Intelligent Cyber threat detection using Optimized Deep Neural Network approach for IoT social networks

Ms. Subhalakshmi B
Research Scholar
Department of Applied Computing & Emerging Technologies
School of Computing Sciences
VISTAS, Pallavaram
Chennai, India
Email: subhalakrishnan@gmail.com

Dr. T. Kamalakannan
Professor
Department of Applied Computing & Emerging Technologies
School of Computing Sciences
VISTAS, Pallavaram
Chennai, India
Email: kkannan.scs@vistas.ac.in

Abstract-The nature of cyber threat detection in social networks of Internet of Things (IoT) is demanding in terms of high data heterogeneity, network dynamics, and changing patterns of attack. The conventional techniques of cyber threat detection usually have low accuracy, high false positive rates and do not have good scalability. The research will provide a solution to these drawbacks by stating an intelligent cyber threat detection framework that would be built using an optimized deep neural network in an IoT social network setting. First, an extensive data preprocessing and normalization process is implemented to improve quality and consistency of records of IoT traffic. After that, Improved Gorilla Troops Optimization (IGTO) is used with the help of a Decision Tree approach to select the best features to exclude the redundant and irrelevant attributes, but not to lose discriminative information. The chosen features are then categorized with the help of a deep neural network the parameters of which are optimally adjusted with the Harris Hawks Optimization (HHO) algorithm to enhance the convergence and classification. The suggested framework is tested with the CICIoT2023 data that includes various benign and malicious IoT traffic case scenarios. As experimental data shows, the given model leads to greatly enhanced detection accuracy, precision, recall, and F1 Score with lowered false-positive rates as compared to the current deep learning-based methods. The results prove that the combination of bio-inspired optimization methods and deep neural networks presents a powerful and scalable approach to intelligent cyber threat detection in dynamic environments of IoT social networks.

Keywords- Cyber threat detection, IoT, social networks, Malicious, traffic data, DL, optimization, feature selection, classification.

I. INTRODUCTION

The rapid development of the Internet of Things (IoT) has enabled traditional networks to become intelligent and interconnected ecosystems in which devices will autonomously communicate and exchange information. IoT is a paradigm shift that will allow creating a seamless connection of smart devices in healthcare, transportation, industry, and social settings and, thus, transforming a variety of industries (Hammad et al., 2025). Over the past years, a new concept has appeared, called Social IoT (SIoT), whereby IoT devices form social connections, as human social networks do, to promote service discovery, trust management, and collaborative decisions. Although Social IoT enhances scalability and automation, it also exposes the system to cyber vulnerabilities since it is hugely interconnected through heterogeneous protocols and is decentralized.

IoT also brings serious privacy and security issues, especially with the lack of sufficient resources in the device, poor authentication, and decentralized communication protocols (Mishra et al., 2022). Limitlessly increasing the number of IoT devices entering the Internet means exponentially growing the network traffic, which is an increased attack surface on the part of the opponents (Anwer et al., 2021). In Social IoT settings, cyber threats can be in different attack vectors; these are: Distributed Denial of Service (DDoS), botnets, spoofing, malware injection, and data exfiltration. These attacks take advantage of the weaknesses in the firmware of the devices, unsecured communication systems, and inadequate traffic monitoring systems. IoT traffic is dynamic and large-scale thus making it extremely difficult to detect malicious activity at early stages.

Cyber threat detection is a very important part of IoT security since it detects the abnormal operations of a system and thus allows the detection and containment of malicious operations in time (Rafique et al., 2024). Intrusion Detection Systems (IDS) are common tools used to protect IoT infrastructures by observing the traffic with suspicious behavior. Nevertheless, traditional IDS systems fail to work in the IoT setting because of the large-dimensional traffic data, dynamic attack patterns, unequal data sets, and resource limitations. Despite the excellent performance of deep learning methods in nonlinear network modeling, the conventional IDS solutions continue to experience the problem of scalability, as well as a high level of false-positive rates in IoT scenarios (Aldhaheri et al., 2024). In addition, superfluous and unwanted traffic characteristics deteriorate the quality of detection as well as raising the computation cost.

Motivated by these problems, there is an urgent necessity of a smart, scalable and optimized cyber threat detection system that should be able to perceive heterogeneous IoT traffic, and adjust to evolving attack patterns. The combination of bio-inspired optimization methods and deep neural networks can seriously improve the choice of features, tuning of parameters, and classification strength. Deep learning frameworks based on optimization improve detection accuracy, decrease false alarms and convergence time, and are appropriate in real-time IoT social network contexts. Thus, this study suggests

an improved Deep Neural Network-based smart cyber threat detection system that uses Improved Gorilla Troops Optimization (IGTO) with respect to feature selection and Harris Hawks Optimization (HHO) with regard to classifier parameters. The major contributions of this research as follows:

- To introduces a smart cyber threat detection system to suit dynamically changing Social IoT environment.
- To design a massive preprocessing and normalization pipeline to improve the quality of IoT traffic data.
- Development of a Better Gorilla Troops Optimization (IGTO) algorithm with a Decision Tree analysis to select the best features.
- Fine-tuning Deep Neural Network parameters with the help of Harris Hawks Optimization (HGO).
- The experimental validation using CICIoT2023 dataset to show better performance based on accuracy, precision, recall, F1-score and error rate.
- Delivery of a scalable and robust platform that would be applicable in real-time IoT social network security applications.

