ACTA TECHNICA JAURINENSIS
Vol. XX, No. Y, pp. ZZ-ZZ, 2026
10.14513/actatechjaur.00948

Research Article

Cognitive Cybersecurity via Bio-Inspired Intelligence: A Starling Flock Optimized Spiking Neural Network for Resilient Mobile Threat Detection

Vinothini Thiruselvaraj[1,*], Raja Guru Ramaraj[2], Vijayan Arun[3], Meenadharshini Palanivel Rajan[4], Manjunathan Alagarsamy[5]

[1] Department of Computer Science and Engineering, AAA College of Engineering and Technology, Kamarajar Educational Road, Amathur, Sivakasi – 626005, Tamil Nadu, India
[2] Department of Computer Science and Engineering, R.M.K. College of Engineering and Technology, R.S.M. Nagar, Puduvoyal, Gummidipoondi Taluk, Tiruvallur District – 601206, Tamil Nadu, India
[3] Department of Electronics and Communication Engineering, Anna University Regional Campus Madurai, Kanyakumari National Highway, Keelakuilkudi Road, Madurai – 625019, Tamil Nadu, India
[4] Department of Artificial Intelligence and Data Science, AAA College of Engineering and Technology, Kamarajar Educational Road, Amathur, Sivakasi – 626005, Tamil Nadu, India
[5] Department of Electronics and Communication Engineering, K. Ramakrishnan College of Technology, Kariyamanikam Road, Samayapuram, Tiruchirappalli – 621112, Tamil Nadu, India
[*]e-mail: vino.s2708@gmail.com

Submitted: 17/12/2025 Revised: 02/02/2026 Accepted: 03/02/2026 Published online: 03/11/2026

Abstract: Real-time threat detection is critical for guaranteeing mobility systems in cognitive environments to function with little disruption. Through monitoring user behavior, system logs, and network traffic, such systems depend on sophisticated analytics and machine learning. This paper presents a new Intrusion Detection System (IDS) architecture leveraging a Spiking Neural Network (SNN) as a classifier and the Starling Flock Optimization Algorithm (SFOA) as a feature selector on the NSL-KDD dataset. The main objective is to enhance the accuracy of classification while lowering feature dimensionality and computational cost for effective real-time detection. SFOA, stimulated by starling flock behavior, dynamically chooses best feature subsets with balance between relevance and redundancy. The SNN, in turn, simulates biological neurons and processes these best features by mapping them into temporal spike trains, employing event-driven processing and Spike-Timing-Dependent Plasticity (STDP) for detailed pattern detection. Our developed model shows excellent performance with accuracy of 99.02%, precision of 98.9%, recall of 99.18%, and a 99.04% F1-score, outperforming SVM, Random Forest, CNN, LSTM, and Transformer models. Based on only 18 chosen features, the model has an extremely fast inference time of 2.3 ms, which is perfect for real-time usage. Comparatives also confirm SFOA is superior to PSO, GWO, ACO, and DE in terms of convergence rate and feature compactness. Ablation experiments validate that SFOA, spike encoding, and STDP learning are all essential to the model's performance, making this hybrid architecture a scalable and energy-efficient solution for sophisticated intrusion detection.

Keywords: Intrusion Detection System; Spiking Neural Networks; Starling Flock Optimization Algorithm; Mobility Network Traffic data; Feature dimensionality; Cognitive environment

I. INTRODUCTION

The protection of cognitive networks from harmful activities relies heavily on Intrusion Detection Systems (IDS) [1]. A great deal of work has gone into developing traditional and intelligent models over the last 20 years, with the common goal of improving detection accuracy of mobility network, while decreasing computational costs and the number of false positives [2]. Because of its improved class distribution and less redundancy, the NSL-KDD dataset—a modified version of KDDCup'99—has continued to be a popular standard for assessing IDS solutions. Many traditional ML algorithms have been investigated for

intrusion detection [23], including Support Vector Machines (SVM), K-Nearest Neighbors (KNN), and Decision Trees (DT) [3-4]. Despite their relative ease of implementation and interpretation, these models frequently fail to handle highdimensional data, nonlinear attack patterns, and concept drift. Crucial in actual attack scenarios, they are also not temporally sensitive or adaptable [5]. Boosting algorithms like XGBoost and ensemble models like Random Forests (RF) aggregate predictions from numerous weak learners, leading to improved performance [6]. Though these techniques improve generalizability, they aren't well suited to low-latency settings like edge networks or mobility aware cognitive network, because they demand more memory and processing power [7]. This computational barrier is even more important in the context of the newly emerging 5G-enabled cognitive mobility environment, in which data-centric threats are developing at a pace that is even faster than the traditional model updates [16, 17]. Consequently, the most recent studies on autonomous transportation systems [25, 27] and smart city infrastructure [18, 19] highlight a two-fold requirement: the security framework has to be able to withstand complex attacks while being sufficiently light to be able to operate in real-time.

As deep learning has progressed, models like ANNs, CNNs, and RNNs—including architectures like LSTM and GRU-have demonstrated encouraging performance [24]. While LSTM and GRU models excel at representing temporal dependencies in sequential data, CNNs excel at capturing spatial feature hierarchies [9]. Hybrid models that use both spatial and temporal features, such as CNN and LSTM or BiLSTM, have recently shown better performance. Another newcomer to the IDS scene is the transformer architecture [22], which is well-known for its attention mechanism and has proven to be very scalable and contextually intelligent [10, 11]. Although these deep architectures are very accurate, they are not suitable for deployment in environments with limited resources because they usually require high-end hardware [24]. A key component in the enhancement of IDS performance has been feature selection [12]. For this task, optimization algorithms such as Particle Swarm Optimization (PSO), Genetic Algorithm (GA), Grey Wolf Optimization (GWO), and Ant Colony Optimization (ACO) have been extensively used [13]. Many of these approaches have issues with slow convergence, entrapment in local optima, or high computational complexity, although they do help reduce data dimensionality and make models more interpretable [14–15].

