# A FUSION OF CHICKEN SWARM OPTIMIZATION AND NAIVE-BAYES CLASSIFIER FOR INTRUSION DETECTION

**Dr.A.Shanthisona[1] & Dr.A.Krishnaveni[2]**

**Assistant Professors[1&2],**

**PG & Research Department of Computer Science, Tiruppur Kumaran College for Women, Tirupur[1]&**

**Department of Computer Science & Research Centre, Thassim Beevi Abdul Kader College for Women, Kilakarai[2].**

***Abstract*—**An efficient intrusion detection system (IDS) is utilized in wireless ad hoc network for detecting the intrusion data on various nodes with higher security. The main aim of HCSO-NB method is to improve the classification of data as normal or malicious with higher intrusion detection accuracy. Here, better detection of analogous node is achieved by monitoring the system behaviour. An anomaly-based intrusion detection system is more efficient for classifying normal or anomalous data. In HCSO-NB method, chicken swarm optimization is introduced at first with four different rules of chicken behaviour. Here, NB classifier is used in network to identify the faulty hubs in system. Hence, time taken for detecting intrusion data is minimized with less false rate and helps to enhance the anomaly intrusion detection accuracy.

**Keywords—*Intrusion Detection, Swarm Optimization, Naive Bayes, Anomaly, False Rate***

## 1. INTRODUCTION

Wireless Ad-hoc networks suggest a capability of connecting multiple nodes without a centralized access point. It provides the explanation to avoid network intruders for effective communication and for detecting the malicious in network. Network intrusion detection system is a device that monitors network for detecting the normal or malicious behaviour. IDS are located at essential point within the network to monitor data traffic to and from each device on the network. Thus, it increases the data transmission in a secured manner. It comprises with two detection approaches such as signature based intrusion detection and anomaly based intrusion detection. Anomaly-based intrusion detection system is mostly used for identifying the network intrusions by examining and classifying the normal or anomalous behaviour. Recently, many techniques aimed on intrusion detection in wireless networks. The designed conventional techniques are difficult to extract the intrusion behaviour features from high dimensional dataset.

### 1.1. Paper Outline

This paper is divided into five portions for the remainder of it. The problems and difficulties with intrusion detection in related works are explained in detail in Section 2. The model for feature selection and classification-based intrusion detection is described in Section 3. Section 4 conducts an experimental evaluation using a dataset, and Section 5 discusses the performance outcomes of different metrics. Lastly, the work's conclusion is given in section 6.

## 2. RELATED WORKS

Yuk Ying Chunga et al. [1] proposed a new hybrid intrusion detection system that uses simplified swarm optimization for intrusion data classification and intelligent dynamic swarm based rough set (IDS-RS) for feature selection. To choose the most pertinent elements that can best depict the network traffic pattern, IDS-RS is suggested. To enhance the SSO classifier's performance, a novel weighted local search (WLS) approach integrated with SSO is suggested. This novel local search approach aims to find the best solution from the vicinity of the SSO-produced current solution. Using the KDDCup 99 dataset, the suggested hybrid system's performance has been assessed in comparison to two other widely used benchmark classifiers and the conventional particle swarm optimization (PSO). According to the test findings, the suggested hybrid system can classify objects with a better accuracy than the others (93.3%), making it a competitive classifier for intrusion detection systems.

The hybrid model created in this proposed study by A.Shanthi Sona et.al [2] fusing the Chicken Swarm and Naive Bayes optimization algorithms perform better. The experimental findings demonstrate that varied outcomes can be obtained by selecting a base algorithm and integrating it with the swarm optimize concept. The results obtained for the proposed hybrid CSO-NB algorithm demonstrate that, by filtering normal data, it is more efficient and faster at detecting unknown attacks. It can also detect intrusions more easily by comparing other swarm intelligence and Naïve Bayes techniques, using different network fields. Thanks to hybrid optimization, the accuracy has significantly increased from the current 76% to 87.27%.

Fadi Saloa et al. [3] proposed hybrid algorithm based classification for intrusion detection. The methods are Information Gain, Principal Component Analysis, Multilayer

Perceptron, Support Vector Machine and Instance based Learning methods. The presentation of this IG-PCA-Group technique was assessed in view of three notable datasets, to be specific ISCX 2012, NSL-KDD, and Kyoto 2006+.

