# An Enhanced Machine-Learning Model For Network Intrusion Detection System

**Zinah Sattar Jabbar Aboud**[(1)] The Lebanese University, Lebanon
**Rami Tawil**[(2)] The Lebanese University, Lebanon
**Mustafa Salam Kadhm**[(3)] Computer Department, College of Basic Education, Mustansiriyah University,Iraq
sattarzeina@gmail.com rami.tawil@ul.edu.lb
mst.salam@uomustansiriyah.edu.iq

## Abstract
The internet and technological advancements have facilitated faster communication and information sharing. However, cybercrime, including malware, phishing, and ransomware, remains a severe problem despite technical progress. A significant challenge that has emerged with the quickening pace of technological advancement is detecting the intrusion through Intrusion Detection System (IDS) in wireless networks (WSN) and network communication. To address these challenges, this paper proposes two accurate approaches for intrusion detection in the network and WSN using machine-learning methods include Chaotic Maps (Circle and Logistic), Cauchy Mutation, Support Vector Machine (SVM), Pearson Correlation Coefficient Analysis (PCCA), and Nomadic People Optimizer (NPO). The proposed approaches have five main stages, which are data collection, pre-processing, feature selection, classification, and evaluation. Two datasets help in evaluating the proposed methods, and for WSN-DS and NSL-KDD attain accuracy 99.98 and 99.96% correspondingly.
**Keywords:** NPO, IDs, Chaotic Maps, PCCA.

## Introduction
In cybersecurity, constant change of network security policies is necessary to offset the always-expanding landscape of network attacks. Although awareness of this is rising, present solutions do not adequately protect computer systems or internet infrastructure. Because intrusion methods are always changing, traditional security mechanisms including firewalls, user authentication, and encryption show insufficient [1]. Incorporating extra protections like Intrusion Detection Systems (IDS) becomes vital in order to meet such obstacles. By means of machine learning (ML), developing IDS has shown success in improving network security and providing more degree of protection against intrusion [2].

In network security, evolution in measurements is a response to the complex nature regarding cyber threats. Conventional methods are inadequate, which drives a change toward intelligent and adaptive plans. Recent research supports the utilization of ML, artificial intelligence (AI), and nature-inspired algorithms to strengthen network defenses [1] [3], [4] [5].

a) Signature-Based Detection Systems

Although effective, signature-based systems have drawbacks. They rely on preset attack signatures and demand ongoing changes to identify new threats. Their experience with new intrusion methods emphasizes the requirement of consistent signature database updates. [4] [5]

b) Anomaly-Based Detection Systems

Analyzing deviations from typical behavior, anomaly-based systems identify unknown and known attacks. False alarms, inadequate labeled data for training and handling big data volumes are among the problems [6].

c) Self-Learning Systems

Self-learning systems, using ML concepts, is the third system type used to detect the complex attack patterns. Those adaptive systems provide strong protection against evolving threats by learning from network behavior all the times [7] [8].

The following is a list of proposed system's primary contributions:

• The NPO improved via position update equation.
• Logistic map is used for improve NPO via initialize the population.
• Circle map is used for improve NPO via distribution process.
• Cauchy mutation used to introduce a better diversity of the clans.
• Pearson Correlation Coefficient Analysis (PCCA) applied to find the best correlations between the dataset’s attributes.
• A proposed fitness function based on SVM included in CNPO.
• The update equation of NPO is improved.
• SVM with RBF kernel utilized for classification
• The proposed system assessed with the use of two datasets WSN-DS and NSL-KDD.
• The acquired results regarding the proposed system put to comparison with the most recent works in intrusion detection.

**Related Works**

Several works done for intrusion detection for both network and WSN. The recent works focused on detecting attacks using various machine-learning methods. Some works used different classifiers and deep learning for better detection results. However, other works employed optimization algorithms

for feature selection process, thereby improving the detection performance. The following is a brief summary of recent intrusion detection research.

"Intrusion Detection System in IoT Based on GA-ELM Hybrid Method" by Maseno, Wang, and Liu (2023) mostly addresses the creation on IDS for IoT systems. IoT devices' limited computing and storage capabilities make conventional IDSs inappropriate for such networks. IoT device protocols and requirements cause challenges for intrusion detection in IoT systems [9]. Combining extreme learning machines (ELM) with genetic algorithms (GA), the paper proposes a hybrid method to IoT intrusion detection. The objectives of GA-ELM hybrid method are better detection performance as well as adaptability concerning IDSs in IoT environments.

"A new hybrid teaching learning-based Optimization-Extreme learning Machine model based Intrusion- Detection system" by Reflish, Al-sudani, Adnan, and Moorthy (2023) presents a new hybrid model for IDSs using teaching learning based optimization (TLBO) as well as extreme learning machines (ELM). In network security, the paper addresses the increasing need for efficient IDS particularly in view of the IoT device growth and increasing cyber threats. The proposed hybrid model tries to enhance IDS performance by means of TLBO's optimization features as well as ELM's learning capacity. The paper develops intrusion detection field by suggesting a new approach that might improve the accuracy and efficacy of intrusion detection in network systems. The methodical investigation of ML and DL approaches in network IDSs [10] shows how the focus of the study on hybrid models and ML techniques corresponds with current patterns in intrusion detection research.

Moreover, recent research on the predictive performance of IDSs utilizing hybrid ensemble models [11] indicates that field of additional investigation is IDS performance optimization utilizing ensemble models. All things considered, the Reflish, Alsudani, Adnan, and Moorthy (2023) paper significantly adds to the intrusion detection field and is suitable for publication in allied publications. Its new approach and prospective consequences for raising the efficacy of IDS make this addition to the corpus of knowledge in this field important.