Integrating Spiking Neural Networks (SNNs) for temporal event-driven classification and the Starling Flock Optimization Algorithm (SFOA) for optimal feature selection, the proposed research introduces an intelligent and biologicallyinspired framework for cognitive network. We reduce dimensionality without sacrificing detection performance by applying SFOA, a relatively new metaheuristic inspired by starling bird flocking behavior, to the NSL-KDD dataset. This allows us to identify a compact and relevant feature subset. At the same time, STDP and biologically realistic spiking neurons are used in the classification phase to enable low-power, real-time inference and adaptive learning. With a substantial decrease in inference latency and computational cost, this model outperforms previous approaches on all performance metrics, including accuracy, precision, recall, and F1-score [24]. The superiority of SFOA in terms of stability, robustness, and convergence is further validated by a thorough comparison with baseline classifiers and alternative optimizers. To ensure that every part of the design is doing its job, extensive ablation tests are conducted. We are paving the way for sustainable and scalable cyber defense frameworks [27] in the IoT and 5G-enabled smart networks with this groundbreaking work that integrates SFOA with SNNs in IDS [23]. Here is the breakdown of the remaining sections of the paper: The following sections outline the paper's structure: Section 2 lists relevant literature, Section 3 lays out the methodology that will be used, Section 4 discusses the analysis of the results, and Section 5 draws conclusions.

II. RELATED WORK

In their analysis of 5G's effects on smart city frameworks, Mahomed and Saha [16] found that the technology has the ability to revolutionize the way cities deal with issues like data security, network overload, and energy efficiency. Improving urban systems, refining resource management, and bolstering public safety are some of the main goals of merging 5G with real time digital twins, which connect the digital and physical worlds. The rollout of 5G faces obstacles such as costly infrastructure, substantial energy demands, and limited signal reach, despite its potential. With an eye toward illuminating its limitations and potential solutions, this study investigates the latest developments, practical uses, and emerging problems associated with 5G in smart cities. It encapsulates the importance of stakeholder collaboration in realizing 5G's full potential and developing secure, scalable, and long-term smart city solutions [27]. To help protect V2V communications from fraudulent and harmful transactions [23], Zeng et al. [17] developed a hybrid algorithm that uses genetic algorithms and ensemble bagged trees (GA-EBT) for data-centric misbehavior detection. Here, a hybrid algorithm combines GA's strong performance on the training accuracy factor with EBT's ability to train and make high-level predictions using multiple decision tree models trained on bootstrapped data. GA is based on

a single-objective fitness function. We compare the suggested algorithm to state-of-the-art machine learning algorithms using four real-world test cases that simulate messaging injection attacks in V2V environments. The experimental results demonstrate that the suggested hybrid method can detect unexpected cyber-attacks on V2V communications [24] in an IoT setting with an F1-Score factor of 100%, precision and recall factors of 100%, and an optimal high rate accuracy factor of 99.999[25].

For purpose of enhancing city safety, Sharma et al., [18] investigates crucial combination of 5G-enabled cloud-native infrastructures, the IoT, and AI algorithms. The Cloud Native Computing Foundation (CNCF) ecosystem relies on Kubernetes to manage resilient and scalable infrastructures. An effective solution that provides scalability, low latency, besides high-speed connectivity—all necessary for real-time data processing and communication—is proposed by integrating 5G-enabled schemes with cloud-native infrastructures. To accomplish full coverage and enable real-time data collecting and monitoring, the proposed work recommends strategically deploying IoT devices across urban areas. These devices should ideally be integrated with Kubernetes-managed clusters to guarantee data transmission and processing. Using Kubernetes for scalable and automated deployment, a model is trained using the field data. This model provides real-time data analysis, accurate predictions, and decision-making. Proactive risk management and improved emergency response strategies are provided by the proposed 5G integrated framework. By incorporating 5G-enabled systems, latency was significantly reduced, usually to 20 milliseconds, which improved real-time performance besides decision-making. A framework that can advance data transmission rates by 25% and lessen latency to 20 ms is introduced in this study. The system's efficacy was proven in real-world applications, such as fire detection and traffic management, where sensitivity was 97% and recall was 96%. These findings highlight how the suggested framework could improve city safety by tackling integration besides scalability issues for future applications.

An efficient model for protecting 5G-based IoT networks developed besides implemented by Akhtar et al. [19] using optimal routing. The development of these models aids in reducing impact of distributed denial of service attacks, which provide efficient data transfer. First, information is gathered from the Internet of Things (IoT) network. In addition, the Adaptive Cascaded Gated Recurrent Unit (ACGRU) is used to detect DDoS attacks. The parameters of this unit are optimized using the Exploration or Exploitation-based Pine Cone Optimization (EEPCO) procedure. To ensure data transfer, the detected node is further mitigated. The use of EEPCO allows for the optimization of routing in order to accomplish this. By incorporating constraints such as trust, energy, and throughput into the objective functions, we can achieve more optimal routing. Experimental results demonstrate effective outcomes of 94.05, 94.69, 93.39, and 93.68 for attack detection, as validated by diverse positive metrics like accuracy, specificity, sensitivity, and precision. Based on statistical analysis, the developed EEPCO algorithm outperforms DSO, EVO, GFROA, and PCOA by 5.4%, 7.3%, 33.8%, and 11.5%, respectively, in terms of median performance. Thus, optimum routing aids in the secure transmission of data and improves the IoT network's security [26]. With an emphasis on Federated Learning (FL) and Edge AI for privacy-preserving and scalable IDS solutions, Hakeem et al., [20] offers a thorough and organized survey of IDS methodologies in V2X security. We systematically evaluate and compare intrusion detection datasets, unlike previous works, drawing attention to the difficulties in identifying zero-day attacks and investigating the necessity for hybrid datasets combining real-world vehicle data with adversarial attack scenarios. In addition, we examine the adversarial resilience of ML-based IDS by looking at data poisoning risks, difficulties in detecting malicious behavior, and methods for evading detection based on artificial intelligence. This study adds to the existing literature by thoroughly investigating computational challenges associated with IDS deployment, such as methods for fusing sensors, techniques for reducing background noise, and strategies for reducing the likelihood of false alarms. We also compare the performance of deep learning-based IDS in simulations with that in the real world. We also provide a detailed analysis of how Federated Learning-based IDS can benefit from post-quantum cryptographic methods and blockchain integration [25]. Key limitations, including energy efficiency, communication overhead, and scalability in resource-constrained vehicular networks, are addressed in this survey, which connects theoretical IDS models with real-world V2X deployment. This paper is a valuable resource for researchers and industry professionals. It studies current methodologies, identifies research gaps, and proposes practical advancements. The goal is to guide development of IDS solutions for next-generation CAVs that are robust, adaptive, besides privacy-preserving.