Alaa O. Khadidos et al. [4] introduced a novel IDS framework SCADA by implementing a combination of methodologies, such as clustering, optimization, and classification for increasing the accuracy. Beatriz Flamia Azevedo et al. [5] investigated the techniques involved in prediction of intrusion detection. They underlined all the trustworthy methods for intrusion and highlightening the hybrid methods and its importance. Zhenwu Wang et al. [6] suggested adaptive chicken swarm optimization algorithm for intrusion detection. They consider the basic functionalities and cosine function to updating the speed and position.

Mhamad Bakro et al. [7] identify the challenges in feature selection and introduced the hybrid feature selection method using genetic and grasshopper algorithm for efficient search in intrusion detection and reduced the irrelevancy in feature selection process. Mohammad Azmi Ridwan et al [8] suggested a hybrid ML-IDS and ML-RA algorithm to boost traffic quality of service and the resilience of the MPLS network. The suggested ML-IDS is an ML algorithm that learns the traffic pattern at the ingress router through classification. ML-IDS predict and categorize incoming traffic as either normal or attack based on prior data. The anticipated attack traffic will be rejected and prevented from entering the network domain. In the meanwhile, the expected flow of traffic will be arranged in a priority queue. Mohit Tiwari et al. [10] studied a total learn about the interruption discovery, kinds of interruption location strategies, kinds of assaults, various devices and procedures, research necessities, challenges lastly foster the IDS Device for research reason That instrument are fit for identify and forestall the interruption from the interloper.

## 3. METHODOLOGY

### 3.1 Chicken Swarm Optimization and Naive Bayes Classifier Method

An efficient Hybrid module Chicken Swarm Optimization and Naive Bayes classifier method is proposed for the detection of anomaly intrusion in wireless ad-hoc network. To achieve efficient intrusion detection in network, new reliable hybrid method designed by Mehrnaz Mazini et al., (2019). It only detects the intrusion attacks but not provide the data classification in wireless network. These issues are overcome by developing proposed method for anomaly intrusion recognition in wireless ad-hoc

network. Let us consider various nodes in wireless ad hoc network that specified as ‘N_i=N_1,N_2,…,N_n’ distributed in a given rectangular area of ‘M*N’ with a communication range ‘R’. The main aim of proposed method is to recognize the anomaly intrusion. The anomaly intrusion nodes allow any data packets to transmit from source node ‘SN’ to any destination node ‘DN’ through intermediate nodes. Here, a set of data packets ‘〖DP〗_i= 〖DP〗_1, 〖DP〗_2,…, 〖DP〗_n’ are transmitted. The architecture diagram of HCSO-NB method for anomaly intrusion detection and data classification is shown in below Figure 1.