Presented in "Cyber-Attacks in WSN & Security Optimization by a Novel Technique based Intensive Binary Pigeon Optimization (IBiPO) & Bi-LSTM-based IDS Framework" by Nabi (2023), an original and computationally efficient IDS framework for protecting WSNs proposed. Combining a Bidirectional Long Short-Term Memory (Bi-LSTM) network with Intensive Binary Pigeon Optimization (IBiPO) [12] the proposed IBiPO

+ Bi-LSTM model aims to improve the identification of cyberattacks in WSNs.

A model, which combines enhanced chaotic salp swarm algorithm with LightGBM for the task of intrusion detection in MQTT-based IoT environments, presented in the research paper "An efficient intrusion detection system for MQTT-IoT using enhanced chaotic salp swarm algorithm and LightGBM" by Prajisha & Vasudevan [13]. Through employing LightGBM for classification and streamlining the FS procedure, the model seeks to increase intrusion detection's accuracy and effectiveness.

A model, which combines a K-NN classifier with FS for network intrusion detection in IoT environments, presented in the research paper "An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection" by Mohy-eddine et al. [14]. Through using FS and ML approaches for detecting and mitigating network attacks, the model seeks to improve IoT security.

Table 1 Comparison of Literature review

| Aspect | Maseno et al. (2023) | Alsudani et al. (2023) | Bansal and Singhrova (2023) | Nabi (2023) |
|---|---|---|---|---|
| **Title** | IDS in IoT Based upon GA-ELM Hybrid Method | TLBO + ELM Model-based IDS | Review on IDS for IoT/IIoT | IBiPO + Bi-LSTM-based IDS Framework |
| **Objective** | Develop IDS for IoT using GA-ELM | Propose TLBO + ELM Model for IDS | Review existing IDS for IoT/IIoT | Develop IBiPO + Bi-LSTM-based IDS for WSNs |
| **Relevance** | Addresses IoT-specific challenges | Addresses network security trends | Provides a comprehensive review | Addresses WSN-specific challenges |
| **Methodology** | GA-ELM hybrid approach | TLBO optimization + ELM | Literature survey | IBiPO optimization + Bi-LSTM |
| **Performance** | Outperforms existing methods | Comparative improvement | N/A (Review) | Outperforms existing methods |
| **Challenges Addressed** | Limited IoT resources | General network security | Limited IoT/IIoT resources | Limited WSN resources |
| **Validation Strategy** | Experimental comparison | Limited comparative analysis | Literature-based analysis | Experimental comparison |

| | | | | |
|---|---|---|---|---|
| **Future Directions** | Integration of advanced techniques | Explore other techniques | Identify open problems | Explore future research directions |
| **Strengths** | Relevance, Innovation, Performance | Innovation, Optimization | Relevance, Comprehensive review | Relevance, Innovation, Performance |
| **Weaknesses** | Limited comparison, Validation details | Limited comparison, Validation details | Limited comparison, Validation details | Limited comparison, Validation details |
| **Aspect** | **Muhammad, Sukarno, Wardana (2023)** | **Ragab, Alshammari, Al-Ghamdi (2023)** | **Illy et al. (2023)** | **Mirlekar and Kanojia (2023)** |
| **Objective** | Enhance real-time IDS using integrated SIEM + ML | Improve IDS through modified metaheuristics + deep learning | Develop ML-based IDPS for home IoT networks | Evaluate ML algorithms for IDS, emphasizing multiclass classification |
| **Relevance** | Addresses real-time intrusion detection challenges | Focuses on real-time IDS improvement | Proposes ML-based IDPS for home IoT security | Conducts comprehensive study on ML algorithms for IDS |
| **Methodology** | SIEM + IDS integration with ML techniques | Modified metaheuristics + deep learning for IDS | ML-based IDPS for home IoT with unsupervised and supervised learning | Detailed analysis of various ML algorithms for IDS |
| **Performance** | Outperforms existing approaches in accuracy and processing time | Outperforms existing approaches in accuracy and processing time | Shows improvement in accuracy, realistic evaluation with real-world attacks | Demonstrates promising results, particularly with k-Nearest Neighbor algorithm |
| **Challenges Addressed** | Real-time detection, adaptability of IDS | Real-time detection, adaptability of IDS | Development of home IoT security | Evaluation and performance of ML algorithms for IDS |

| | | | | |
|---|---|---|---|---|
| **Validation Strategy** | Experimental results showcasing improved accuracy and processing time | Experimental results demonstrating superiority in accuracy and processing time | Evaluation with real-world attacks, comparison with related works | Comprehensive analyses of various ML methods |
| **Weaknesses** | Limited comparison, validation strategy details | Limited comparison, validation strategy details | Single dataset evaluation, scalability, lack of attack-specific analysis | Lack of dataset characteristics, absence of rule-based IDS comparison |
| **Future Directions** | Potential for more extensive comparisons, detailed validation strategies | Future research directions, practical implications | Scalability considerations for larger IoT networks | Emphasis on generalizability, comparison with traditional rule-based IDS |
| **Comparison with Related Works** | Addresses challenges of real-time detection | Presents an innovative approach with modified metaheuristics | Outperforms related works in accuracy and false positive rate | Complements other studies, particularly in multiclass classification |
| **Aspect** | **Himthani and Dubey [9]** | **Basahel et al. [10]** | **Ogundokun *etal*. [11]** | **Prajisha and Vasudevan [12]** |
| **Objective** | Systematic review of ML in IDS | Improve cloud-IDS with ECODL-IDSCS model | Enhance IDS with ICA-based FS and SVM | Optimize feature selection and classification for MQTT-IoT IDS |
| **Relevance** | Comprehensive overview of ML in IDS | Addresses cloud security challenges | Relevant for cloud and IoT security | Addresses MQTT-based IoT security |
| **Methodology** | Systematic review of ML in IDS | Enhanced coyote optimization + deep learning | ICA-based feature selection + SVM classification | Enhanced chaotic salp swarm + Light GBM |
| **Performance** | Not applicable (review study) | Novel approach, but needs extensive empirical evaluation | High accuracy and low false positive rates | High accuracy and low false positive rates |