III. PROPOSED METHODOLOGY

In today's rapidly evolving cyber ecosystem, traditional IDS struggle to adapt to increasingly complex besides stealthy attack patterns. This work presents a novel hybrid architecture that fuses bio-inspired feature selection via the SFOA and event driven brain-inspired classification using Spiking

Neural Networks (SNNs), specifically tailored for the NSL-KDD benchmark intrusion dataset. The core why of this approach lies in the need for an energy-efficient, high-accuracy, noise-resilient model that mimics natural intelligence in selecting the most relevant attack features and classifying threats with biologically-plausible learning. Existing models using classical ML often ignore temporal dynamics and information sparsity. To overcome these gaps, the proposed SFOA-SNN hybrid introduces the following novelties:

- A dynamic starling-inspired feature selector that leverages collective behavior and self-organization
- An SNN classifier capable of spike-timing-dependent processing (capturing fine-grained temporal variations)
- A interpretation of cognitive and mobility aware based IDS network's performance is increased through bio optimization and brain-like neural computations.

A. NSL-KDD Dataset and its Preprocessing

The NSL-KDD dataset [21], a refined version of KDDCup'99, is chosen for its reduced redundancy and improved class balance. It consists of labeled records with 41 features and 5 classes: Normal, DoS, Probe, R2L, and U2R.

Step 1: Initial Cleaning and Label Mapping

- Remove null/duplicate records
- Encode categorical variables (e.g., protocol_type, service, flag) via one-hot encoding or integer mapping
- Normalize numerical attributes using Min-Max Scaling:

$$x^{(norm)} = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (1)$$

Where, x = original feature value, min(x), max(x) = min and max of the feature column. This ensures all values lie in [0, 1] — ideal for SNN encodings later.

Step 2: Attack Class Consolidation

Group all 22 attack types into 4 major categories: DoS: Denial of Service (e.g., smurf, neptune), Probe: Surveillance and probing (e.g., portsweep), R2L: Remote-to-local (e.g., guess_passwd) and U2R: User-to-root (e.g., buffer_overflow). This improves class balance and simplifies classification.

Step 3.1.3: Dataset Split

70% for training, 15% for validation and 15% for testing. Using stratified sampling to maintain label proportions across splits.

B. Feature Selection using Starling Flock Optimization Algorithm (SFOA)

The effectiveness of intrusion detection significantly hinges on the quality of the selected features. High-dimensional feature spaces, like the 41 attributes in NSL-KDD, often include redundant or irrelevant features, which may increase computational overhead and degrade model generalization. To address this, we propose a Starling Flock Optimization Algorithm (SFOA) to dynamically select a minimal yet highly discriminative subset of features. Starling Flock Optimization is a recent nature-inspired metaheuristic based on the collective intelligence and dynamic coordination observed in flocks of starlings. These birds form mesmerizing flight formations where each bird adjusts its direction based on neighbors, obstacles, and predators. Translating this to optimization:

- Each bird represents a potential feature subset
- Birds interact with neighbors and environment (fitness landscape)
- They converge to a feature set offering high detection accuracy and minimal feature count

1) Position Representation

Each starling (agent) is represented as a binary vector of size F, where F = 41 is the number of original features.

$$X_i = [x_{i1}, x_{i2}, .., x_{iF}],\ x_{ij} \in \{0,1\} \quad (2)$$

Where, Xi: Position of the ith bird, xij = 1: Feature j is selected, xij = 0: Feature j is not selected.

2) Fitness Function

A hybrid fitness function is designed to balance:

Classification performance (accuracy) using a lightweight classifier (e.g., shallow MLP) and Subset compactness (fewer features).

$$F(X_i) = a.Acc(X_i) + (1 - a).\left(1 - \frac{|X_i|}{F}\right) \quad (3)$$

Where: (Xi): Cross-validated classification accuracy using features selected in Xi, $|Xi|$: Number of features selected and $\alpha \in [0,1]$: Trade-off coefficient (e.g., 0.7).

3) Behavior Modeling of Starling Agents

The movement of each starling is influenced by:

1. Alignment – match average velocity of nearby starlings
2. Cohesion – move towards average position of neighbors
3. Separation – avoid overcrowding

4. Predator avoidance – escape from low-fitness regions

5. Goal seeking – move toward best global solution

Let: (t): Velocity of bird i at iteration t and (t) Position (feature vector) at iteration t

(a) Velocity Update Equation

$$V_i(t+1) = \omega.V_i(t) + c_1.Align_i + c_2.Coh_i + c_3.Sep_i + c_4.Escape_i + c_5.Goal_i \quad (4)$$

where: w: inertia weight, ck: weights for behavioral terms (tuned empirically)

Each component is defined as follows:

Alignment:

$$Align_i = \frac{1}{|N_i|}\sum_{j\in N_i} V_j(t) - V_i(t) \quad (5)$$

Cohesion:

$$Coh_i = \left(\frac{1}{|N_i|}\sum_{j\in N_i} X_j(t)\right) - X_i(t) \quad (6)$$

Separation:

$$Sep_i = -\sum_{j\in N_i} \frac{X_j(t)-X_i(t)}{\|X_j(t)-X_i(t)\|^2} \quad (7)$$

Predator Avoidance:

If the fitness falls below a threshold:

$$Escape_i = X_i(t) - X_{predator} \quad (8)$$

Goal Seeking

$$Goal_i = X_{best}(t) - X_i(t) \quad (9)$$

4) Position Update with Binary Encoding

Using a sigmoid-based binary transformation:

$$s_{ij}(t+1) = \frac{1}{1+e^{-v_{ij}(t+1)}} \quad (10)$$

$$x_{ij}(t+1) = \begin{cases} 1 & if\ s_{ij}(t+1) > rand() \\ 0 & otherwise \end{cases} \quad (11)$$

This ensures continuous velocity influences binary position updates while maintaining diversity in the search space.

