $\sigma(b) = \frac{b}{1+e^{-b}}$, and the hyperbolic tangent $\tanh(b) = \frac{1-e^{-2b}}{1+e^{-2b}}$. w is the input vector. The output vector is indicated by$u$. The weights and associated biases are denoted by X and a.

$$GRUFormulation = \begin{cases} l_o = \sigma(X_l.[T_{o-1}, w_o] + w_o) \\ y_o = \sigma(X_y.[T_{o-1}, w_o]) \\ T'_o = \tanh(X.[y_o * T_{o-1}, w_o]) \\ T_o = (1 - l_o) * T_{o-1} + l_o * T'_o \end{cases} \tag{19}$$

The input vector is denoted by w. The calculated prediction is T_o. The update function is indicated by l_o. X defines the associated strength. Similar to the LSTM in Eq. 19, the GRU squashes the data using the sigmoid activation functions and the hyperbolic tangent.

The Grey Recurrence Neuro Net (GRNN) combines the Grey System hypothesis, which is efficient at simulating uncertain and partial data that is common in IoT and smart logistics, to improve on conventional recurrent neural networks. By using the Grey Wolf Optimizer (GWO) for hyperparameter tuning, GRNN avoids local minima more effectively and converges more quickly than well-known RNN variations like LSTM and GRU. By enhancing the

model's resilience to ambiguous and noisy sequential data, this combination results in more precise and trustworthy cyber threat identification. Because of this, GRNN is far superior to conventional RNN architectures in managing intricate, real-world data circumstances.

3.5.2. GWO

The GWO improves the processing of sequential data, adjusts hyperparameters, and enhances feature selection to achieve accurate cyber-threat detection in smart logistics networks. GWO is a swarm-intelligence algorithm that mathematically models the social structure and hunting behavior of grey wolves. In this model, wolves are divided into four groups: alpha, beta, delta, and omega. The alpha wolves make decisions, the betas assist and help maintain order, the deltas follow and manage the lower levels, and the omegas occupy the subordinate position within the hierarchy.

The inspiration for GWO comes from the social intelligence of grey wolves, particularly their leadership structure and coordinated hunting strategies. In nature, a grey wolf pack is organized around a dominant alpha that leads the group during feeding, movement, and hunting. The beta wolves support the alpha and have significant authority, while the delta and omega wolves hold lower-ranking roles.

This hierarchical structure, illustrated in Fig. 2, forms the basis of how GWO models search, leadership, and optimization behavior.

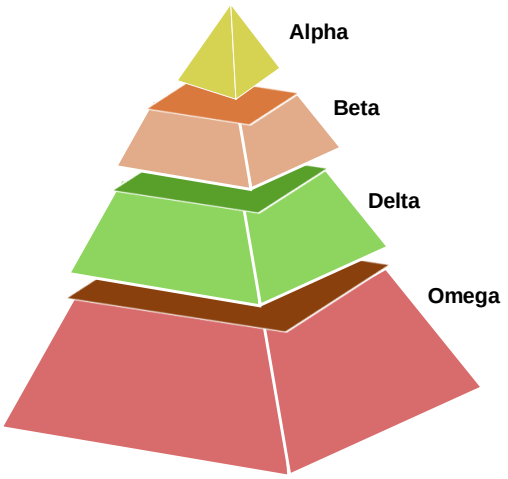

Fig. 2: Social hierarchy of grey wolves

Encircling: Chasing and encircling are the initial stages of the hunting procedure. Mathematically, GWO takes into account multiple wolves (points) in this phase for a space with n dimensions, and it modifies the first one's location dependent on the second one based on Eq. 20.

$$W(s+1) = W(s) - B.C \quad (20)$$

where, $W(s+1)$ denotes the wolf's upcoming position, $W(s)$ denotes its present setting, B is a set of parameters, and D is a vector that is calculated using Eq. 21 and is based upon the prey's position (Wo).

$$C = |D.W_O(s) - W(s)| \quad (21)$$
$$D = 2.q_2 \quad (22)$$

where, q_2 is a vector ∈ [0,1] that is randomly generated. A solution can move around a different outcome by utilizing both of these Eq. 23.

$$B = 2b.q_1 - b \quad (23)$$

Consequently, during the operation, the values for a, the vector, decline linearly from 2 to 0. A randomly generated vector from the interval [0, 1] is denoted by $q1$. The following is the equation to update the parameter b.

$$b = 2 - s\left(\frac{2}{s}\right) \quad (24)$$

where, s is the maximum number of iterations and s indicates the present iteration.