| | | | | |
|---|---|---|---|---|
| **Challenges Addressed** | Understanding ML strategies, databases, and metrics in IDS | Robust intrusion detection in cloud environments | Enhanced accuracy in IDS, scalability | Optimized feature selection for MQTT-IoT |
| **Validation Strategy** | Not applicable (review study) | Needs more extensive empirical evaluation | Experimental results with high accuracy | Experimental results with high accuracy |
| **Weaknesses** | Lack of individual algorithm performance analysis | Limited empirical evaluation, scalability and limitations not discussed | Limited comparison with other IDS, scalability | Limited discussion of challenges and limitations |
| **Future Directions** | Detailed analysis of individual algorithms and practical applicability | More empirical evaluation, scalability considerations | Scalability and adaptability considerations | Detailed discussion of challenges and limitations |
| **Comparison with Related Works** | Complements research focusing on specific aspects of ML in IDS | Distinguishes with hybrid optimization and deep learning | Unique integration of ICA-based feature selection and SVM | Unique integration of enhanced chaotic salp swarm and LightGBM |

## The Proposed System

In the proposed system, two approaches represented. The first one based one improved NPO with Chaotic Maps, while the second approach based on improved NPO with Cauchy mutation.

### 1- The Proposed Approach (First Contribution)

Number of stages taken into consideration in the proposed intrusion detection process. In order to obtain the highest detection results, several stages are involved which are data collection, pre-processing, feature selections, classification, and evaluation. Fig. 1 shows the main stages of the proposed work.

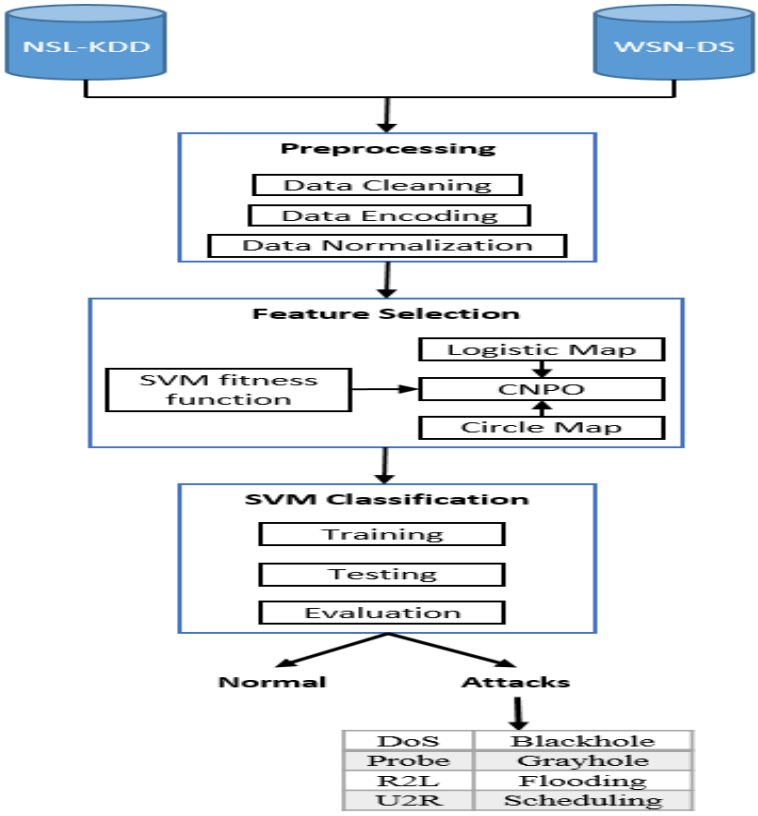


**Fig 1: Proposed System (First Contribution).**

In the proposed system, two datasets used for evaluating the system performance. The first dataset is NSL-KDD dataset [15], and the second one is WSN-DS [16]. NSL-KDD dataset is updated version of KDD'99 dataset.

In the pre-processing stage, the NSL-KDD and WSN-DS datasets go through three crucial steps, which are data cleaning, encoding and Normalization. The cleaning process removes missing and unnecessary values, such as the "num_outbound_cmds" values in NSL-KDD, which are always 0. Thus, the attribute values become beneficial for the next proposed system stages.

In the proposed system an improved version of nomadic people optimizer (NPO) called CNPO for feature selection process using two chaotic maps (logistic and circle) and proposed fitness function (depending on SVM) is presented. The CNPO select the most relevant features with highest impact

on the obtained results based on optimal features criteria. The proposed feature selection method shown in Fig. 2.