II. LITERATURE SURVEY

The recent developments in artificial intelligence have changed the mechanism of detecting cyber threats in the environments of IoT substantially. A thorough review of AI-enabled threat detection systems by Dhanushkodi and Thejas (2024) demonstrated that machine learning-based and deep learning-based approaches enhance the detection accuracy of the cybersecurity system and automate its processes. Their research placed a strong focus on adaptive AI-based structures to alleviate changing attack vectors in doing so with the issue of data imbalance, scalability, and adversarial manipulation. In spite of the general information about AI-based cybersecurity in the review, it does not present a focused optimization plan to better fit the needs of a highly dynamic environment of the IoT social networks.

Hu et al. (2025) recommended a cyber-physical system with AI enhancement in the smart infrastructure segment by incorporating Convolutional Neural Networks (CNNs) in crowd surveillance and anomaly detection. Their framework allows the real-time detection of the threat using the smart grid energy integration and the distributed CPS nodes. Although the architecture works in smart energy systems, it is more than a crowd density and physical-threat architecture but not a large-scale IoT traffic intrusion detector.

Alamro et al. (2024) presented an Advanced Ensemble Transfer Learning model (AETL-CDLPS) on Bayesian optimization to detect cyber-attacks in the context of limited resources on the IoT device. Their strategy improves low-power IoT systems performance in terms of detection with the use of transfer learning. Equally, Li et al. (2026) created NFIIoT-DTL-IDS that combines deep transfer learning with genetic algorithm (GA) optimization and ensemble-based intrusion detection of the Industrial IoT (IIoT). These models which are based on transfer learning show enhanced adaptability but are very dependent on the pretrained knowledge and are likely to be affected by domain shift problem in heterogeneous IoT social networks.

Deep learning methods that are powered by hardware have also drawn attention. To enhance the computational efficiency and real-time analysis, Nazari et al. (2025) suggested a CUDA-based hybrid CNN-DNN architecture to detect multi-class malware in the IoT networks. The article by Shafiq et al. (2025) proposed the GRIOT-FENCE and the DYNAMO-IoT algorithm of the multi-view adaptive intrusion detection to improve the credibility of consumer IoT ecosystems. Although these models increase the processing speed and flexibility, they do not exhaust the optimum choice of features and the adaptation of parameters through the sophisticated bio-inspired optimization methods.

The real-time cyber defense of hybrid AI systems is a popular subject. The study by Wang et al. (2025) suggested a hybrid RNN-LSTM model, which is optimized by Particle Swarm Optimization (PSO) to detect cyber threats on the smart city. Kong et al. (2025) designed DPI-ITD which is a dual-perspective insider threat detection model combining user-centric and behavior-centric analysis. Despite the fact that these studies increase the detection capability in certain areas, they are oriented at the behavioral or sequential modeling, but not at the optimization of the traffic at the level of the Social IoT.

IoT security research has been further developed as a result of the integration of transformer-based architectures. A model with high contextual learning capability is presented in Ferrag et al. (2024), which introduces SecurityBERT, a privacy-sensitive BERT-based model that is used in the detection of cyber threats in an IoT or IIoT network. Equally, Sana et al. (2024) used Vision Transformer (ViT) in conjunction with the conventional ML and LSTM models to boost the detection of anomaly in IoT contexts. Transformer models are also very accurate but are generally resource-intensive since they need massive computation resources, which are not possible in large, resource-constrained IoT networks.

Graph-based intrusion detection has become a research issue of promising direction. The paper by Villegas-Ch et al. (2025) suggested a dynamic graph modeling model based on Graph Neural Networks (GNNs) to address structural connections of IoT traffic. In another study, Pomsathit (2025) combined GNNs with rehearsal-based continual learning to detect adaptive Advanced Persistent Threat (APT) with the help of Wazuh EDR telemetry data. Graph-based models are very effective in modelling relational dependencies but are high computationally complex and may not scale well in real-time social networking in IoT.

Integration structures of security-edges have been explored. To provide secure transmission of data to cloud analytics, Huang (2026) suggested a Security Edge-Cloud Integration model of holographic IoT systems, which presents a combination of Security-enriched Elliptic Curve Cryptography (SECC). Inasmuch as encryption ensures a high degree of confidentiality and integrity, the framework mostly focuses on the secure communication and not the efficiency of intelligent intrusion detection.

Explainable AI (XAI) methods have been a part of the IDS structure to add interpretability. Le et al. (2023) proposed a model of blending-based attack classification that integrates the use of counterfactual explanations and LIME in enhancing transparency, and it is tested on the CICIoT2023 dataset. Gupta et al. (2024) have developed an AI-driven anomaly-detection scheme with the help of fuzzy logic and bio-inspired optimization algorithms, i.e. Intelligent Water Drop (IWD) and BiogeographyBased Optimization (BBO) to select features in the transport network of IoT. Although the optimization-based methods of feature selection enhance the efficiency of detection, they do not jointly optimize the parameters of classifiers by multi-stage bio-inspired methods.

Based on the existing literature, it can be concluded that there has been a major advancement in AI-based IoT intrusion detection based on deep learning, transfer learning, graph neural networks, transformer models, and optimization methods. Nevertheless, the bulk of literature only addresses the issue of classifier improvement, feature selection, hardware acceleration or encryption algorithm on its own. There is limited investigation that combines both bio-inspired optimization methods of feature selection and parameter optimization of the deep neural network in a Social IoT system. Thus, the current framework will fill this gap and provide better feature selection with better parameter tuning of deep neural networks via Improved Gorilla Troops Optimization (IGTO) and Harris Hawks Optimization (HHO), which will guarantee scalable, accurate, and adaptive detection of cyber threats in dynamic IoT social networks.