Attacking (hunting) phase: The GWO improves cyber threat detection by modeling the social hierarchy of wolf packs. Alpha, beta, and delta solutions guide optimization instead of random relocation in a hypersphere, ensuring better accuracy in Eq. 25, and Fig. 3 shows the architecture of GWO.

$$W(s+1) = \frac{1}{3}W_1 + \frac{1}{3}W_2 + \frac{1}{3}W_3 \quad (25)$$

where, Eq. 26 is used to calculate W_1, W_2, W_3.

$$W_1 = W_\alpha(s) - B_1.C_\alpha$$
$$W_2 = W_\beta(s) - B_2.C_\beta \quad (26)$$
$$W_3 = W_\delta(s) - B_3.C_\delta$$

where, $C_\alpha C_\beta C_\delta$ can be computed using Eq. 27.

$$C_\alpha = |D_1.W_\alpha - W|$$
$$C_\beta = |D_2.W_\beta - W| \quad (27)$$
$$C_\delta = |D_3.W_\delta - W|$$

The categories and types of the main hyperparameters utilized in the GWO-based RNN classification are listed in Table 1. These include layer numbers, neuron counts, learning rate, batch size, and epochs.

The model's structure and training performance are determined by the Optimized Grey Recurrences Neuro Net Classifier's hyperparameters. Model depth and temporal pattern learning ability are controlled by the number of RNN layers (1–3) and neurons per layer (16–128). By randomly disregarding neurons during training, the dropout rate (0.1–0.5) helps avoid overfitting, while the learning rate (0.0001–0.01) determines how rapidly the model updates weights. Curriculum stability and memory utilization are impacted by batch size (16–128). Loss minimization is guided by optimizer type (Adam, RMSprop, SGD), whereas activation algorithms (ReLU, Tanh, Sigmoid) introduce non-

linearity. The RNN processes a certain number of time steps based on the sequence length (10–100). These are optimized by GWO to enhance classification performance.