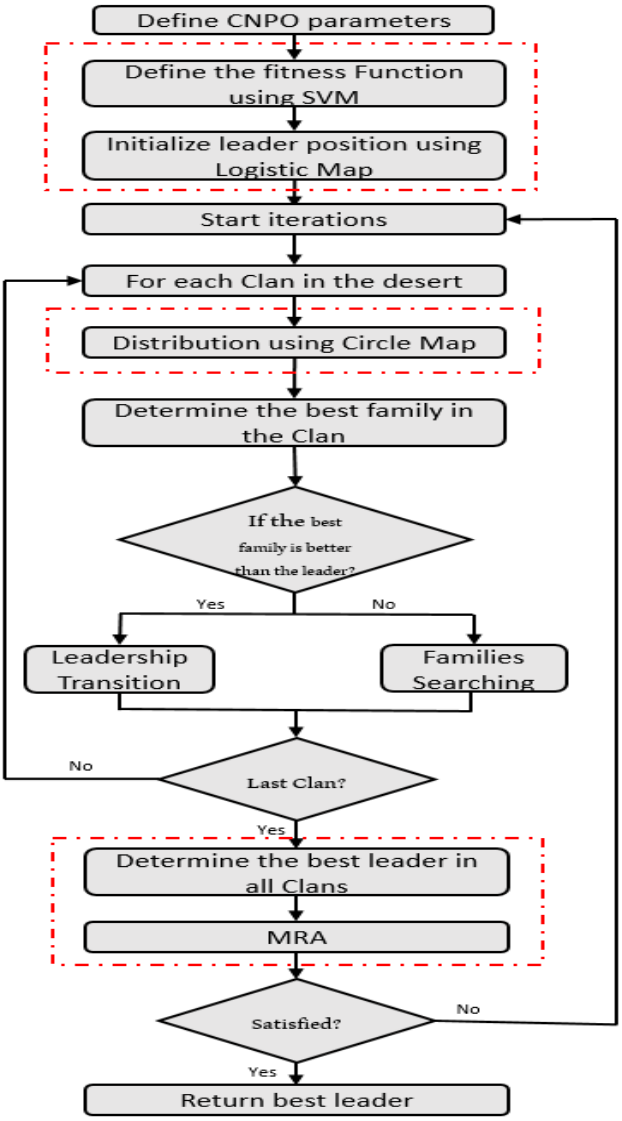


**Figure 2: Proposed Feature Selection Approach (CNPO)**

**2- Second Approach (Second Contribution)**

In the second approach, several stages considering. These stages work together to achieve best possible detection results for detecting any intrusion in the networks. The stages include data collection, pre-processing, feature

selection, classification, and evaluation. The main stages of the proposed system illustrated in Fig. 3.

Since the datasets have some attributes with text representation (like the attack types, protocols, etc.), and the next stages work only with numerical values, an encoding process is applied to convert the text to numerical representation using indexing in the second step of the pre-processing stage. Besides, each attack types will have a label and the normal behavior will have a label to be use in the classification stage.

Data normalization is the third pre-processing step. The classification stage is less affected by the variance of the numerical data range after the normalization step [17] is used in the proposed system for normalizing the data into scale [0,1]. The final step of the proposed preprocessing stage is the correlation. A statistical approach for the determination the direction and strength of a linear relation between two variables is the Pearson Correlation Coefficient Analysis (PCCA). The Pearson correlation coefficient (r), which could vary from -1 to +1, used to express the outcome [18].

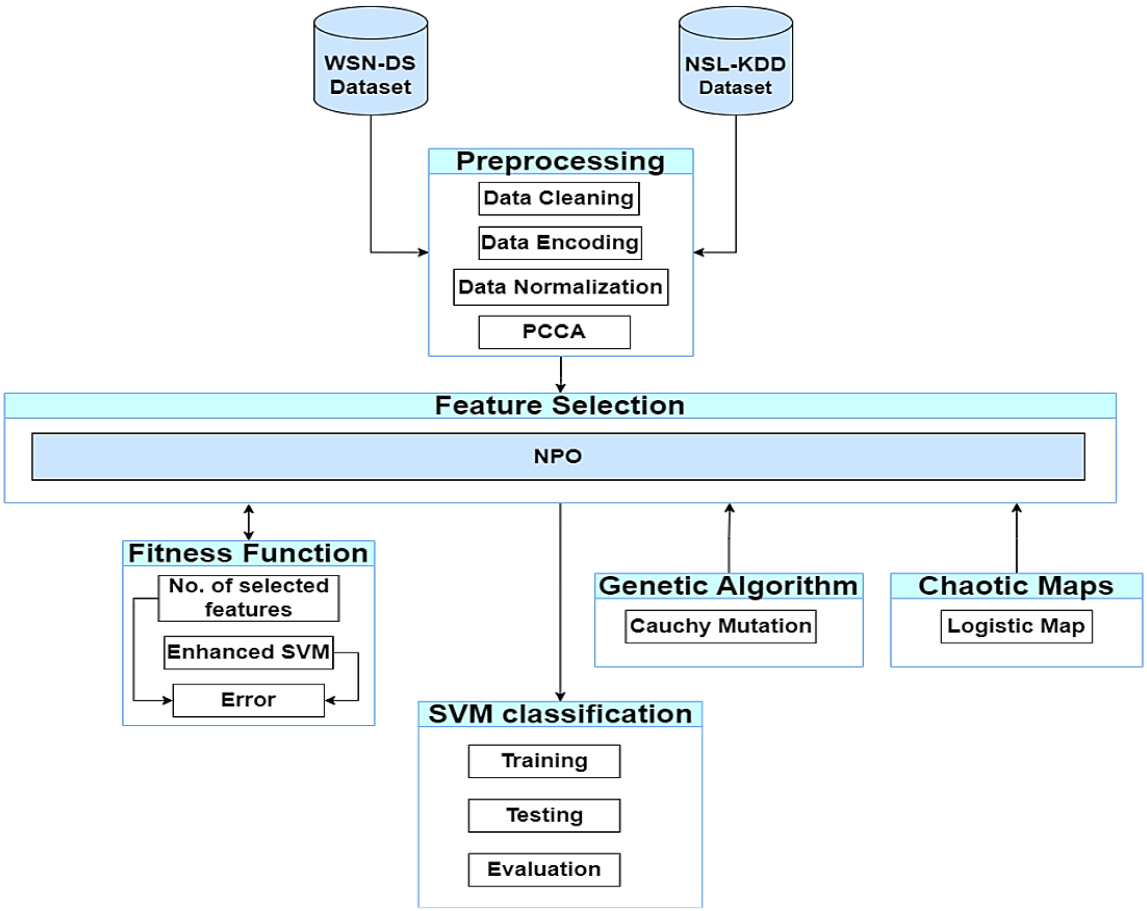


**Figure 3: Proposed System (Second Contribution).**

In the proposed system an improved version of NPO called INPO for feature selection process using chaotic map (logistic), Cauchy mutation and proposed fitness function (depending on SVM) is presented. The INPO select the relevant features with highest impact on the obtained results based on optimal features criteria. The proposed feature selection method shown in Fig. 4.