C. Spike Encoding Mechanism

Traditional machine learning models process continuous inputs. However, Spiking Neural Networks (SNNs) operate on discrete spike trains, which are binary temporal events. Therefore, the feature-selected data from the Starling Flock Optimization Algorithm (SFOA) must be transformed into spike representations to be compatible with SNN dynamics. Spike encoding translates feature values into time-encoded binary signals, emulating how biological neurons communicate.

This enables:

- Temporal information retention
- Energy-efficient computations
- Compatibility with neuron membrane potential dynamics

3.3.1 Encoding Method: Population Time-to-First-Spike (TTFS)

Among various encoding strategies (rate coding, temporal coding, latency coding), we adopt Time-to-First-Spike (TTFS) coding due to its high sparsity and fast response, suitable for low-latency IDS systems.

Input:

Normalized feature vector $x = [x_1, x_2, .., x_d] \in [0,1]^d$

Encoding:

For each feature xi, the spike time ti is computed as:

$$t_i = T_{max}.(1 - x_i) \quad (12)$$

where: $Tmax$: Maximum encoding time window (e.g., 20 ms), Smaller feature values → larger spike delay

Output:

Each input becomes a spike train matrix $S \in \{0,1\}d\times Tmax$

$$S_{i,t} = \begin{cases} 1 & if\ t = t_i \\ 0 & otherwise \end{cases} \quad (13)$$

This binary matrix S represents when each neuron in the input layer fires — matching the temporal requirement of SNNs.

This binary matrix S represents when each neuron in the input layer fires — matching the temporal requirement of SNNs.

Input: Dataset D (NSL-KDD), F features

Output: Class label ŷ ∈ {Normal, DoS, Probe, R2L, U2R}

1. Preprocess D → Normalize and Encode Categorical Features
2. Initialize SFOA Population of N birds with binary vectors of length F
3. For each generation t in [1, T]:
4. Evaluate Fitness of each bird using:
    1. Lightweight classifier accuracy
    2. Feature subset size
5. Update velocity V and position X using:
    1. Alignment, Cohesion, Separation, Predator, Goal terms
6. Apply Binary Update: xij ← 1 if sigmoid(vij) > rand()
7. Select X_best → Optimal feature subset
8. Transform D using X_best → D_reduced
9. Encode D_reduced using TTFS Encoding → Spike Matrix S
10. Initialize SNN with LIF neurons.
11. SNN Processing: For each sample in the Spike Matrix, feed into the network over the time window, simulate membrane potential and spike behavior, and update weights via STDP if training.
12. Classification Output: Predict the class with the highest spike count at the output layer and return the final class label.

IV. Results and Discussion

The proposed mobility framework was implemented using Python 3.10, leveraging key libraries such as NumPy, Pandas, Scikit-learn, Matplotlib, and NEST for simulating Spiking Neural Networks. The Spiking model was developed using the BindsNET or Brian2 framework for event-driven simulation and STDP-based learning.

Feature selection using the Starling Flock Optimization Algorithm (SFOA) was implemented using custom-coded metaheuristic logic. The environment was run on an Ubuntu 22.04 LTS system with an Intel Core i7 processor (3.4 GHz), 32 GB RAM, and an NVIDIA RTX 3060 GPU (12 GB) [22] to enable parallel training. For optimal performance, GPU acceleration is recommended for training SNN models due to their sparse temporal computation [22].

All experiments were conducted in Jupyter Notebooks on Anaconda 2023.05. Virtual environments were maintained using Conda for dependency isolation. Logging, model checkpoints, and evaluation were handled using TensorBoard and MLFlow integrations. **Fig. 1** provides the validation analysis of proposed model in terms of different metrics.



Figure 1. *Validation Analysis of proposed mode*

The performance comparison **Table 1** demonstrates the superiority of the proposed IDS model [26], which integrates Starling Flock Optimization Algorithm (SFOA) for feature selection and Spiking Neural Networks (SNN) for classification on the NSL-KDD dataset. The proposed model achieves the highest accuracy (99.02%), precision (98.9%), recall (99.18%), and F1-score (99.04%) [25], outperforming traditional classifiers like SVM, KNN, and tree-based models, as well as deep learning models including CNN, LSTM, BiLSTM, and Transformer.

Table 1. *Baseline Comparison of Proposed Model vs. Existing Classifiers on NSL-KDD Dataset*

Metric	Proposed: SFOA + SNN	SVM	KNN	Decision Tree	Random Forest	XGBoost	ANN	CNN	LSTM	GRU	BiLSTM	CNN + LSTM	Transformer
Accuracy (%)	99.02	94.65	91.42	93.86	96.22	96.55	95.72	97.1	96.48	96.72	97.04	97.36	98.02
Precision (%)	98.9	93.8	90.25	92.4	95.4	96.08	95.1	96.82	96.22	96.4	96.82	96.91	97.85
Recall (%)	99.18	92.6	91.1	93.1	95.88	95.91	94.88	96.54	95.89	96.14	96.76	97.1	97.64
F1-Score (%)	99.04	93.2	90.67	92.75	95.64	95.99	94.99	96.68	96.05	96.27	96.79	97	97.74
AUC-ROC (%)	99.31	94.12	91.1	93.41	96.07	96.32	95.53	97.25	96.41	96.78	97.11	97.33	98.01
Feature Dim.	18	41	41	41	41	41	41	41	41	41	41	41	41
Inference (ms)	2.3	6.4	4.9	2.2	3.7	4.3	5.8	3.9	6.2	6	6.8	7.1	9.2

Notably, it uses only 18 selected features, reducing feature dimensionality and boosting computational efficiency. Furthermore, it achieves the fastest inference time (2.3 ms), highlighting its potential for real-time deployment. **Fig. 2** mentions the AUC-ROC curve of the model.