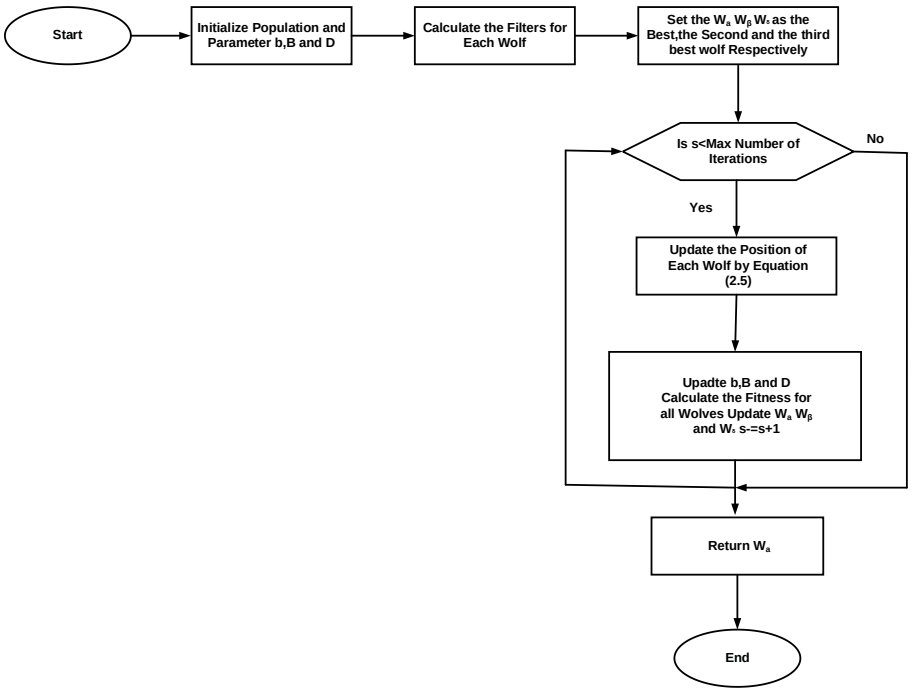

Fig. 3: GWO flowchart

Table 1: Hyperparameters used in grey wolf optimizer-based RNN classification

No.	Hyperparameter	Type	Range / Options	Description
1	Number of RNN layers	Integer	[1, 3]	Number of recurrent layers (e.g., LSTM or GRU)
2	Neurons per layer 1	Integer	[16, 128]	Number of hidden units in the first RNN layer
3	Neurons per layer 2	Integer	[16, 128]	Only used if layers > 1
4	Neurons per layer 3	Integer	[16, 128]	Only used if layers > 2
5	Learning rate	Continuous	[0.0001, 0.01]	Step size for optimizer during weight updates
6	Dropout rate	Continuous	[0.1, 0.5]	Dropout fraction to prevent overfitting
7	Batch size	Integer	[16, 128]	Number of samples processed before updating weights
8	Activation function	Categorical	{0: ReLU, 1: Tanh, 2: Sigmoid}	Activation function for RNN hidden layers
9	Optimizer type	Categorical	{0: Adam, 1: RMSprop, 2: SGD}	Optimization algorithm used to minimize the loss function
10	Sequence length	Integer	[10, 100]	Length of input sequences (time steps) fed to the RNN

4. Results

To identify cyberthreats in smart logistics networks, the suggested Optimized Grey Recurrence Neuro Net Classifier demonstrated exceptional accuracy. Table 2 shows the experimental setup. Current methods for deep learning include (LSTM + CNN) (Alzahrani and Asghar, 2024) and CNN + bidirectional gated recurrent unit (BIGRU) (Alzahrani and Asghar, 2023), which have been used in smart logistics networks to detect cyber threats.

Table 2: Results of the experimental setup

Stage	Details
Dataset	Kaggle (cyber threat data for smart logistics)
Classifier	Optimized grey recurrence neuro net
Programming	Python
Libraries	Scikit-learn, TensorFlow/Keras, NumPy, Pandas
Evaluation	Accuracy, precision, recall, F1-score, ROC-AUC
Validation	Smart logistics simulation environment

A confusion matrix is a measure of performance used to compare expected and actual labels to identify how true a classification model is. Its 4 principal values are $TruePositives$ (TP), $TrueNegatives$ (TN), $FalsePositives$ (FP), and $FalseNegatives$ (FN). To test well, the Optimized Grey Recurrence Neuro Net Classifier identifies threats within smart logistics networks and employs a confusion matrix. Improved model performance is evident in high TP and TN ratios, whereas diminished FP and FN ensure fewer risks are misinterpreted.

The strength and reliability of the proposed framework are enhanced with this analysis. High precision is reflected in the confusion matrix, which shows 146716 TP and 7 TN. 15 FN and 3 $FN$are instances of misclassifications. Fig. 4 represents the outcome of the Confusion Matrix.