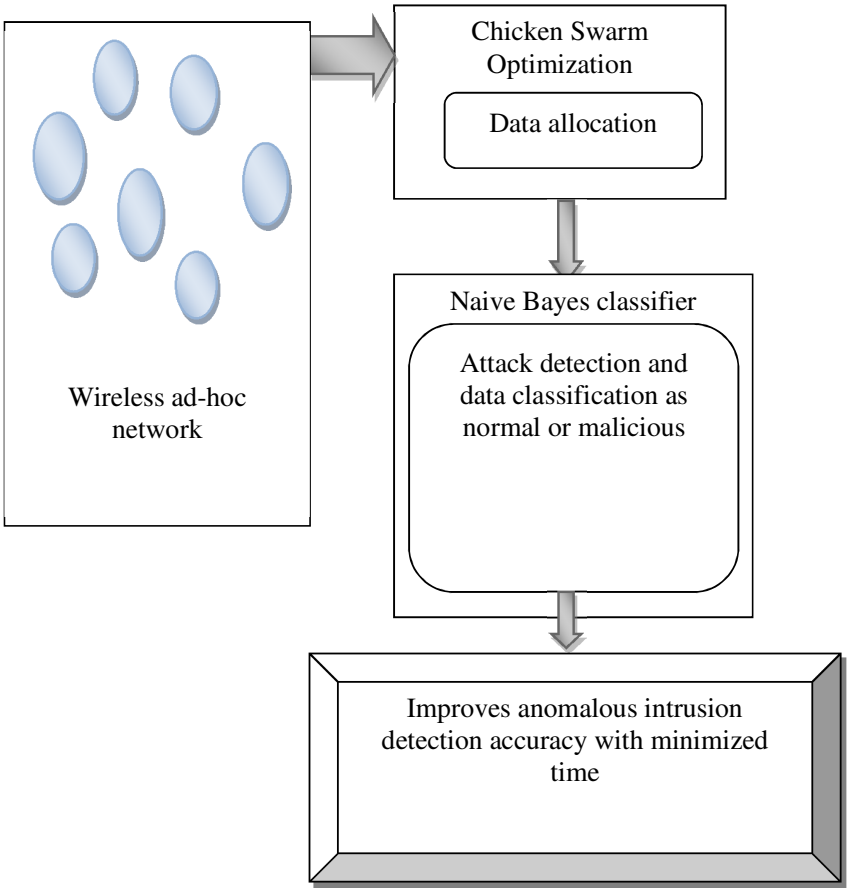


**Figure 1 Architecture diagram of Hybrid module Chicken Swarm Optimization and Naive Bayes classifier**

Figure 1 demonstrate that the construction diagram of proposed classifier for detecting intrusion in network. The proposed HCSO-NB method is composed of two procedures namely data allocation from dataset and detection of attacks by classifying data as normal or anomaly data. The main objective proposed method is improving the anomaly intrusion detection accuracy with minimum time. A novel intrusion-detection system called as Enhanced Adaptive Acknowledgment was introduced by Elhadi M. Shakshuki et al. (2013) to improve the detection of malicious data in network. Though, it causes a difficulty on identifying the data for separating normal or anomalous data.

Therefore, HCSO-NB method is proposed for improving the anomaly intrusion detection in wireless ad-hoc network. Here, a malicious data activity is extracted through the optimization technique. After that, the attack detection and data classification is carried out using naive Bayes classifier based on the obtained data.

Initially, chicken swarm optimization is performed in proposed method for selecting data of chicken behaviours with random variables. It comprises with different rules of chicken that is generated by various attacks in network. Based on the data value, chickens are divided into separate values for different classes. After selecting the data attributes, Naive Bayes classifier is used to accurately distinguish the malicious activities. It performs the classification task for avoiding the failure of unrecoverable process. This helps to drop intruder data in the attack classification process. With the use attack classification process, the malicious behaviour from the normal data is accurately identified.

### 3.2 NB-Chicken Swarm Optimization

With the comparison of other classifier algorithm, proposed Naive Bayes classifier algorithm improves the performance analysis of intrusion detection. With the use of NB classifier, the attacks detection and classification is performed on selected data features. The anomaly intrusion detection is carried out using developed classifier with the reduction of intruders. Thus, the process description of proposed. Hybrid module Chicken Swarm Optimization and Naive Bayes classifier (HCSO-NB) method is explained in following algorithm.

**Dataset: // training and test dataset**
Normal 'F' declares 42 features of NSL-KDD-99 dataset
//feature selection
**//Hybrid NB-Chicken Swarm Optimization Algorithm:**
**Begin**
**Initialize:** G divide into several time steps (initialization)
For each parameter Naïve Bayes linear function is applied
**Step 1:** Remove irrelevant features
**Step 2:**Apply NB fitness function to evaluate alternative subsets of attributes
**Step 3:** Compare the rooster fitness value to adapt data access

$$y_{i,j}^{t+1} = y_{i,j}^{t+1} * (1 + randn(0, \sigma^2))$$

**Step 4:** The dataset attributes are distributed using Gaussian function with means as zero and standard deviation as $\sigma$.
**Step 6:** Find the exact difference among all attributes and gives priority.
**End**