III. PROPOSED METHODOLOGY

The general structure of the proposed intelligent system of detecting cyber threats to the IoT social network settings is shown in figure 1. The model comprises five key stages, including IoT traffic acquisition, data preprocessing, optimal feature selection, optimized deep neural network classification, and performance evaluation. First, the traffic of IoT social networks is gathered at the interconnected smart devices, which can be sensors, wearable devices, mobile nodes, and cloud-connected systems. Data preprocessing stage will clean up the data to eliminate any missing, duplicate and noisy data and then normalize the data to bring the feature values to a common range. The action increases the stability of convergence and better performance of the classifiers.

After preprocessing, combination of Improved Gorilla Troops Optimization (IGTO) algorithm and Decision Tree approach is used for feature selection. IGTO conducts a smart search of the most topical subset of features by compromising exploration and exploitation. The Decision Tree mechanism analyzes the importance of features and directs the process of optimization in the process of choosing discriminative features. The step causes a reduction in dimensions, removal of redundancy and also reduces the overhead of computation without affecting the classification accuracy.

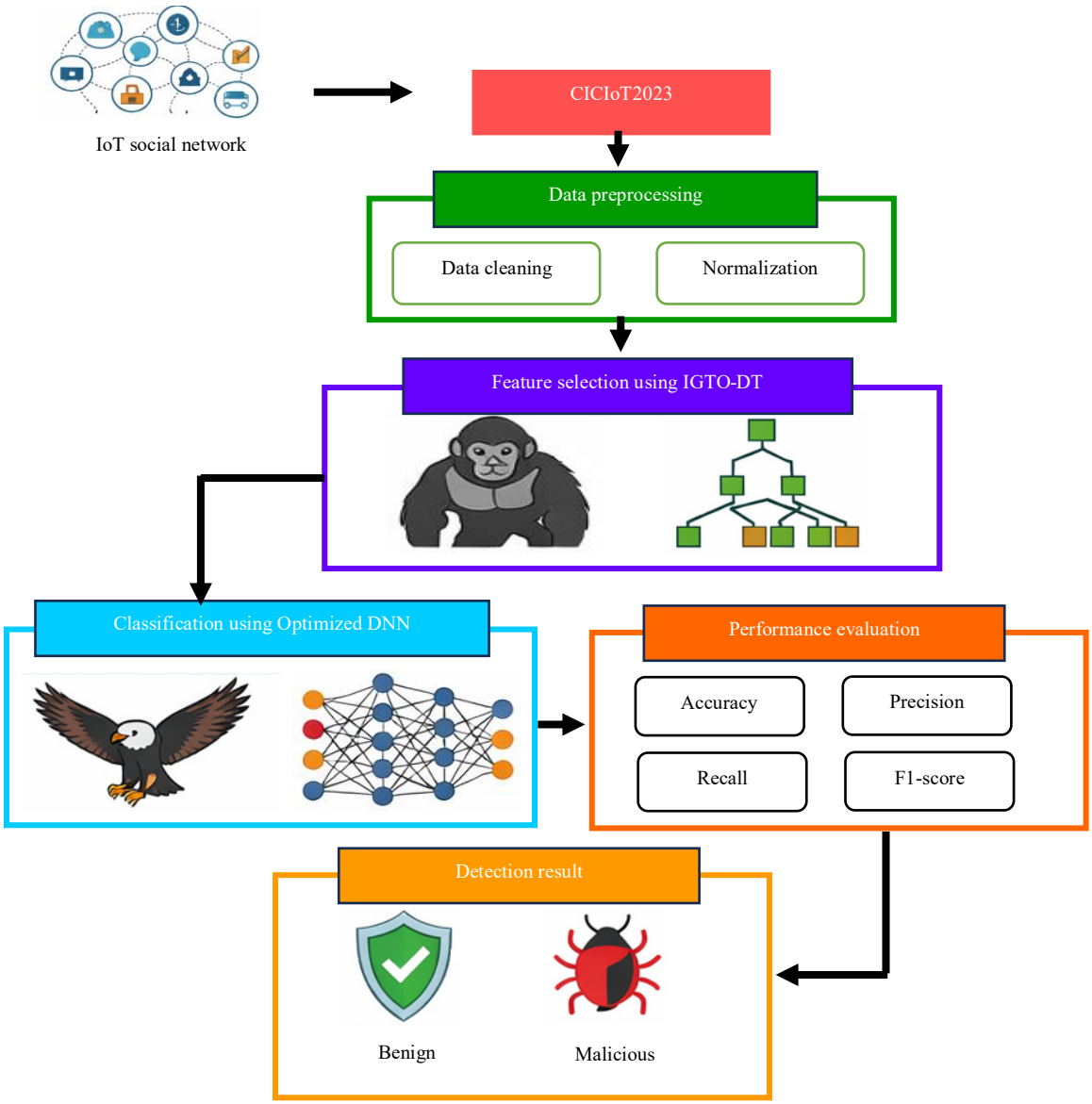

Fig. 1. Proposed architecture diagram

The optimal subset of the feature is then fed to the Optimized Deep Neural Network (DNN) module. The Harris Hawks Optimization (HHO) is applied during the given stage to optimize the DNN hyperparameters such as the learning rate, the count of hidden neurons, and weight parameters. HHO increases the rate of convergence and does not allow the model to be stuck in local minima. The optimized DNN is trained to learn complicated nonlinear patterns in IoT traffic data and conduct binary classification to differentiate between the benign and malicious activities. Lastly, the Performance Evaluation stage measures the usefulness of the proposed framework with the help of conventional evaluation metrics (Accuracy, Precision, Recall, F1-Score, and False Positive Rate (FPR)). The system produces results of the detection, which based on the output of the classification result in Benign and Malicious traffic.