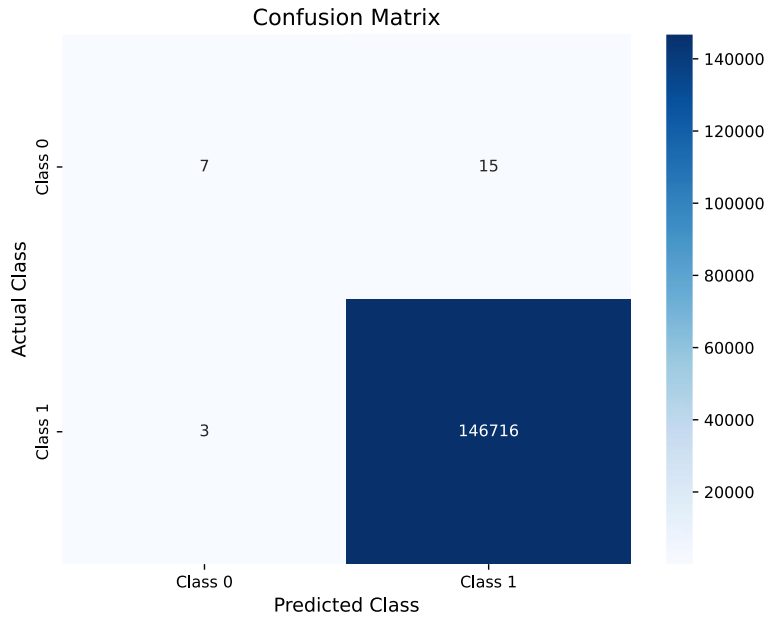

Fig. 4: Result confusion matrix

The Optimized Grey Recurrence Neuro Net Classifier's classification performance in identifying cyber threats in smart logistics networks is assessed by the image's ROC Curve. An AUC of 0.9735 indicates a very effective model when the $TruePositiveRate$ (TPR) is plotted against the $FalsePositiveRate$ (FPR). The model's ability to differentiate between threats and non-threats improves with an AUC near 1. This bolsters the extract's assertion that the suggested approach improves the precision and effectiveness of cyber threat detection in intelligent logistics networks. Fig. 5 represents the outcome of the ROC curve. In the dataset used for cyber threat detection in smart logistics networks, the graph depicts a correlation matrix that shows the links between Principal Components (PCs) and the attack variable. The correlation coefficient is represented by each value in the matrix; blue denotes weak or no correlation (near 0), and red denotes strong correlation (close to 1). Because reduced reductions are accomplished by principal component analysis (PCA), which guarantees that only the most pertinent characteristics are kept, this analysis is essential to the investigation. The outcomes contribute to the Optimized Grey Recurrence Neuro Net Classifier's increased effectiveness in detecting cyber threats. Fig. 6 represents the outcome of the Correlation Matrix.

4.1. Accuracy and precision

The cyber threats in smart logistics networks. Accuracy refers to the correct identification of threats, while precision measures how many identified threats are truly malicious, reducing false positives and improving threat detection reliability. While the CNN + BIGRU model performs marginally worse with 94% accuracy and precision, the LSTM + CNN model obtains 95.73% accuracy and 96.64% precision, and Bidirectional Encoder Representations from Transformers (BERT) finds 98.2% accuracy and 98.00% precision. Both models are greatly outperformed by the suggested Optimized Grey Recurrence Neuro Net Classifier, which achieves an astounding 99.99% accuracy and precision (Fig. 7).

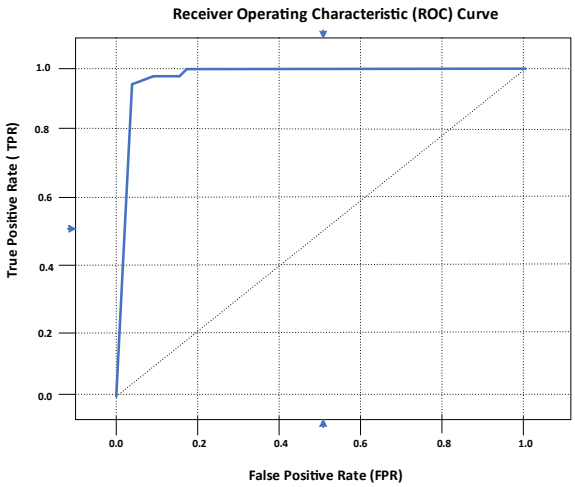

Fig. 5: Outcome of the ROC curve

4.2. Recall and F1 score

Recall gauges how well smart logistics networks can detect real cyber threats, while the F1 Score strikes a compromise between precision and recall, providing a single metric for assessing overall detection performance that minimizes false positives and negatives. CNN + BIGRU had 94% for both recall and F1-score metrics, whereas LSTM + CNN had 94.15% recall and 95.52% F1-score, and BERT achieved 98.00% both recall and F1-score. With a perfect 1.000% recall and 99.99% F1 score. Fig. 8 and Table 3 represent the outcome of the overall result. The suggested GWO-RNN model performs better than other metaheuristic-trained RNN variations with the highest recall, accuracy, F1 score, and precision. When it comes to cyber threat identification for smart logistics, Grey Wolf Optimizer–trained Recurrent Neural Network (GWO-RNN) performs better than Particle Swarm Optimization–trained RNN (PSO-RNN), Genetic Algorithm–trained RNN (GA-RNN), Differential Evolution–trained RNN (DE-RNN), and Ant Colony Optimization–trained RNN (ACO-RNN). The outcome of this optimizer is shown in Table 4.