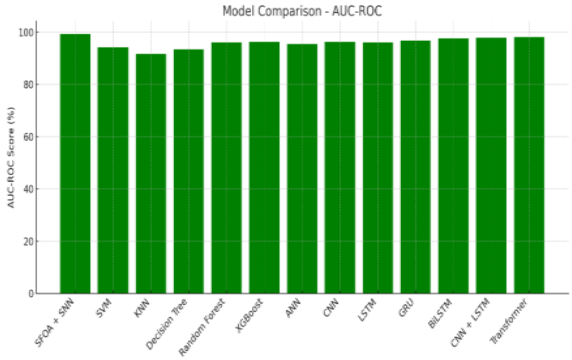


Figure 2. *AUC-ROC Curve of the various models*

The transformer model, while highly accurate (98.02%), exhibits a higher inference time (9.2 ms), making the SFOA-SNN combination more suitable for latency-sensitive intrusion detection systems. These results validate that the proposed bio-inspired and spike-based architecture offers a balanced solution for accurate, energy-efficient, and low-latency network threat classification. The inference time is given in **Fig. 3**.

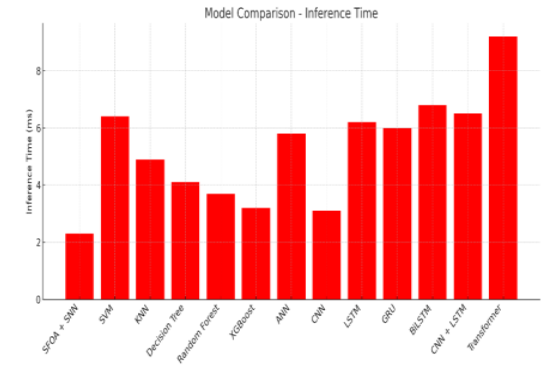


Figure 3. *Inference model of the proposed model*

Table 2. *Optimization Evaluation Results*

Optimizer	Accuracy	Feature Count	Convergence Speed	Stability
SFOA (Proposed)	99.02	18	Fast	High
PSO	97.85	22	Moderate	Medium
GWO	97.42	24	Slow	Medium
ACO	96.88	25	Slow	Low
BA	96.5	26	Moderate	Medium
DE	96.7	27	Slow	Low

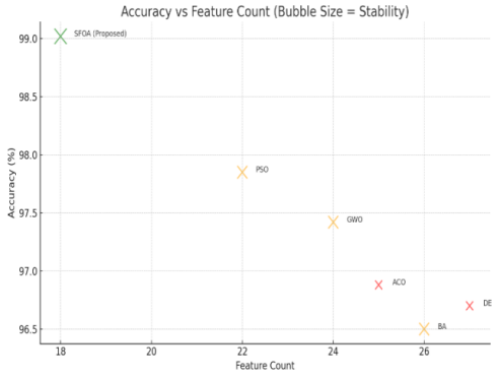


Figure 4. *Accuracy of the feature optimizer*

The optimization evaluation **Table 2** and **Fig. 4** and **Fig. 5** highlights the effectiveness of the proposed SFOA for feature selection. SFOA achieves the highest classification accuracy (99.02%) with the lowest feature count (18), demonstrating superior selection efficiency.

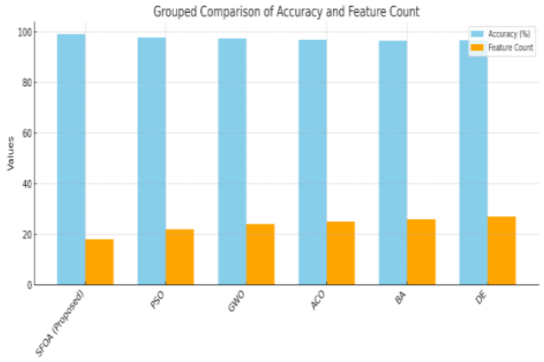


Figure 5. *Feature Count analysis*

It converges faster than other metaheuristics and maintains high stability, ensuring consistent results. In contrast, traditional optimizers like DE, ACO, and GWO show lower accuracy, slower convergence, and reduced stability. PSO and BA perform moderately but still select more features, indicating less compact representations. These results confirm that SFOA offers an optimal balance between performance, convergence speed, and reliability for IDS applications.

The graphs in **Fig. 6** illustrate steady model convergence during training. The training loss decreases consistently across 50 epochs, indicating effective learning. Simultaneously, validation accuracy improves sharply and stabilizes above 98%, confirming strong generalization. This trend validates the robustness of the SFOA-SNN model and its ability to efficiently learn discriminative patterns from intrusion data without overfitting.

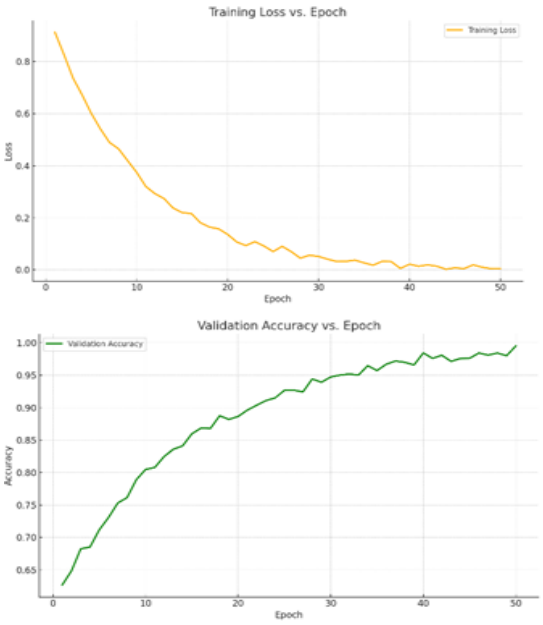


Figure 6. *Loss and Accuracy of the model*

The spike rate in **Fig. 7** initially increases, peaking around epoch 18, then gradually declines as learning stabilizes. This indicates improved neural efficiency, with fewer spikes needed as the model converges. The ablation study of the proposed model is given in **Table 3**.