A. Data preprocessing

The dataset gathered is in the form of high-dimension feature vectors that characterize network traffic instances where each record is characterized by a series of numerical features and a label indicating the class. Since the real-time IoT traffic data is heterogeneous, the raw one might contain gaps in its entries, duplicate entries, and irregularly scaled features. Thus, there is a preprocessing pipeline that is structured in such a way to increase the quality of data prior to feature selection and classification.

First, the data is converted to a structured format in the form of a matrix. The samples that are not consistent are filtered and only valid numerical feature attributes are used to learn. Then, the scaling of features is carried out to remove dominance of magnitudes among the attributes. As the values of features in the uploaded data set take up different ranges, the normalization is used to escalate all data points of different features to a common bounded range. This guarantees numerical stability, speedy convergence of the deep learning model, and avoids gradient instability in the process of optimization. Let us assuming that, input dataset can be denoted in below equation:

$$\mathcal{D} = \{(\mathbf{x}_i, y_i)\}_{i=1}^{N}$$

Herein, N total number if instances in the dataset, $\mathbf{x}_i \in \mathbb{R}^d$ feature vector of the i^{th} trial, d is the total number of numerical features y_i class label.

The complete feature matrix is written as:

$$\mathrm{X} = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1d} \\ x_{21} & x_{22} & \dots & x_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ x_{N1} & x_{N2} & \dots & x_{Nd} \end{bmatrix} \in \mathbb{R}^{N \times d}$$

A row is associated with a single record of network traffic and a column with a particular feature that has been extracted in the dataset.

Noise and inconsistent traits are identifies using statistical deviation analysis. For every attribute j, the mean μ_j and standard deviationσ_j are computed in below equations

$$\mu_j = \frac{1}{N}\sum_{i=1}^{N} x_{ij}$$

$$\sigma_j = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_{ij} - \mu_j)^2}$$

Let us assuming that, x_{ij} lies the values feature j in sample i. If feature consists missing entries, they are replaced using mean imputation is computed in below equation,

$$x_{ij}^{*} = \begin{cases} x_{ij}, & \text{if value exists} \\ \mu_j, & \text{if missing} \end{cases}$$

Here, x_{ij}^{*} denotes the updated feature values and μ_j denotes the mean of feature value. For each attribute dimension j, compute:

$$x_j^{\min} = \min_{1 \le i \le N} x_{ij}$$

$$x_j^{\max} = \max_{1 \le i \le N} x_{ij}$$

Where, x_{ij} refers the value of the j^{th}feature in the i^{th}sample, $x_j^{\min}$ denotes Minimum value of feature j and $x_j^{\max}$– Maximum value of feature j. These parameters are the minimum and maximum values of every feature dimension and they are applied to transform features to a normal numerical range.

In order to remove the imbalance in scales between features, each feature is normalized by a bounded normalization:

$$\tilde{x}_{ij} = \frac{x_{ij} - x_j^{\min}}{x_j^{\max} - x_j^{\min}}$$

The equation below provides the normalized feature matrix is denoted in below equation.

$$\tilde{\mathrm{X}} = \begin{bmatrix} \tilde{x}_{11} & \tilde{x}_{12} & \dots & \tilde{x}_{1d} \\ \tilde{x}_{21} & \tilde{x}_{22} & \dots & \tilde{x}_{2d} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{x}_{N1} & \tilde{x}_{N2} & \dots & \tilde{x}_{Nd} \end{bmatrix}$$

The final processed dataset is:

$$\widetilde{\mathcal{D}} = \{(\tilde{\mathrm{x}}_i, y_i)\}_{i=1}^{N}$$

The normalized dataset $\widetilde{\mathcal{D}}$ is the input in the next phase of feature selection and optimized deep learning classification.

B. Improved Gorilla Troops Optimization (IGTO) with Decision Tree

Once the preprocessing and normalization phase is done, an IGTO algorithm that incorporates a DT mechanism is applied to select the important features. Each gorilla of the IGTO population is initially a candidate feature subset which is represented as a binary selection vector. Decision Tree is used as an evaluation feature to assess the discriminative capacity of the chosen set of features. The DT generates a decision score that is an indication of how well the chosen features differentiate between malicious and benign traffic patterns. The IGTO algorithm builds on candidate solutions by using gorilla troop social behaviours to update exploration and exploitation behaviours. In the process of optimization, the decision measure based on DT serves as the measure of fitness which directs the search to feature subsets that will be optimal in terms of maximizing classification separability and minimizing redundancy. IGTO finds an optimal sub-set of features that will be most valuable in detecting cyber threats through a series of position updates and leader-guided learning. The population of gorillas G be denoted in below equation,

$$G = \{G_1, G_2, \dots, G_M\}$$

Herein, M denotes total number of gorilla individuals, and G_k lies the candidate solution representing feature subset. The position of every gorilla can be represented as a binary vector computed below equation:

$$G_k = [g_{k1}, g_{k2}, \dots, g_{kd}]$$

Where,

$$g_{kj} = \begin{cases} 1 & \text{feature } j \text{ selected} \\ 0 & \text{feature } j \text{ not selected} \end{cases}$$

Every gorilla defines a potential feature set where a binary value is used to denote the presence of a feature in a given set. The quality of every gorilla solution is measured in accordance with a Decision Tree information gain criterion. The entropy of dataset $\widetilde{\mathcal{D}}$ is defined as below equation,

$$H(\widetilde{\mathcal{D}}) = -\sum_{c=1}^{C} p_c \log_2(p_c)$$

Herein, C lies the number if classes, and p_c denotes the probability of class c.