This mutation operator is designed to introduce diversity into a population by allowing larger, more frequent mutations compared to Gaussian mutations, which makes it particularly useful for escaping local optima in optimization problems.

A random jumping method using the Cauchy mutation added to the NOP to improve the capability for jumping out of the local optimum, increasing population diversity and enhancing the capacity of search to leave local optima. An additional goal Cauchy mutation enhance the capacity for NPO exploitation in relation to family search and to keep the family kin from disintegrating into the neighborhood ideal. The Cauchy mutation has the potential to yield different random variables that adhere to the Cauchy distribution to revise the position of the leaders to improve the search-ability of clans.

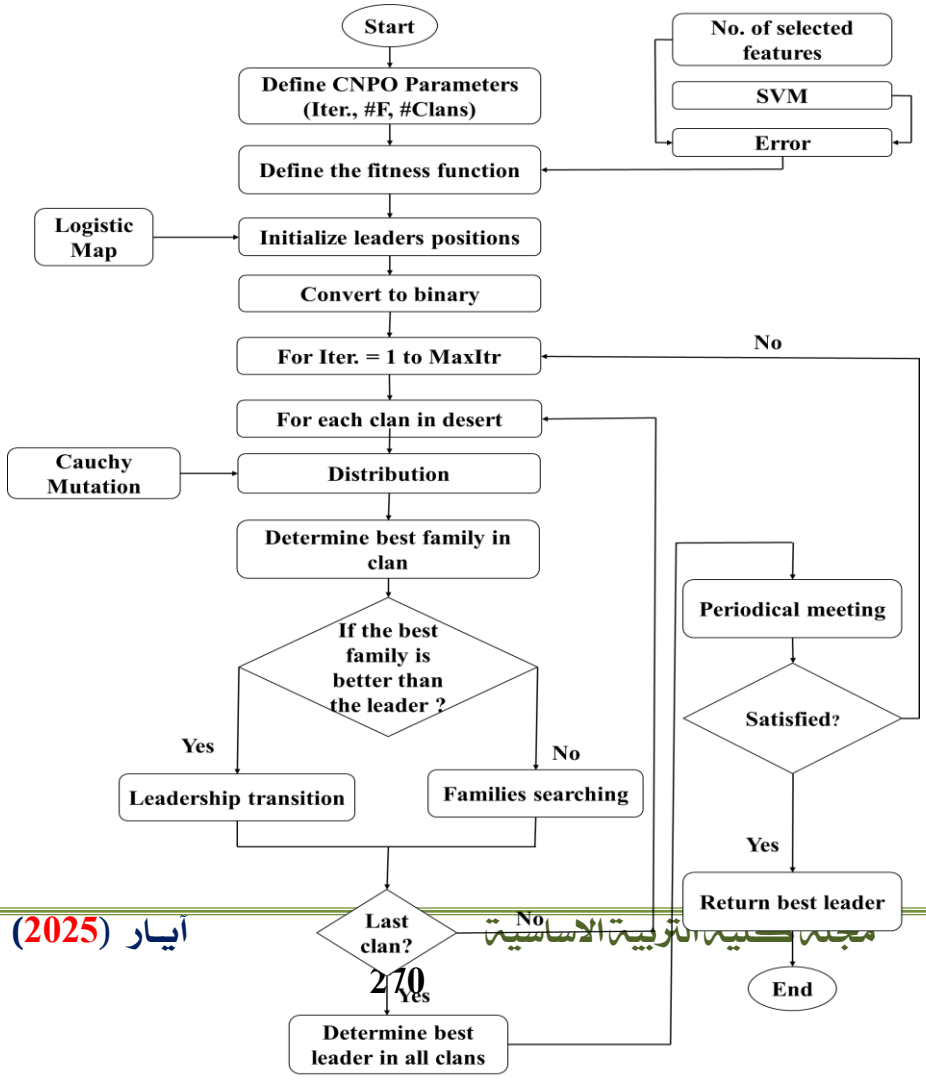

**Figure 4: Proposed Feature Selection Algorithm (INPO).**

**Results and Discussions**

The proposed work tested using the Python programming language and the Windows 11 environment on two intrusion detection datasets: WSN-DS and NSL-KDD. A total of 30% of the datasets were utilized to test the proposed work, while 70% were used for training. The outcomes of using the proposed work shown in Table 2.