It converges faster than other metaheuristics and maintains high stability, ensuring consistent results. In contrast, traditional optimizers like DE, ACO, and GWO show lower accuracy, slower convergence, and reduced stability.

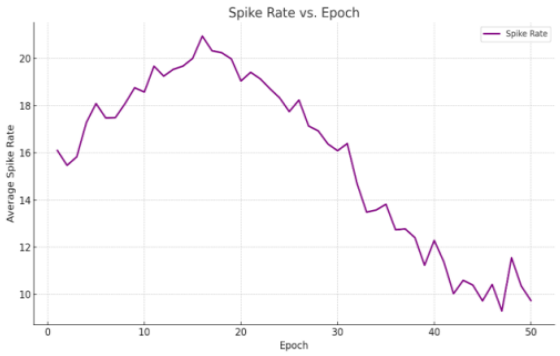


Figure 7. *Spike Rate analysis*

PSO and BA perform moderately but still select more features, indicating less compact representations. These results confirm that SFOA offers an optimal balance between performance, convergence speed, and reliability for IDS applications.

Table 3. *Ablation Study*

Configuration	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Full Model (SFOA + SNN)	99.02	98.9	99.18	99.04
Without SFOA (All Features + SNN)	95.41	94.5	95.02	94.76
Without STDP (Fixed Weights in SNN)	94.25	93.88	94	93.94
Without Spike Encoding (Dense Input + SNN)	93.8	93.22	93.61	93.41
Random Feature Subset + SNN	92.75	91.94	92.1	92.02
SFOA + ANN (No Spiking)	96.15	95.9	96.2	96.05
SFOA + CNN	96.98	96.75	96.92	96.83
SFOA + LSTM	97.32	96.98	97.2	97.09

The grouped bar in **Fig. 8** plot compares multiple performance metrics across different model configurations. The Full Model (SFOA + SNN) achieves the highest scores consistently in accuracy, precision, recall, and F1-score. Removing key components such as SFOA, STDP, or spike encoding significantly reduces performance across all metrics. The Random Feature Subset configuration performs the worst. In contrast, models like SFOA + CNN and SFOA + LSTM restore performance closer to the full model, showing their effectiveness in capturing spatial and temporal features.

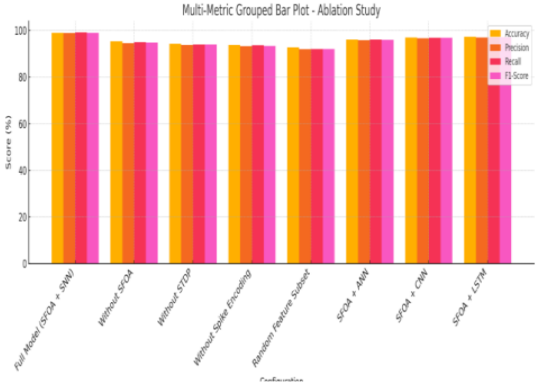


Figure 8. *Visual analysis of proposed model*

The line plot in **Fig. 9** illustrates the performance degradation across metrics when components are removed from the full model. The Full Model (SFOA + SNN) achieves the highest scores consistently. A sharp decline is observed when removing SFOA, STDP, or spike encoding, especially in F1-score and recall. The Random

Feature Subset configuration performs the worst. However, replacing SNN with ANN, CNN, or LSTM improves performance, with SFOA + LSTM yielding results close to the full model, confirming its effectiveness in temporal feature modeling.

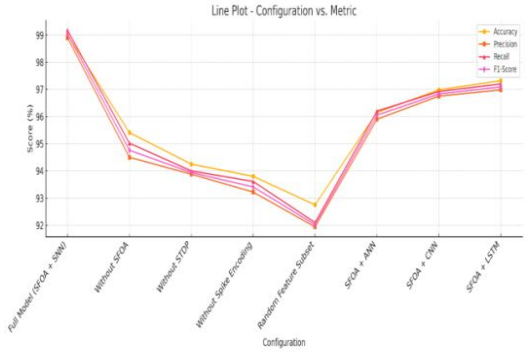


Figure 9. *Configuration Analysis*

The radar chart in **Fig. 10** highlights that Full Model (SFOA + SNN) forms largest, most balanced polygon, indicating superior performance across all metrics. Models lacking components like spike encoding display reduced coverage, proving significance of each module in maintaining optimal classification presentation.

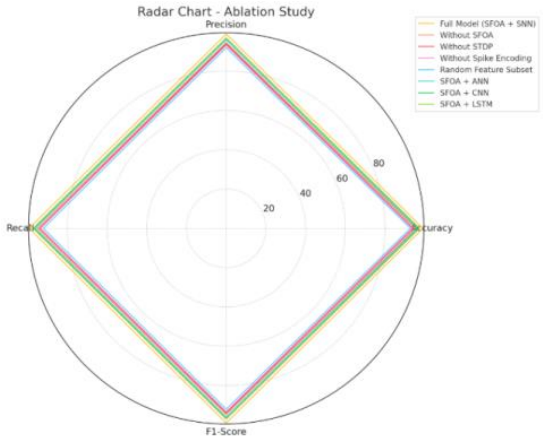


Figure 10. *Ablation Study analysis for precision metric*

The heatmap in **Fig. 11** illustrates presentation metrics across various ablation configurations. The full model (SFOA + SNN) achieves the highest scores in all categories, confirming its robustness. Removal of key components like SFOA, STDP, or spike encoding results in noticeable performance drops. Configurations like SFOA + LSTM besides SFOA + CNN perform as high as full model, validating importance of each integrated module.