Information Gain is a measure of the amount of uncertainty that has been removed upon splitting the set of data based on feature f_j.

$$IG(D, f_j) = H(\widetilde{\mathcal{D}}) - \sum_{v \in V_j} \frac{|\, D_v \,|}{|\, D \,|} H(D_v)$$

Herein, V_j denotes possible values of feature f_j, D_v refers the subset of dataset corresponding to value v, and $|\, D \,|$ lies total number samples. The function IGTO objective has the capability to classify and reduce features:

$$F(G_k) = \alpha \cdot Acc(G_k) + \beta\left(1 - \frac{|\, S_k \,|}{d}\right)$$

Let us assuming that, $Acc(G_k)$ denotes feature selection accuracy using DT from feature subsetG_k, $|\, S_k \,|$ refers to number of selected features and d total features in the dataset, and α, β are the coefficient features.

This objective-oriented balancing is one of the two goals, where one aims to maximize the detection accuracy and the other aims to reduce the size of the selected features. In exploration, gorillas walk at random in the search space denoted in below equation,

$$G_k^{t+1} = G_k^t + r_1(G_r^t - G_k^t)$$

Where, t refers to current iteration, $r_1$lies the random number in [0, 1], and G_r– randomly selected gorilla. The movement stimulates a variety of exploration of feature combinations. Closer to the best region, gorillas approach the best solution computed in below equation:

$$G_k^{t+1} = G_k^t + r_2(G_{best}^t - G_k^t)$$

This mechanism enables the algorithm to utilize the good subsets of features. The values of the gorilla positions are continuous, so to be converted into binary selections through a sigmoid function:

$$P(g_{kj}) = \frac{1}{1 + e^{-G_{kj}}}$$

$$g_{kj} = \begin{cases} 1 & \text{if } P(g_{kj}) > \tau \\ 0 & \text{otherwise} \end{cases}$$

Assuming that, $P(g_{kj})$ denotes the probability of selecting feature j, τ selection threshold. Such conversion guarantees that every gorilla solution is a valid binary set of features. After Titerations, the best gorilla solution is gained represent in below equation:

$$G^* = \arg\max_{G_k} F(G_k)$$

The subset of features that is finally chosen is

$$S^* = \{f_j \mid g_j = 1\}$$

According to the optimization outcomes of the CICIoT2023 data, the IGTO-DT algorithm identifies nineteen important attributes, such as flow time, header size, the type of protocol, the parameters of the traffic rate, the statistics of packets, and the features of interaction over time. The chosen attributes are useful in summarizing network traffic patterns and protocol dynamics that are related to malicious IoT operations like DoS, DDoS, and flood-based attacks. The selected few features enhance the learning capacity of the resultant optimized deep neural network classifier and also increases the computational efficiency.

C. Optimized deep neural network (ODNN)

Once the optimal cyber-threat features are selected, these are provided to the ODNN approach to be classified as an attack. The ODNN comprises of input, hidden layers which train hierarchical representations of the chosen traffic features. The layers carry out nonlinear transformations to obtain more profound semantic patterns that match with malicious patterns of the IoT networks. The network parameters, including weights, and biases are optimized in a bid to enhance convergence of learning and classification functionality with the help of the HHO algorithm. Here the hawks are the candidate solutions, each one of which is a neural network with the network parameters it holds. These parameters are optimized through the repeated process of simulating the cooperative hunting of Harris hawks, hence balancing the exploration and exploitation in the search. The classification loss obtained with the neural network is used to determine the fitness of each solution. In this manner of adaptation optimization, the ODNN acquires discriminative representations of cyber-attack traffic, thereby enhancing the precision and speed of convergence of the detection system.

Assuming that the chosen feature set is denoted as:

$$X = \{S^*_1, S^*_2, S^*_3, \ldots, S^*_n\}$$

Herein, X denotes the input feature vector, S_i lies the i^{th} selected feature, and n lies the total number of selected features. The deep neural network is applied to the input vector to classify it. Then result of every hidden neuron is calculated in below equation:

$$h_j = f\left(\sum_{i=1}^{n} w_{ij} X_i + b_j\right)$$

Assuming that, h_j lies the output of the j^{th} hidden neuron, w_{ij} refers weight connecting input $i$to neuron j, b_j lies the bias of neuron j, $f(.)$ denotes activation function, and X_i signifies the input feature. This step converts the input features into the higher levels feature representations. The probability of the predicted class is computed in below equation

$$y_k = g\left(\sum_{j=1}^{m} v_{jk}\, h_j + c_k\right)$$

Herein, y_k probability of predicted class k, v_{jk} denotes the weight among hidden neuron j and output neuron k, c_k denotes the bias of output neuron, m denotes number of hidden neurons and $g(.)$ signifies the activation function.

The loss that is used to measure each solution candidate is:

$$L = \frac{1}{N}\sum_{i=1}^{N} (y_i - \hat{y}_i)^2$$

Assuming that, L denotes the loss function, N number of training samples, y_i lies the actual label and $\hat{y}_i$ lies predicted label. The aim of the optimization process is to reduce this loss.

The candidate parameter vectors are each denoted as a hawk, defined below equation

$$H_i = \{w_1, w_2, \ldots, w_{dn}\}$$

Assuming that, H_i means position of i^{th}hawk, dn signifies the dimensionality of the parameter space, and w signifies the neural network parameters. The energy lost (escaping energy) E by the prey is following as:

$$E = 2E_0\left(1 - \frac{t}{T}\right)$$

Herein, E_0 implies the initial energy, T denotes maximum iterations, and t denotes the current iteration. This value is used to phase out the exploration and exploitation stages.