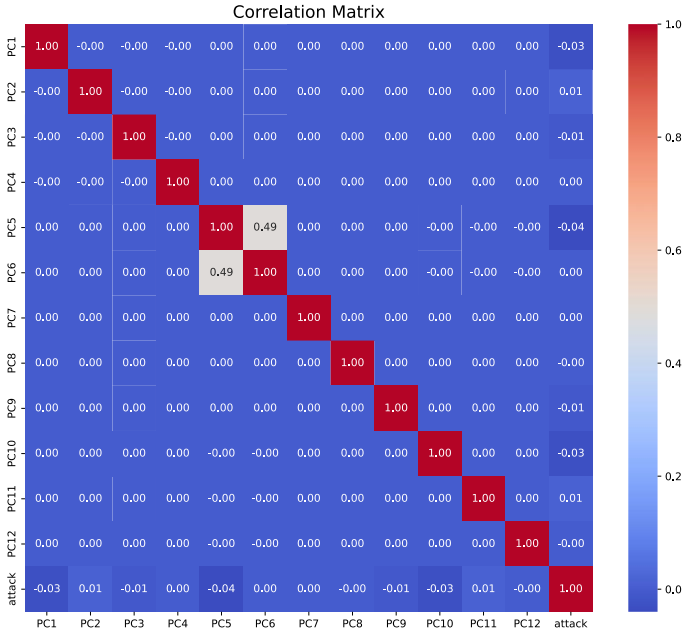

Fig. 6: Result of correlation matrix

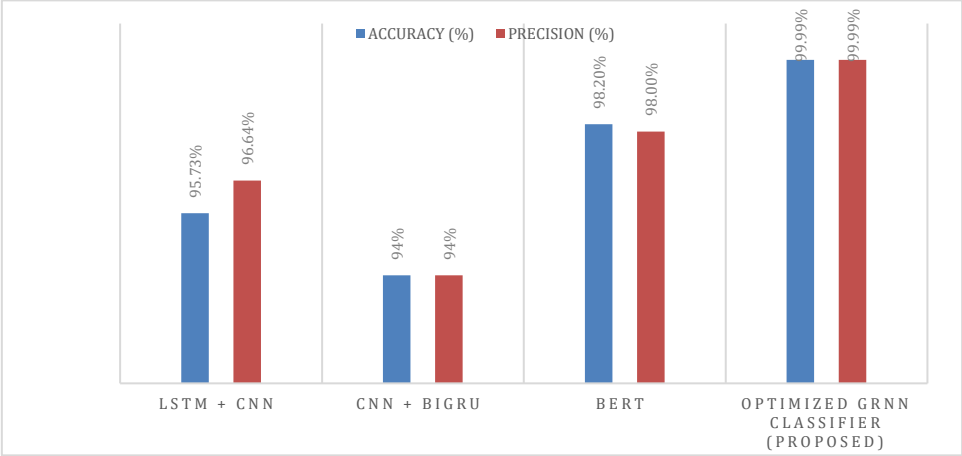

Fig. 7: Graphical representation of precision and accuracy output

Table 3: Overall comparison result

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1 score (%)
LSTM + CNN (Alzahrani and Asghar, 2024)	95.73 %	96.64 %	94.15 %	95.52 %
CNN + BIGRU (Alzahrani and Asghar, 2023)	94 %	94 %	94 %	94 %
BERT (Ferrag et al., 2024)	98.2%	98.00%	98.00%	98.00%
Optimized grey recurrence neuro net classifier (proposed)	99.99 %	99.99 %	1.000 %	99.99 %

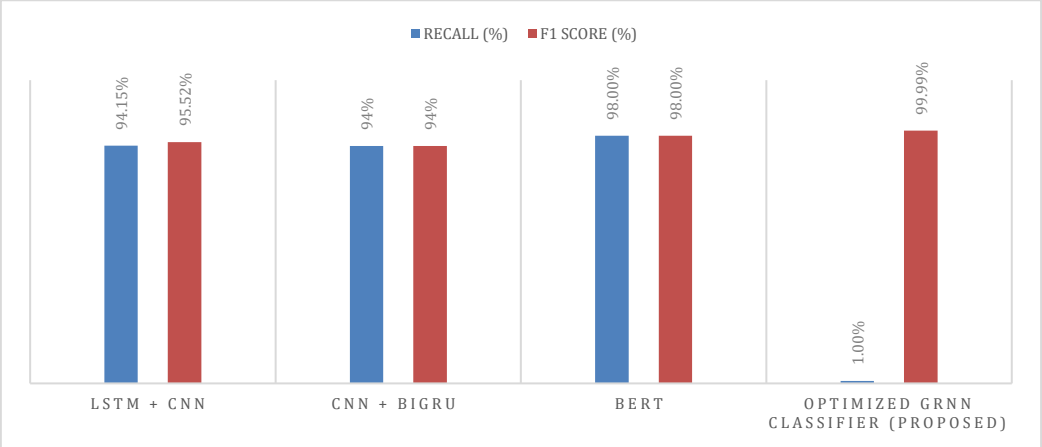

Fig. 8: Graphical representation of recall and F1 score output

Table 4: Ablation study results

Method	Accuracy	Precision	Recall	F1 score
GWO-RNN (proposed)	99.99%	99.99%	1.000	99.99%
PSO-RNN	98.85%	98.83%	0.988	98.84%
GA-RNN	98.78%	98.75%	0.987	98.76%
DE-RNN	98.81%	98.80%	0.988	98.79%
ACO-RNN	98.73%	98.70%	0.986	98.71%