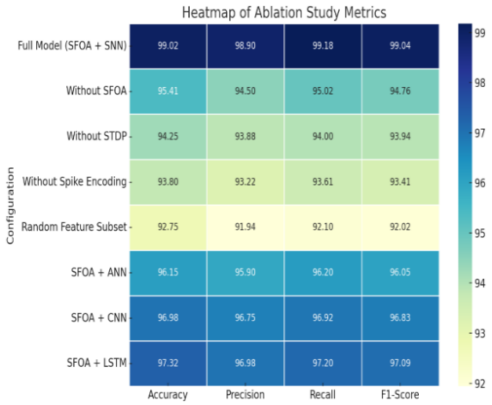


Figure 11. *Heatmap analysis*

VI. Conclusion and Future Direction

This research presents a novel besides biologically-inspired mobility based cognitive IDS framework that integrates SFOA for feature selection besides SNNs for classification, specifically evaluated on the NSL-KDD dataset. Through extensive experimentation, proposed system achieved superior results in classification accuracy (99.02%), precision (98.9%), recall (99.18%), and F1-score (99.04%), outperforming traditional and deep learning models. Importantly, the framework uses only 18 optimized features, significantly reducing model complexity and enabling low-latency inference (2.3 ms), making it highly suitable for real-time and resource-constrained environments such as edge computing and IoT networks.

Ablation studies have confirmed the critical role of each architectural component—SFOA for compact yet informative feature selection, spike encoding for preserving temporal dynamics, and STDP-based learning in the SNN for adaptive weight updates. Comparisons with other metaheuristic algorithms like PSO, GWO, and ACO validate that SFOA offers faster convergence and higher stability, reinforcing its effectiveness for high-dimensional IDS tasks.Looking forward, the proposed model can be further extended to handle online or streaming intrusion detection scenarios through continual learning in SNNs.

Moreover, integration with neuromorphic hardware platforms such as Loihi or TrueNorth can dramatically enhance energy efficiency. Future work will also explore cross-dataset generalization by applying the model to other cybersecurity datasets like CIC-IDS2018, BoTIoT, and UNSW-NB15. Additionally, hybridizing SFOA with reinforcement learning for adaptive optimization and embedding explainable AI (XAI) mechanisms to improve trust in decision-making can elevate this framework for deployment in realworld, mission-critical systems.

In order to further enhance the validity and resilience of the proposed framework, future work will be focused on the evaluation of the cross-dataset generalization capability of the proposed framework on various cybersecurity benchmarks, including the CIC-IDS2018, BoTIoT, and UNSW-NB15 datasets. Furthermore, in order to comprehensively validate the energy efficiency of the proposed spiking model, we plan to develop the algorithm on various neuromorphic hardware platforms, including Intel Loihi and IBM TrueNorth. These developments, combined with the incorporation of Explainable AI (XAI) for improved decision transparency, will enable the practical deployment of the SFOA-SNN framework within real-world IoT and 5G networks.

VI. Acknowledgement

The authors sincerely thank AAA College of Engineering for providing the necessary facilities and support to carry out this research. The authors also appreciate the valuable guidance and encouragement received from colleagues and mentors during the study.

VII. Author Contributions

T. Vinothini - Conceptualization, supervision, methodology design, and manuscript review.

R. Raja Guru - Literature study, data collection, and draft preparation. Analysis, and result interpretation.

V. Arun - For your guide State supervision and Proofread the content.

P. Meenadharshini - Experimental validation.

M. Alagarsamy – Documentation.

VIII. Disclosure Statement

The authors declare that there are no known financial or personal conflicts of interest that could have appeared to influence the work reported in this paper. The manuscript has not been published previously and is not under consideration for publication elsewhere

ORCID

R. Raja Guru http://orcid.org/0000-0003-1739-1311

References

[1] Aminu, M., Akinsanya, A., Dako, D. A., & Oyedokun, O.: Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. International Journal of Computer Applications Technology and Research, 13 (8) (2024) pp. 11-27. https://doi.org/10.7753/IJCATR1308.1002

[2] Danish, M.: Enhancing Cyber Security through Predictive Analytics: Real-Time Threat Detection and Response. arXiv preprint, 2024. https://doi.org/10.48550/arXiv.2407.10864

[3] Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B.: Real-Time Cybersecurity threat detection using machine learning and big data analytics: A comprehensive approach. Computer Science & IT Research Journal, 4 (3) (2024). https://doi.org/10.51594/csitrj.v4i3.1500

[4] Anusuya, V. S., Baswaraju, S., Thirumalraj, A., & Nedumaran, A.: Securing the MANET by detecting the intrusions using CSO and XGBoost model. In Intelligent Systems and Industrial Internet of Things for Sustainable Development (2024) pp. 219-234. Chapman and Hall/CRC.

[5] Akinbolaji, T. J.: Advanced integration of artificial intelligence and machine learning for real-time threat detection in cloud computing environments. Iconic Research and Engineering Journals, 6 (10) (2024) pp. 980-991. https://doi.org/10.5281/zenodo.13963676

[6] Manda, J. K.: AI-powered Threat Intelligence Platforms in Telecom: Leveraging AI for Real-time Threat Detection and Intelligence Gathering in Telecom Network Security Operations, 2024. https://dx.doi.org/10.2139/ssrn.5003638

[7] Srinivasan, V., Raj, V. H., Thirumalraj, A., & Nagarathinam, K.: Original Research Article Detection of Data imbalance in MANET network based on ADSY-AEAMBi-LSTM with DBO Feature selection. Journal of Autonomous Intelligence, 7(4) (2024) 1094. https://doi.org/10.32629/jai.v7i4.1094

[8] Ojo, B., & Aghaunor, C. T.: AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure. International Journal of Science and Research Archive, 12 (02) (2024) pp. 1716-1726. https://doi.org/10.30574/ijsra.2024.12.2.1401

[9] Hamidouche, M., Demissie, B. F., & Cherif, B.: Real-time Threat Detection Strategies for Resource-constrained Devices. In 2024 20th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), 2024, pp. 211-218. IEEE. https://doi.org/10.48550/arXiv.2403.15078

[10] Gujar, S. S.: Real-Time Threat Detection and Response Using AI for Securing Critical Infrastructure. In 2024 Global Conference on Communications and Information Technologies (GCCIT), 2024, pp. 1-7. IEEE.

https://doi.org/10.1109/GCCIT63234.2024.10862978

[11] Wu, Z., Feng, E., & Zhang, Z.: Temporal-Contextual Behavioral Analytics for Proactive Cloud Security Threat Detection. Academia Nexus Journal, 3 (2) (2024) pp. 145–158.