This equation is used to update the hawk position enabling the hawks to search various areas of the search space.

$$H_{t+1} = H_{rand} - r_1 \mid H_{rand} - 2r_2 H_t \mid$$

Assuming that, H_{t+1} denotes the updated hawk position, H_t implies the current hawk position, H_{rand} lies the randomly selected hawk, and r_1, r_2 are the random numbers in [0, 1]

The optimal parameters of the neural network are received as:

$$Cl_{out} = \begin{cases} 0, & \text{Benign IoT network traffic} \\ 1, & \text{Malicious cyber threat traffic} \end{cases}$$

The Harris Hawks Optimization algorithm is optimal in modifying the weights and biases of the deep neural network by reducing the loss of classification. The adaptive optimization algorithm enhances the convergence speed, minimizes the training error, and increases the

accuracy of detecting cyber threats in the IoT network traffic.

IV. EXPERIMENTAL RESULT ANALYSIS

The proposed cyber threat detection framework is developed in Python and tested with the CICIoT2023 Dataset, which consists of 238,687 records of IoT network traffic containing 47 features of benign and malicious activities. The advantages of the proposed model were put in contrast to the current deep learning strategies, i.e., RNN-LSTM, CNN-DNN, and GNN. The experimental findings indicate that the proposed structure is more accurate, precise, recall high F1 Score and has a low error rate compared to the current approaches. This has been largely boosted by the presence of well-chosen features and optimal neural network parameter tuning that allows the model to distinguish malicious IoT traffic and enhances the performance of cyber threat detection on the internet of things social networks.

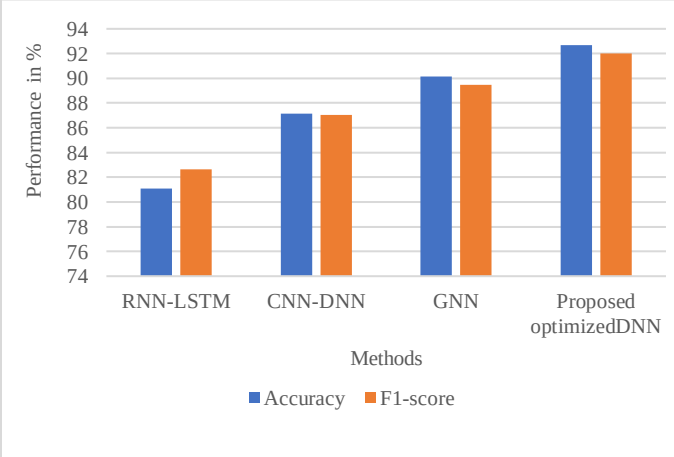

Fig. 2. Comparison of Accuracy and F1-score performance for cyber threat detection

Figure 2 shows a comparison of accuracy and F1-score of various models of cyber threat detection, such as RNN-LSTM, CNN-DNN, GNN, and the optimized deep neural network model suggested. These findings demonstrate that the RNN-LSTM model has a high accuracy of 81.06% and F1-score of 82.64%, which means it is moderately effective when detecting cyber threats. CNN-DNN is a better tackling approach (87.16% accuracy and 87.03% F1-score) and it represents features of the IoT traffic patterns in a much better way. The GNN model also achieves better detection accuracy (90.16%) and F1 Score (89.47%), since it successfully models the relationship between network traffic features. Comparatively, the suggested optimized deep neural network has the highest performance of 92.7% accuracy and 92.03% F1-score, which implies that the optimized network has a better capability to differentiate between normal and malicious IoT traffic. This is especially enabled by an optimized feature selection and parameter tuning strategy, contributing to the improvement of the learning aspect of the model and reducing the occurrence of misclassification in the detection of cyber threats.

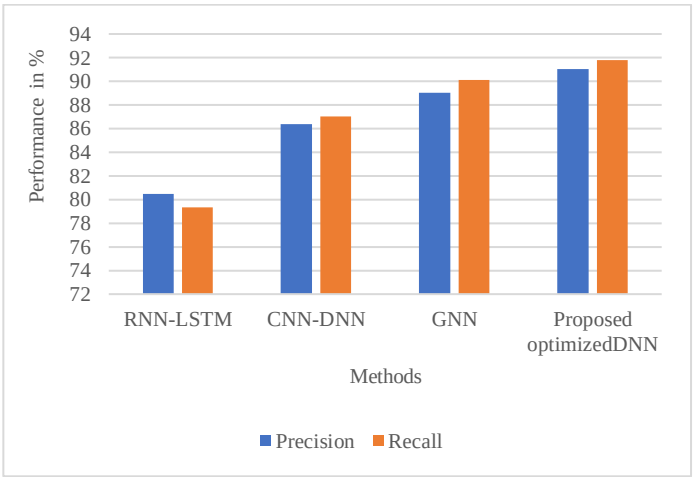

Fig. 3. Comparison of Precision and Recall performance for cyber threat detection

Figure 3 shows the precision and recall rate of detecting cyber threats with various deep learning networks and models such as Recurrent Neural Network-Long Short-Term Memory (RNN-LSTM), Convolutional Neural Network-Deep Neural Network (CNN-DNN), Graph Neural Network (GNN), and the suggested optimized deep neural network system. RNN-LSTM model has a precision of 80.47 and a recall of 79.32, which means that the model has a relatively low effectiveness in identifying malicious traffic cases correctly. The CNN-DNN model is more effective in terms of detection, as it will reach 86.35 precision and 87.03 recall that is seen to be more successful in extracting features of IoT traffic. The GNN model also improves the outcomes and reaches 89.04% precision and 90.11% recall meaning that the model has better ability to reflect complicated relationship between network features. Conversely, the suggested optimized deep neural network model is the most successful with 91.06 percent precision and 91.8 percent recall meaning that it is more competent in the ability to identify cyber threats effectively and also reduce the number of misclassifications. The success is primarily explained by the ability of selecting the features with the help of the Improved Gorilla Troops Optimization and parameter optimization with the help of the Harris Hawks Optimization that have been used to improve the classification performance of the deep neural network on the IoT social network setting.