The optimum outcomes were obtained by the suggested GWO-RNN, which demonstrated close to perfect classification with 99.99% accuracy, precision, recall, and F1-score. Consistently behind, with a 98.85% accuracy rate and significant precision and recall, was the PSO-RNN. The accuracy of the GA-RNN and DE-RNN was comparable, with differences between 98.78% to 98.81%. The accuracy of ACO-RNN was the lowest, at 98.73%. These findings demonstrate the accuracy with which GWO optimizes RNN parameters, outperforming conventional techniques in the identification of cyberthreats for Internet of Things networks.

5. Discussion

Cyber threats in smart logistics networks refer to malicious attacks targeting interconnected systems, such as IoT devices, transportation management software, and supply chain data. Such risks can undermine operations, leak personal data, and negatively affect the finances and reputation. In the LSTM + CNN system, there are limitations in handling large and high-dimensional data that are typical of smart logistic networks. The model has issues in identifying the dependencies over a considerably long time in dynamic environments, and training sessions are also time-consuming for the model. This CNN + BIGRU (Alzahrani and Asghar, 2023) model attracts criticisms in handling unbalanced datasets and faces problems in offering generality of results under different network conditions. This technique has reduced its performance over real-time operating conditions due to the fact that it requires extensive computational power, and it cannot effectively integrate data from multiple hyper-sources.

A model's viability in the real world is largely dependent on deployment difficulties and computing expenses. The practical application of sophisticated models may be restricted by high processing requirements, particularly in resource-constrained settings such as computing on the edge in smart logistics or Internet of Things devices. Keeping energy economy, ensuring minimal latency for immediate decision-making, and integrating with current legacy systems are some of the deployment issues. Furthermore, regular retraining of the model to accommodate changing threats may result in higher operating expenses. Resolving these issues is essential to moving from theoretical performance to real-world implementation, which calls for scalable infrastructure, effective algorithms, and lightweight models to balance usability, cost, and performance in real-world scenarios.

It addresses practical constraints by utilizing Grey System Theory to handle data imbalance, reduce complexity, and extract features efficiently. In dynamic contexts, the Grey Wolf Optimizer improves flexibility by speeding up training and fine-tuning the model. IoT and logistical networks with limited resources can benefit from real-time deployment thanks to this lightweight, scalable method that reduces latency and computing expenses. The Optimized Grey Recurrence Neuro Net Classifier effectively treats the data imbalance by using feature extraction through the grey system science. The system has enhanced computational performance with this type of architecture, and it can make better real-time decisions, besides its flexibility in a large-scale dynamic environment of smart logistics networks.

6. Conclusions

A solution was examined to address the increasing cyber challenges on smart network logistics by concentrating on best practices in supply chain management in the logistics sector. In the suggested approach, the initial data manipulation

methods are data normalizing using Z-scores and dimensionality reduction using PCA before conducting more advanced classification steps. With RFE, a model can focus on finding key characteristics since selection is improved. To demonstrate the potential of imbuing its ability to enhancement the security of supply chains with the assistance of advanced machine learning integration, the proposed technique existing ahead with accuracy (99.99%), precision (99.99%), recall (1.000%), and F1 score (99.99%) against the current methods. The system faces three main constraints, including challenges with the scale-up of big data processing, while also being sensitive to parameter adjustments and hard to interpret in real-time threat identification processes. The approach has potential limitations when it comes to fully resolving newly developing as well as complex adaptable cyber threats in evolving smart logistics settings. The future scope includes enhancing scalability to handle large-scale data, integrating real-time adaptive learning for evolving threats, improving model interpretability, and expanding its applicability to other smart network domains. Advancements in hybrid AI techniques could further optimize cyber threat detection and prevention.

6.1. Limitation

Despite its great accuracy, the suggested GWO-RNN model is highly computational because of its deep learning and iterative optimization procedures, which could make it difficult to implement on IoT devices with low resources. The model's dependence on static datasets also restricts its capacity to adjust in real time to changing cyberthreats. Practical difficulties arise when integrating with the logistics infrastructure that is already in place; further development is necessary to guarantee smooth functioning in a variety of settings.

6.2. Future work

Future research will concentrate on creating GWO-RNN variations that are lightweight and energy-efficient in order to facilitate implementation on edge and Internet of Things devices. The dynamic detection of emerging dangers will be improved by the use of adaptive methods and online learning. Furthermore, extending comparative research using transformer-based models and investigating hybrid architectures can enhance smart logistics networks' operational scalability and detection accuracy.