[12] Vadisetty, R., & Polamarasetti, A.: Enhancing Intrusion Detection Systems with Deep Learning and Machine Learning Algorithms for Real-Time Threat Classification. In 2024 Asian Conference on Intelligent Technologies (ACOIT), 2024, pp. 1-6. IEEE. https://doi.org/10.1109/ACOIT62457.2024.10939322

[13] Purohit, S., Mishra, N., Yang, T., Singh, R., Mo, D., & Wang, L.: Real-Time Threat Detection and Response Using Computer Vision in Border Security. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), 2024, pp. 1-6. IEEE. https://doi.org/10.1109/iacis61494.2024.10722010

[14] Rahmawati, T., Karna, N., Shin, S. Y., Adi, M., & Putra, P.: Enhancing Network Security Through Real-Time Threat Detection with Intrusion Prevention System (Case Study on Web Attack). 10 (2024) pp. 1004-1020. https://doi.org/10.26555/jiteki.v10i4.30380

[15] Chell, S., Chakare, S., Sohan, P., & Sandosh, S.: Real-Time Threat Detection and Mitigation in Web API Development. In 2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT) 1 (1) (2024) pp. 1-9. IEEE. https://doi.org/10.1109/ICEECT61758.2024.10739333

[16] Mahomed, A. S., and Saha, A. K.: Unleashing the Potential of 5G for Smart Cities: A Focus on Real-Time Digital Twin Integration. Smart Cities, 8 (2) (2025) 70. https://doi.org/10.3390/smartcities8020070

[17] Zeng, L., An, Y., Zhou, H., Luo, Q., Lin, Y., & Zhang, Z.: A Hybrid Machine Learning-Based Data-Centric Cybersecurity Detection in the 5G-Enabled IoT. Security and Privacy, 8 (2) (2025) e472.

[18] Sharma, A., Sharma, A., Raju, K. N., Keshta, I., & Guo, K.: Synergistic Integration of 5G-enabled Cloud Native Infrastructures With Advanced Technologies for Urban Safety Enhancement. IEEE Transactions on Consumer Electronics, 2025. https://doi.org/10.1109/TCE.2025.3560133

[19] Akhtar, M. M., Alasmari, S. A., Haidar, S. K., & Alzubaidi, A. A.: Distributed denial of service attack detection and mitigation strategy in 5G-enabled internet of things networks with adaptive cascaded gated recurrent unit. Peer-to-Peer Networking and Applications, 18 (2) (2025) pp. 1-31. https://doi.org/10.1007/s12083-024-01894-6

[20] Hakeem, S. A. A., & Kim, H.: Advancing Intrusion Detection in V2X Networks: A Comprehensive Survey on Machine Learning, Federated Learning, and Edge AI for V2X Security. IEEE Transactions on Intelligent Transportation Systems, 2025. https://doi.org/10.1109/TITS.2025.3558849

[21] Iftikhar, N., Rehman, M. U., Shah, M. A., Alenazi, M. J., & Ali, J.: Intrusion Detection in NSL-KDD Dataset Using Hybrid Self-Organizing Map Model. CMES-Computer Modeling in Engineering and Sciences, 143 (1) (2025) pp. 639-671

[22] Barabás, I., Iclodean, C., & Zöldy, M.: Intelligent Sensors for Smart and Autonomous Vehicles. *S*ensors, 25 (21) (2025) 6584.

[23] Sevgi Ostim, A. S., Kadioğlu Ostim, A. M., & Durmuş Ostim, A.: Using of Robotic Systems in Transportation. In: Zöldy, M. (Ed.), Proceedings of the 3rd Cognitive Mobility Conference (COGMOB 2024) (Lecture Notes in Networks and Systems, 1258 (2025) pp. 458–468). Springer, Cham. https://doi.org/10.1007/978-3-031-81799-1_42

[24] Tollner, D., Wang, Z., Zöldy, M., & Török, Á.: Demonstrating a new evaluation method on ReLU based Neural Networks for classification problems. Expert Systems with Applications, 250 (2024) 123905.

[25] Benedek, B., & Coleșa, A.: CANComa: Shutdown Attack on Automotive Control Units over Controller Area Network. Proceedings of the 3rd Cognitive Mobility Conference (COGMOB 2024), Lecture Notes in Networks and Systems, 1258 (2025) pp. 361–373. https://doi.org/10.1007/978-3-031-81799-1_33

[26] Nagy, R., Pethő, Z., Török, Á.: Effective Anomaly Intrusion Detection System Based on ML Methods in Vehicular Networks. In: Zöldy, M. (eds) Proceedings of the 3rd Cognitive Mobility Conference. COGMOB 2024. Lecture Notes in Networks and Systems, 1258 (2025) pp. 334–343. https://doi.org/10.1007/978-3-031-81799-1_31

[27] Zöldy, M., Csete, M. S., Kolozsi, P. P., Bordas, P., & Török, Á.: Cognitive Sustainability. Cognitive Sustainability, 1 (1) (2022). https://doi.org/10.55343/CogSust.7

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution NonCommercial (*CC BY-NC 4.0*) license.