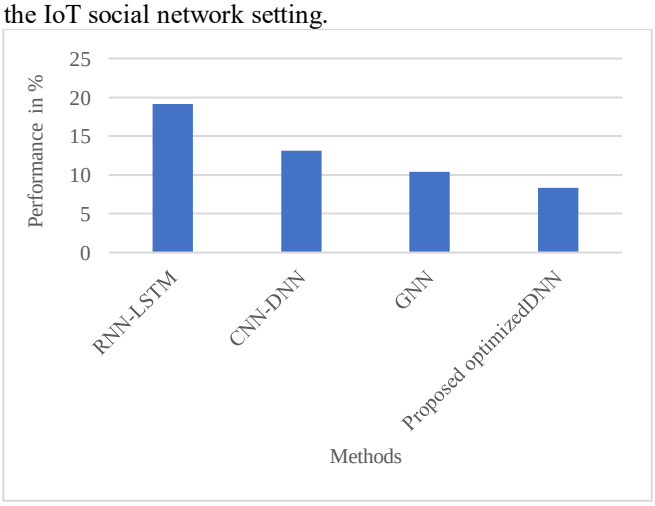

Fig. 4. Comparison of error rate performance

Figure 4 shows the error-rate performance of cyber threat detection with the help of various models, such as Recurrent Neural Network-Long Short-Term Memory (RNN-LSTM), Convolutional Neural Network-Deep Neural Network (CNN-DNN), Graph Neural Network (GNN) and the proposed optimized version of deep neural network. The RNN-LSTM model has the largest error rate of 19.14 per cent, which means that there is more misclassification between benign and malicious IoT traffic. The CNN-DNN model enhances the classifying ability as 13.14 percent error rate is lower, and it learns more characteristics of the traffic. The GNN model also reduces the error rate to 10.4 per cent, which is the capacity of the model to identify the connection between nodes within the network and traffic patterns in a better way. By comparison, the optimized deep neural network method proposed best reduces the error rate at 8.3% which represents high detection and low false classification. The reduced error rate proves that the combination of optimized feature selection with Improved Gorilla Troops Optimization with parameter tuning with Harris Hawks Optimization is very useful in increasing the accuracy of cyber threats detection in the settings of IoT social networks.

TABLE I. OVERALL PERFORMANCE

Author [Ref]	Methods	Precision (%)	Recall (%)	F1-score (%)	Accuracy (%)	Error rate (%)
T. Wang [12]	RNN-LSTM	80.47	79.32	82.64	81.06	19.14
Nazari et al. [10]	CNN-DNN	86.35	87.03	87.03	87.16	13.14
W. Villegas-Ch et al. [18]	GNN	89.04	90.11	89.47	90.16	10.4
Proposed optimized DNN		91.06	91.8	92.03	92.7	8.3

Table 1 provides the performance of various models of cyber threat detection in relation to precision, recall, F1 Score, accuracy and error rate in a general manner. The RNN-LSTM approach provides an accuracy of 81.06 with a fairly high error rate of 19.14%, which suggests that it is not able to differentiate between malicious and benign traffic of IoT devices. CNN-DNN model enhances the performance of the detection with 87.16% accuracy and 13.14% error rate. Equally, the GNN advances the performance even more by extracting the network relations to 90.16% accuracy and 10.4% error rate.

Conversely, the proposed optimized deep neural network approach is the most accurate (92.7%), the most precise (91.06%), the most recollect (91.8%), and the most F1-score (92.03 percent) with the least error rate (8.3%). This is made possible by effective feature selection by Improved Gorilla Troops Optimization and Decision Tree evaluation and parameter optimization of the deep neural network by Harris Hawks Optimization which further improves feature representation and model convergence resulting in more accurate cyber threat detection in IoT settings.

V. CONCLUSION

The study proposed a smart cyber threat detection model of Social IoT networks based on an optimized deep learning model. The suggested strategy combines Improved Gorilla Troops Optimization (IGTO) that ensures the selection of the features and Harris Hawks Optimization (HHO) that should optimize Deep Neural Network (DNN) classifier parameters. The effectiveness of the framework was tested using the CICIoT2023 data with 238,687 records and 47 features. The results of the experiment prove that the proposed optimized DNN model is well-performing with 92.7% accuracy, 91.06% precision, 91.8% recall, and 92.03%, F1-score with a low error rate of 8.3%. The proposed method is better in detection accuracy and reliability compared to current methods, including RNN-LSTM, CNN-DNN and GNN. Thus, feature selection via IGTO-based techniques and parameter optimization via HHO-based techniques are essential in improving the detection of cyber threats within the IoT environment.

REFERENCES

[1] Hammad, Atheer & Falih, May & Abd, Senan & Ahmed, aadaldeen. (2025). Detecting Cyber Threats in IoT Networks: A Machine Learning Approach. International Journal of Computing and Digital Systems. 17. 1-25.