**Table 2. Result of NPO and CNPO algorithms**

| Meth. | Dataset | Acc.% | Prec.% | Rec.% | F1% |
|---|---|---|---|---|---|
| NPO | NSL-KDD | 93.5 | 94.4 | 94.4 | 96.6 |
| | WSN-DS | 92.3 | 94.1 | 94.1 | 96 |
| CNPO | NSL-KDD | 99.96 | 99.6 | 99.6 | 99.9 |
| | WSN-DS | 99.98 | 99.98 | 99.98 | 99.9 |
| INPO | NSL-KDD | 99.97 | 99.7 | 99.7 | 99.9 |
| | WSN-DS | 99.99 | 99.99 | 99.99 | 99.9 |

The proposed CNPO outperform the standard NPO in the two used datasets. CNPO achieve accuracy 99.96% and 99.98% for NSL-KDD, and WSN-DS respectively, which is better about 6% than the NPO results. Besides, it

achieved precision 99.6%, 99.98%, recall 99.6%. 99.98, and F-score 100 for both datasets NSL-KDD, and WSN-DS. In another hand, the proposed INPO outperform the standard NPO in the two used datasets. INPO achieve accuracy 99.97% and 99.99% for NSL-KDD, and WSN-DS respectively, which is better about 7% than the NPO results. Besides, it achieved precision 99.9%, 99.99%, recall 99.9%. 99.99, and F-score 100 for both datasets NSL-KDD, and WSN-DS.

The results of applying all chaotic maps in the proposed system listed in Table 3 below.

**Table 3. Result of NPO and CNPO algorithms using different chaotic maps**

| Alg. | Chaotic Maps | Dataset | Accuracy % |
|---|---|---|---|
| CNPO | Chebyshev | NSL-KDD | 99 |
| | Chebyshev | WSN-DS | 99.1 |
| CNPO | Circle | NSL-KDD | 99.96 |
| | Circle | WSN-DS | 99.98 |
| CNPO | Gauss/mouse | NSL-KDD | 98.8 |
| | Gauss/mouse | WSN-DS | 99 |
| CNPO | Iterative | NSL-KDD | 98 |
| | Iterative | WSN-DS | 98 |
| CNPO | Logistic | NSL-KDD | 99.96 |
| | Logistic | WSN-DS | 99.98 |
| CNPO | Piecewise | NSL-KDD | 99.2 |
| | Piecewise | WSN-DS | 99.2 |
| CNPO | Sine | NSL-KDD | 99.2 |

| | | | |
|---|---|---|---|
| | Sine | WSN-DS | 99.3 |
| CNPO | Singer | NSL-KDD | 98.4 |
| | Singer | WSN-DS | 98.4 |
| CNPO | Sinusoidal | NSL-KDD | 98.5 |
| | Sinusoidal | WSN-DS | 98.8 |
| CNPO | Tent | NSL-KDD | 98.6 |
| | Tent | WSN-DS | 98.6 |
| INPO | Chebyshev | NSL-KDD | 99.4 |
| | Chebyshev | WSN-DS | 99.4 |
| INPO | Circle | NSL-KDD | 99.97 |
| | Circle | WSN-DS | 99.99 |
| INPO | Gauss/mouse | NSL-KDD | 99 |
| | Gauss/mouse | WSN-DS | 99 |
| INPO | Iterative | NSL-KDD | 99 |
| | Iterative | WSN-DS | 99 |
| INPO | Logistic | NSL-KDD | 98.9 |
| | Logistic | WSN-DS | 98.9 |
| INPO | Piecewise | NSL-KDD | 99 |
| | Piecewise | WSN-DS | 99 |
| INPO | Sine | NSL-KDD | 98.8 |

| | | | |
|---|---|---|---|
| | Sine | WSN-DS | 98.9 |
| INPO | Singer | NSL-KDD | 99 |
| | Singer | WSN-DS | 99 |
| INPO | Sinusoidal | NSL-KDD | 99.4 |
| | Sinusoidal | WSN-DS | 99.4 |
| INPO | Tent | NSL-KDD | 99.4 |
| | Tent | WSN-DS | 99.5 |

The obtained results in Table 3 indicated that, the best results of the both proposed algorithms CNPO, INPO were using Circle and Logistic maps. Using circle map for initializing the population and logistic map for clan distribution in CNPO achieve 99.96% accuracy in NSL-KDD and 99.98% in WSN-DS, which are, outperform other chaotic maps. In another hand, using circle map for initializing the population and in INPO achieve 99.97% accuracy in NSL-KDD and 99.99% in WSN-DS, which are, outperform other chaotic maps.

Another comparison made between the SVM classifier and other machine learning classifiers with the proposed CNPO and INPO as exhibited in Table 4.

**Table 4. Results of Different Classifiers**

| Class. | Alg. | Dataset | Acc.% | Prec.% | Rec.% | F1% |
|---|---|---|---|---|---|---|
| KNN | CNPO | NSL-KDD | 95.2 | 95.2 | 95.2 | 97.5 |
| | | WSN-DS | 96 | 96 | 96 | 97.9 |
| ANN | CNPO | NSL-KDD | 97.9 | 97.9 | 97.9 | 98.9 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | WSN-DS | 98.5 | 98.5 | 98.5 | 99.2 |
| SVM | CNPO | NSL-KDD | 99.96 | 99.96 | 99.96 | 99.9 |
| | | WSN-DS | 99.98 | 99.98 | 99.98 | 99.9 |
| KNN | INPO | NSL-KDD | 95.6 | 95.6 | 95.6 | 97.8 |
| | | WSN-DS | 96.3 | 96.3 | 96.3 | 98 |
| ANN | INPO | NSL-KDD | 98.2 | 98.2 | 98.2 | 99 |
| | | WSN-DS | 98.8 | 98.8 | 98.8 | 99.5 |
| SVM | INPO | NSL-KDD | 99.97 | 99.7 | 99.7 | 99.9 |
| | | WSN-DS | 99.99 | 99.99 | 99.99 | 99.9 |

In Table 4, using SVM with the proposed CNPO and INPO achieved the highest precision, accuracy, f-score, and recall results than other classifiers with both NSL-KDD and WSN-DS datasets.