List of abbreviations

3GPP	3rd Generation Partnership Project
5G	Fifth-generation mobile network
ACO-RNN	Ant colony optimization–recurrent neural network
AD	Anomaly detection
AI	Artificial intelligence
AUC	Area under curve
BERT	Bidirectional encoder representations from transformers
BIGRU	Bidirectional gated recurrent unit
BoT-IoT	Botnet Internet of Things dataset
CNN	Convolutional neural network
DDoS	Distributed denial of service
DE-RNN	Differential evolution–recurrent neural network
DL	Deep learning
EDV	Eigen decomposition vector
FN	False negative
FP	False positive
GA-RNN	Genetic algorithm–recurrent neural network
GRFE	Grey recurrence feature embedding
GRG	Grey recurrence graph
GRM	Grey recurrence matrix
GRT	Grey recurrence threshold
GRNN	Grey recurrence neuro net
GRU	Gated recurrent unit
GWO	Grey wolf optimizer
GWO-RNN	Grey wolf optimizer–recurrent neural network
HL	Hidden layer
IDS	Intrusion detection system
IoE	Internet of everything
IoT	Internet of Things
LSTM	Long short-term memory
ML	Machine learning
MLP	Multilayer perceptron
OL	Output layer
ONNX	Open neural network exchange
PCA	Principal component analysis
PC	Principal component
PSO-RNN	Particle swarm optimization–recurrent neural network
RFE	Recursive feature elimination
RNN	Recurrent neural network
ROC	Receiver operating characteristic
RT	Real-time
SCM	Supply chain management
SGD	Stochastic gradient descent
sRNN	Standard recurrent neural network
SLN	Smart logistics network
SVM	Support vector machine
TN	True negative
TP	True positive
vCISO	Virtual chief information security officer

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Alanazi A, Alqahtani A, Alsubai S, and Bhatia M (2024). IoT-inspired smart theft control framework for logistic industry. IEEE Internet of Things Journal, 11(23): 38327–38336. https://doi.org/10.1109/JIOT.2024.3445884

Aljabhan B (2023). Economic strategic plans with supply chain risk management (SCRM) for organizational growth and development. Alexandria Engineering Journal, 79: 411-426. https://doi.org/10.1016/j.aej.2023.08.020

Alrumaih TN, Alenazi MJ, AlSowaygh NA, Humayed AA, and Alablani IA (2023). Cyber resilience in industrial networks: A

state of the art, challenges, and future directions. Journal of King Saud University-Computer and Information Sciences, 35(9): 101781. https://doi.org/10.1016/j.jksuci.2023.101781

Alzahrani A and Asghar MZ (2023). Intelligent risk prediction system in IoT-based supply chain management in logistics sector. Electronics, 12(13): 2760. https://doi.org/10.3390/electronics12132760

Alzahrani A and Asghar MZ (2024). Cyber vulnerabilities detection system in logistics-based IoT data exchange. Egyptian Informatics Journal, 25: 100448. https://doi.org/10.1016/j.eij.2024.100448

Ansari AK and Ujjan RMA (2024). Addressing security issues and challenges in smart logistics using smart technologies. In: Shah IA and Jhanjhi NZ (Eds.), Cybersecurity in the transportation industry: 25-48. Wiley, Hoboken, USA. https://doi.org/10.1002/9781394204472.ch2 **PMid:39496498**

Bhargava A, Bhargava D, Kumar PN, Sajja GS, and Ray S (2022). Industrial IoT and AI implementation in vehicular logistics and supply chain management for vehicle mediated transportation systems. International Journal of System Assurance Engineering and Management, 13(Suppl 1): 673-680. https://doi.org/10.1007/s13198-021-01581-2

Bravos G, Cabrera AJ, Correa C et al. (2022). Cybersecurity for industrial internet of things: Architecture, models and lessons learned. IEEE Access, 10: 124747-124765. https://doi.org/10.1109/ACCESS.2022.3225074

Cheung KF, Bell MG, and Bhattacharjya J (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. Transportation Research Part E: Logistics and Transportation Review, 146: 102217. https://doi.org/10.1016/j.tre.2020.102217

Enache GI (2023). Logistics security in the era of big data, cloud computing and IoT. Proceedings of the International Conference on Business Excellence, 17(1): 188-199. https://doi.org/10.2478/picbe-2023-0021