**Algorithm 1: Algorithmic process of Hybrid module Chicken Swarm Optimization and Naive Bayes classifier method**

The process for classifying the normal and anomalous data in network is described by using above algorithm 1. The NB classifier process categorizes the anomalous intrusion in wireless ad-hoc network. Initially, chicken swarm optimization is placed on each data for the estimation of data attributes. With the support of data features, the data are separated as anomalous or normal data. Foe each data, fitness value is estimated to access data features. Followed by, Gaussian function is presented to distribute dataset attributes. Then, NB classifier is carried for anomalous data detection. It is achieved by removing irrelevant features which resulted in improved anomaly intrusion detection accuracy. As a result, HCSO-NB method efficiently detects the intrusions in network. Thus, it classifies the data as normal or anomalous by monitoring the activities with minimum intrusion detection time.

### 3.3 SIMULATION SETTING

The proposed Hybrid module Chicken Swarm Optimization and Naive Bayes classifier (HCSO-NB) method is simulated by using Java language through NETBEANS 8.2 IDE tool. For the experimental purpose, the network anomaly detection dataset are taken from https://www.kaggle.com/anushonkar/network-anamoly-detection. The considered dataset comprises with 60438 preparing examples, 22544 occasions for testing with 42 attributes and 38 assault sorts. For detecting intrusion detection, training data and test data is presented. The performance of intrusion detection is carried with different factors such as true positive, true negative, false positive and false negative.

- True Positive specifies the number of attributes that correctly assign a classifier to the chicken swarm.
- True Negative denotes the number of attributes that does not assign a classifier to inappropriate groups
- False Positive described as the number of attributes that are incorrectly assigns a classifier to chicks swarm
- False Negative represents number of attributes that belong to the class but which the classifier incorrectly assigns to other chicks or hens

During the experimental consideration, the different number of data ranges from 1000 to 10000 is considered as input from dataset. With the use above parameter values, result analysis is carried out using proposed HCSO-NB method. The experimental analysis is performed by using following parameters.

- Intrusion detection accuracy
- Intrusion detection time

## 4. RESULT ANALYSIS OF HCSO-NB METHOD

The result analysis of proposed Hybrid module Chicken Swarm Optimization and Naive Bayes classifier (HCSO-NB) method is conducted by comparing with different existing methods. The compared methods are namely, Navies Bayes classifier by Jaya Soni and Deepak Xaxa (2016), Swarm intelligence Chicken Swarm Optimization (CSO) by Xianbing Meng et al., (2014) and new reliable hybrid method designed by Mehrnaz Mazini et al., (2019). To evaluate proposed HCSO-NB method, the following metrics are used. Performance is evaluated based on following metrics with the help of table values and graph given below.

### 4.1 Impact of intrusion detection accuracy

The anomaly intrusion detection accuracy is defined as the ratio of numbers of data that are correctly detected as normal data or anomalous data according to the total number of data taken to conduct experimental work. It is measured in terms of percentage (%) and formulated as given below equation.

$$IDA = \frac{N_{correctlydetected}}{Numberofdata} * 100 \qquad \ldots\ldots \text{Eqn (1)}$$

Using above equation (1), intrusion detection accuracy 'IDA' is estimated based on number of data. Here, 'correctly detected' specifies correctly detected data.

**Sample calculation:**

**Existing Navies Bayes classifier:** Number of data correctly detected as normal or anomalous is 760 and the total number of data is 1000. Then the intrusion detection accuracy is determined as

$$IDA = \frac{760}{1000} * 100 = 76\%$$

**Existing Swarm intelligence CSO**: Number of data correctly detected as normal or anomalous is 790 and the total number of data is 1000. Then the intrusion detection accuracy is determined as

$$IDA = \frac{790}{1000} * 100 = 79\%$$

**Existing new reliable hybrid method**: Number of data correctly detected as normal or anomalous is 830 and the total number of data is 1000. Then the intrusion detection accuracy is determined as

$$IDA = \frac{830}{1000} * 100 = 83\%$$

**Proposed HCSO-NB method:** Number of data correctly detected as normal or anomalous is 870 and the total number of data is 1000. Then the intrusion detection accuracy is determined as