In depth, discussion and analyzing the results of the proposed IDS depending on CNPO and INPO presented. CNPO superior from the standard NPO standard NPO in choosing the most relevant features leading to better detection results using NSL-KDD, and WSN-DS datasets.

In another hand, SVM outperform KNN and ANN in the classification accuracy with RBF kernel. The SVM classifier archived the highest classification accuracy in both datasets NSL-KDD, and WSN-DS using RBF kernels within parameters gamma = 0.09, and c = 1.0.

The proposed approach compared with other recent works that have done for intrusion detection using various datasets and method as exhibited in Table 3.

TABLE 3: Results of proposed approach and other works

| Ref. | Dataset | Method | Acc. |
|---|---|---|---|
| [19] | NSL-KDD | GBA | 96.96% |
| [20] | NSL-KDD | CBIGRU<br>ABILSTM<br>(PACENIDS) | 96.59%<br>94.47%<br>97.67% |
| [21] | WSN-DS | GNB+SGD | 98% |
| [22] | UNSW-NB15 | KOMIG IDS | 97.14% |
| [23] | KDD-CUP99 | Cuckoo Algorithm | 89.8% |
| [24] | NSL-KDD | SVM<br>TD<br>RF | 95.2%<br>92.7%<br>94.5% |
| [25] | UNSW-NB15 NSL-KDD<br>CIC-IDS2017 | XGBoost + Mutual Information+ Thresholding | 87.63%<br>80.51%<br>99.89% |
| Proposed (First Approach) | NSL-KDD<br>WSN-DS | CNOP + SVM | 99.96%<br>99.98% |
| Proposed (Second Approach) | NSL-KDD<br>WSN-DS | INOP + SVM | 99.97%<br>99.99% |

**Conclusion**

This paper presents an accurate ML approach for intrusion detection in networks and WSNs by use of Cauchy mutation, chaotic maps, SVM, and NPO classifiers. Two approaches can used to carry out the proposed task. The first approach consists in data collecting, pre-processing, FS, classification, and evaluation. The studies made advantage of two open-source IDS datasets, WSN-DS and NSL-KDD. The first proposed approach yielded outstanding detection performance using the proposed CNPO feature selection and SVM classifier. Top results for the NSL-KDD dataset were 99.96% accuracy, 99.96% recall, 99.9% F1-score, and 99.6% precision. For the WSN-DS dataset, also reached were 99.98% accuracy, 99.98% recall, 99.9% F1-score. Moreover, compared to the most recent IDS works, the proposed approach beats the accuracy of the present efforts. The second proposed approach yielded outstanding detection results using the proposed INPO feature selector and SVM classifier. Top results for the NSL-KDD dataset were 99.97% accuracy, 100% F1-score, 99.97% precision, and 99.97% recall. For the WSN-DS dataset, also reached were 99.99% precision, 99.99% accuracy, 99.99% recall, and 100% F1-score. Moreover, the proposed approach beats the accuracy of the present works in relation to the most recent IDS publications.

**References**

[1] X. Guan, W. Wang, and X. Zhang, “Fast intrusion detection based on a non-negative matrix factorization model,” J. Netw. Comput. Appl., vol. 32, no. 1, pp. 31–44, 2009, doi: 10.1016/j.jnca.2008.04.006.

[2] B. A. Tama, L. Nkenyereye, S. M. R. Islam, and K. S. Kwak, “An enhanced anomaly detection in web traffic using a stack of classifier ensemble,” IEEE Access, 2020, doi: 10.1109/ACCESS.2020.2969428.

[3] S. Kumar, S. Gupta, and S. Arora, “Research Trends in Network-Based Intrusion Detection Systems: A Review,” IEEE Access. 2021. doi: 10.1109/ACCESS.2021.3129775.

[4] B. Alsulami, “A Review on Machine Learning Based Approaches of Network Intrusion Detection Systems,” Int. J. Curr. Sci. Res. Rev., vol. 05, no. 06, Jun. 2022, doi: 10.47191/ijcsrr/V5-i6-47.

[5] A. A. Salih and A. M. Abdulazeez, "Evaluation of Classification Algorithms for Intrusion Detection System: A Review," J. Soft Comput. Data Min., vol. 02, no. 01, Apr. 2021, doi: 10.30880/jscdm.2021.02.01.004.
[6] Y. Shin and K. Kim, "Comparison of Anomaly Detection Accuracy of Host-based Intrusion Detection Systems based on Different Machine Learning Algorithms," Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 2, 2020, doi: 10.14569/IJACSA.2020.0110233.
[7] and N. J. Khan, Javed Akhtar, "A Survey on Intrusion Detection Systems and Classification Techniques," IJSRSET, India, vol. 2, no. 5, pp. 202–208, 2016.
[8] M. H. L. Louk and B. A. Tama, "PSO-Driven Feature Selection and Hybrid Ensemble for Network Anomaly Detection," Big Data Cogn. Comput., vol. 6, no. 4, p. 137, Nov. 2022, doi: 10.3390/bdcc6040137.
[9] Maseno, E.M., Wang, Z. and Liu, F., 2023. Intrusion Detection System in IoT Based on GA-ELM Hybrid Method. Journal of Advances in Information Technology, 14(4), pp.625-629.
[10] Ahmad, Z., Khan, A. S., Shiang, C. W., & Abdullah, J. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(2), DOI:10.1002/ett.4150.
[11] Abbas, Q., Hina, S., Sajjad, H., Zaidi, K. S., & Akbar, R. (2023). Optimization of predictive performance of intrusion detection system using hybrid ensemble model for secure systems. PeerJ Comput Sci, 9, e1552. DOI: 10.7717/peerj-cs.1552.
[12] Nabi, F., & Hasan, R. (2023). Cyber-Attacks in WSN & Security Optimization By Novel Technique based Intensive Binary Pigeon Optimization (IBiPO) & Bi-LSTM-based IDS Framework. Wireless Networks, Computer Networks, Wireless Security, Computer Science and Engineering, Computer Communications (Networks), WSN Security. DOI: 10.36227/techrxiv.24328729. CC BY 4.0.
[13] Prajisha, C. and Vasudevan, A.R., 2022. An efficient intrusion detection system for MQTT-IoT using enhanced chaotic salp swarm algorithm and LightGBM. International Journal of Information Security, 21(6), pp.1263-1282.
[14] Mohy-eddine, M., Guezzaz, A., Benkirane, S. and Azrour, M., 2023. An efficient network intrusion detection model for IoT security using K-NN classifier and feature selection. Multimedia Tools and Applications, pp.1-19.
[15] R. ZHAO, "NSL-KDD", IEEE Dataport, 2022, doi: https://dx.doi.org/10.21227/8rpg-qt98.