[2] Rafique, S. H., Abdallah, A., Musa, N. S., & Murugan, T. (2024). Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection-Current Research Trends. Sensors (Basel, Switzerland), 24(6),

[3] Alyazia Aldhaheri, Fatima Alwahedi, Mohamed Amine Ferrag, Ammar Battah, Deep learning for cyber threat detection in IoT networks: A review, Internet of Things and Cyber-Physical Systems,Volume 4, 2024, Pages 110-128.

[4] Mishra S, Albarakati A, Sharma SK. Cyber Threat Intelligence for IoT Using Machine Learning. Processes. 2022; 10(12):2673. https://doi.org/10.3390/pr10122673

[5] Anwer, M., Khan, S. M., Farooq, M. U., & Waseemullah, . (2021). Attack Detection in IoT using Machine Learning. Engineering, Technology & Applied Science Research, 11(3), 7273–7278. https://doi.org/10.48084/etasr.4202

[6] K. Dhanushkodi and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," in IEEE Access, vol. 12, pp. 173127-173136, 2024, doi: 10.1109/ACCESS.2024.3493957.

[7] S. Hu, F. Zou, Y. Xiao, H. Ke and J. Wang, "Integrating Embedded Cyber-Physical Systems in Smart Energy for AI-Enhanced Real-Time Crowd Monitoring and Threat Detection," in IEEE Transactions on Consumer Electronics, vol. 71, no. 3, pp. 8363-8373, Aug. 2025, doi: 10.1109/TCE.2025.3576383.

[8] H. Alamro et al., "Modeling of Bayesian-Based Optimized Transfer Learning Model for Cyber-Attack Detection in Internet of Things Assisted Resource Constrained Systems," in IEEE Access, vol. 12, pp. 177298-177311, 2024.

[9] J. Li, M. Shahizan Othman, X. Ying, D. S. M. Hassan, H. Chen and L. Mi Yusuf, "Adaptive NetFlow IIoT Intrusion Detection With Deep Transfer Learning, Genetic Optimization, and Ensemble Methods for Network Management," in IEEE Transactions on Network and Service Management, vol. 23, pp. 681-698, 2026, doi: 10.1109/TNSM.2025.3617765.

[10] H. Nazari, A. Hussain Farooqi, B. Raza, S. Kamal, W. Nawaz and W. Abbass, "A CUDA-Accelerated Hybrid CNN-DNN Approach for Multi-Class Malware Detection in IoT Networks," in IEEE Access, vol. 13, pp. 150054-150067, 2025, doi: 10.1109/ACCESS.2025.3602723.

[11] M. Shafiq, P. Li, L. Yin, N. Alasbali and M. Mahtab Alam, "GRIOT-FENCE: Multi-View Adaptive Intrusion Detection for Trustworthy Consumer IoT Cyber Threat Analysis," in IEEE Transactions on Consumer Electronics, vol. 71, no. 4, pp. 12449-12463, Nov. 2025, doi: 10.1109/TCE.2025.3618175.

[12] T. Wang, Y. He and M. Hao, "Real-Time Cyber Threat Detection in Smart Cities Using Artificial Intelligence," in IEEE Transactions on Consumer Electronics, vol. 71, no. 2, pp. 4744-4750, May 2025, doi: 10.1109/TCE.2025.3565011.

[13] K. Kong, X. Jin, D. Liu, S. Xu, Z. Liu and G. Geng, "DPI-ITD: A Dual-Perspective Information-Driven Framework for Insider Threat Detection in IoT Systems," in IEEE Internet of Things Journal, vol. 12, no. 19, pp. 40731-40749, 1 Oct.1, 2025, doi: 10.1109/JIOT.2025.3589636.

[14] M. A. Ferrag et al., "Revolutionizing Cyber Threat Detection With Large Language Models: A Privacy-Preserving BERT-Based Lightweight Model for IoT/IIoT Devices," in IEEE Access, vol. 12, pp. 23733-23750, 2024, doi: 10.1109/ACCESS.2024.3363469.

[15] X. Huang, "Security Edge Cloud Integration of Holographic Consumer IoT: Big Data Encryption and Real-Time Threat Detection," in IEEE Transactions on Consumer Electronics, doi: 10.1109/TCE.2026.3651600.

[16] T. -T. -H. Le, R. W. Wardhani, D. S. C. Putranto, U. Jo and H. Kim, "Toward Enhanced Attack Detection and Explanation in Intrusion Detection System-Based IoT Environment Data," in IEEE Access, vol. 11, pp. 131661-131676, 2023, doi: 10.1109/ACCESS.2023.3336678.

[17] L. Sana et al., "Securing the IoT Cyber Environment: Enhancing Intrusion Anomaly Detection With Vision Transformers," in IEEE Access, vol. 12, pp. 82443-82468, 2024, doi: 10.1109/ACCESS.2024.3404778.

[18] W. Villegas-Ch, J. Govea, A. Maldonado Navarro and P. Palacios Játiva, "Intrusion Detection in IoT Networks Using Dynamic Graph Modeling and Graph-Based Neural Networks," in IEEE Access, vol. 13, pp. 65356-65375, 2025, doi: 10.1109/ACCESS.2025.3559325.

[19] A. Pomsathit, "Adaptive Detection of Advanced Persistent Threats (APT) With Graph Neural Networks and Rehearsal-Based Continual Learning on Wazuh EDR Telemetry," in IEEE Access, vol. 13, pp. 212973-212982, 2025, doi: 10.1109/ACCESS.2025.3639270.

[20] H. Gupta, S. Sharma and S. Agrawal, "Artificial Intelligence-Based Anomalies Detection Scheme for Identifying Cyber Threat on IoT-Based Transport Network," in IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 1716-1724, Feb. 2024, doi: 10.1109/TCE.2023.3329253.