Fatorachian H and Kazemi H (2024). AI-enhanced fault-tolerant control and security in transportation and logistics systems: Addressing physical and cyber threats. Complex Engineering Systems, 4: 17. https://doi.org/10.20517/ces.2024.35

Ferrag MA, Ndhlovu M, Tihanyi N, Cordeiro LC, Debbah M, Lestable T, and Thandi NS (2024). Revolutionizing cyber threat detection with large language models: A privacy-preserving BERT-based lightweight model for IoT/IIoT devices. IEEE Access, 12: 23733-23750. https://doi.org/10.1109/ACCESS.2024.3363469

Junejo AK, Breza M, and McCann JA (2023). Threat modeling for communication security of IoT-enabled digital logistics. Sensors, 23(23): 9500. https://doi.org/10.3390/s23239500 **PMid:38067872 PMCid:PMC10708632**

Kumar P, Gupta GP, and Tripathi R (2021). Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for IoT networks. Arabian Journal for Science and Engineering, 46: 3749-3778. https://doi.org/10.1007/s13369-020-05181-3

Manoharan A and Sarker M (2022). Revolutionizing cybersecurity: Unleashing the power of artificial intelligence and machine learning for next-generation threat detection. International Research Journal of Modernization in Engineering Technology and Science, 4(12): 2151-2164. https://doi.org/10.56726/IRJMETS32644

Nuseir MT, Alquqa EK, Al Shraah A, Alshurideh MT, Al Kurdi B, and Alzoubi HM (2024). Impact of cyber security strategy and integrated strategy on e-logistics performance: An empirical evidence from the UAE petroleum industry. In: Alzoubi HM, Alshurideh MT, and Ghazal TM (Eds.), Cyber security impact on digitalization and business intelligence: Studies in big data: 89-108. Volume 117, Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-31801-6_6

Odimarha AC, Ayodeji SA, and Abaku EA (2024). Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies. World Journal of Advanced Science and Technology, 5(1): 026-030. https://doi.org/10.53346/wjast.2024.5.1.0030

Savic M, Lukic M, Danilovic D, Bodroski Z, Bajović D, Mezei I, Vukobratovic D, Skrbic S, and Jakovetić D (2021). Deep learning anomaly detection for cellular IoT with applications in smart logistics. IEEE Access, 9: 59406-59419. https://doi.org/10.1109/ACCESS.2021.3072916

Shkarupylo V, Alsayaydeh JAJ, Yusof MFB, Oliinyk A, Artemchuk V, and Herawan SG (2024). Exploring the potential network vulnerabilities in the smart manufacturing process of Industry 5.0 via the use of machine learning methods. IEEE Access, 12: 152262-152276. https://doi.org/10.1109/ACCESS.2024.3474861

Singh N, Lai KH, and Huang GQ (2025). Cyberintelligence for logistics: The promise and challenges of cyber-physical systems. Business Horizons. https://doi.org/10.1016/j.bushor.2025.01.001

Soare SR and Burton J (2020). Smart cities, cyber warfare and social disorder. In: Stevens T, Ertan A, Floyd K, and Pernik P (Eds.), Cyber threats and NATO 2030: Horizon scanning and analysis: 108-124. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia.

Szymonik A, Szymonik A, Dymyt M, and Wincewicz-Bosy M (2024). Cybersecurity threats and practices in the logistics industry in Poland. European Research Studies Journal, 27(3): 1108-1123. https://doi.org/10.35808/ersj/3855

Udurume M, Shakhov V, and Koo I (2024). Comparative analysis of deep convolutional neural network: Bidirectional long short-term memory and machine learning methods in intrusion detection systems. Applied Sciences, 14(16): 6967. https://doi.org/10.3390/app14166967

VanYe CM, Li BE, Koch AT et al. (2021). Trust and security of embedded smart devices in advanced logistics systems. In the Systems and Information Engineering Design Symposium (SIEDS), IEEE, Charlottesville, USA: 1-6. https://doi.org/10.1109/SIEDS52267.2021.9483779

Zhan J, Dong S, and Hu W (2022). IoE-supported smart logistics network communication with optimization and security. Sustainable Energy Technologies and Assessments, 52: 102052. https://doi.org/10.1016/j.seta.2022.102052

Zrelli I and Rejeb A (2024). A bibliometric analysis of IoT applications in logistics and supply chain management. Heliyon, 10(16): e36578. https://doi.org/10.1016/j.heliyon.2024.e36578 **PMid:39262942 PMCid:PMC11388369**