[16] J. Pan, Y. Zhuang, S. Fong, "the impact of data normalization on stock market prediction: using SVM and technical indicators", in: International Conference on Soft Computing in Data Science, Springer, pp. 72–88, 2016.
[17] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," J Sens, Vol. 2016, 2016, doi: 10.1155/2016/4731953.
[18] R.F. Tate, Correlation between a discrete and a continuous variable. point-biserial correlation, Ann. Math. Stat. 25 (1954) 603–607.
[19] S. S. Issa, S. Q. Salih, Y. D. Salman, and F. H. Taha, "An Efficient Hybrid Filter-Wrapper Feature Selection Approach for Network Intrusion Detection System," International Journal of Intelligent Engineering and Systems, Vol. 16, No. 6, pp. 261–273, 2023, doi: 10.22266/ijies2023.1231.22.
[20] N. Girubagari and T. N. Ravi, "Parallel ABILSTM and CBIGRU Ensemble Network Intrusion Detection System," International Journal of Intelligent Engineering and Systems, Nol. 17, No. 1, pp. 93–107, 2024, doi: 10.22266/ijies2024.0229.10.
[21] Radcliff, D. (2004, November 8). The Evolution of IDS. Network World. https://www.networkworld.com/article/2319392/the-evolution-of-ids.html
[22] A. S. Afolabi and O. A. Akinola, "Network Intrusion Detection Using Knapsack Optimization, Mutual Information Gain, and Machine Learning," Journal of Electrical and Computer Engineering, Vol. 2024, pp. 1–21, 2024, doi: 10.1155/2024/7302909.
[23] H. Lafta, "Network Intrusion Detection Using Optimal Perception with Cuckoo Algorithm," Wasit Journal for Pure sciences, Vol. 3, No. 1, pp. 95–105, 2024, doi: 10.31185/wjps.326.
[24] B. R. Maddireddy and B. R. Maddireddy, "A Comprehensive Analysis of Machine Learning Algorithms in Intrusion Detection Systems.", Journal of Environmental Sciences and Technology (JEST), Vol. 3, No. 1, pp. 877-893, 2024.
[25] M. A. Faizin, D. T. Kurniasari, N. Elqolby, M. A. R. Putra, and T. Ahmad, "Optimizing Feature Selection Method in Intrusion Detection System Using Thresholding," International Journal of Intelligent Engineering and Systems, Vol. 17, No. 3, pp. 214–226, 2024, doi: 10.22266/ijies2024.0630.18.

# نموذج التعلم الآلي المعزز لنظام كشف التطفل على الشبكات

[1]زينة ستار جبار عبود
الجامعة اللبنانية
sattarzeina@gmail.com

[2]رامي الطويل
الجامعة اللبنانية
rami.tawil@ul.edu.lb

[3]مصطفى سلام كاظم
قسم الحاسبات، كلية التربية الاساسية،
الجامعة المستنصرية
mst.salam@uomustansiriyah.edu.iq

**مستخلص البحث:**
لقد سهّل الإنترنت والتطورات التكنولوجية التواصل وتبادل المعلومات بشكل أسرع. ومع ذلك، لا تزال الجرائم الإلكترونية، بما في ذلك البرامج الضارة والتصيد الاحتيالي وبرامج الفدية، تُشكّل مشكلة خطيرة على الرغم من التقدم التقني. ومن التحديات الكبيرة التي ظهرت مع تسارع وتيرة التقدم التكنولوجي اكتشاف التسلل من خلال نظام كشف التسلل (IDS) في الشبكات اللاسلكية (WSN) واتصالات الشبكة. ولمواجهة هذه التحديات، تقترح هذه الورقة نهجين دقيقين لاكتشاف التسلل في الشبكة وشبكة WSN باستخدام أساليب التعلم الآلي، وهما: الخرائط الفوضوية (الدائرة واللوجستية)، وطفرة كوشي، وآلة المتجهات الداعمة (SVM)، وتحليل معامل ارتباط بيرسون (PCCA)، ومُحسّن الأشخاص الرحل (NPO). تتكون الأساليب المقترحة من خمس مراحل رئيسية هي: جمع البيانات، والمعالجة المسبقة، واختيار الميزات، والتصنيف، والتقييم. تساعد مجموعتا بيانات في تقييم الأساليب المقترحة، وتصل دقة نظامي WSN-DS وNSL-KDD إلى 99.98 و99.96% على التوالي.
**الكلمات المفتاحية : NPO** ، اكتشاف التطفل، التصنيف، الخرائط الفوضوية و PCCA.
**ملاحظة : هل البحث مستل من رسالة ماجستير او اطروحة دكتوراه ؟ نعم**