$$IDA = \frac{870}{1000} * 100 = 87\%.$$

**Table 1 Tabulation of intrusion detection accuracy**

| Number of data | Intrusion detection accuracy (%) | | | |
|---|---|---|---|---|
| | Existing Naïve Bayes classifier | Existing Swarm intelligence CSO | Existing New reliable hybrid method | Proposed HCSO-NB |
| 1000 | 76 | 79 | 83 | 87 |
| 2000 | 78 | 81 | 84 | 89 |
| 3000 | 81 | 84 | 86 | 90 |
| 4000 | 81 | 83 | 85 | 92 |
| 5000 | 84 | 86 | 88 | 90 |
| 6000 | 83 | 85 | 87 | 91 |
| 7000 | 81 | 84 | 86 | 89 |
| 8000 | 85 | 87 | 88 | 90 |
| 9000 | 84 | 86 | 87 | 92 |
| 10000 | 83 | 85 | 86 | 93 |

The simulation result of intrusion detection accuracy is presented in above Table 1. From the table value, number of data in the range of 1000 to 10000 data is considered. While increasing the number of data from dataset, the intrusion detection accuracy gets varied in all the methods. Here, proposed HCSO-NB method is made comparison with existing methods such as Navies Bayes classifier by Jaya Soni and Deepak Xaxa (2016), Swarm intelligence-Chicken Swarm Optimization (CSO) by Xianbing Meng et al., (2014) and new reliable hybrid method designed by Mehrnaz Mazini et al., (2019). From the table values, proposed HCSO-NB method enhances the accuracy on intrusion detection than other existing methods.

### 4.2 Impact of intrusion detection time

The measure of time taken to classify the anomalous data is described as intrusion detection time. It is defined as the amount of time required to classify the data as normal or anomalous according to total number of data from dataset. It is measured in terms of milliseconds (ms). The intrusion detection time is measured by using following expression.

$$IDT = N * time(classifyingnormaloranomalous\ \ data) \quad \text{…… Eqn (2)}$$

The intrusion detection time '$IDT$' is estimated using equation (2) based on '$N$' number of data.

**Sample calculation:**

**Existing Navies Bayes classifier:** Time taken to detect single data as normal or anomalous is 0.032ms and the total number of data is 1000. Then the intrusion detection time is calculated as

$$IDT = 1000 * 0.032 = 32\ ms.$$

**Existing Swarm intelligence CSO**: Time taken to detect single data as normal or anomalous is 0.029ms and the total number of data is 1000. Then the intrusion detection time is calculated as

$$IDT = 1000 * 0.029 = 29\ ms.$$

**Existing new reliable hybrid method**: Time taken to detect single data as normal or anomalous is 0.026ms and the total number of data is 1000. Then the intrusion detection time is calculated as

$$IDT = 1000 * 0.026 = 26\ ms.$$

**Proposed HCSO-NB method:** Time taken to detect single data as normal or anomalous is 0.024ms and the total number of data is 1000. Then the intrusion detection time is calculated as

$$IDT = 1000 * 0.024 = 24\ ms.$$

**Table 2 Tabulation of intrusion detection time**

| | Intrusion detection time (ms) | | | |
|---|---|---|---|---|
| **Number of data** | **Existing Naïve Bayes classifier** | **Existing Swarm intelligence CSO** | **Existing New reliable hybrid method** | **Proposed HCSO-NB** |
| 1000 | 32 | 29 | 26 | 24 |
| 2000 | 39 | 36 | 34 | 32 |
| 3000 | 42 | 41 | 38 | 35 |
| 4000 | 45 | 43 | 40 | 38 |
| 5000 | 48 | 45 | 43 | 41 |
| 6000 | 51 | 49 | 46 | 45 |
| 7000 | 56 | 54 | 51 | 49 |
| 8000 | 61 | 59 | 58 | 56 |
| 9000 | 67 | 64 | 62 | 59 |
| 10000 | 69 | 67 | 65 | 61 |

The experimental performances of intrusion detection time for detailed experiment using proposed and existing methods are tabulated in above table 3.2. For the experimental purposes, different number of data that range from 1000 to 10000 data is considered from dataset. Here, proposed HCSO-NB method is compared with existing methods namely Navies Bayes classifier by Jaya Soni and Deepak Xaxa (2016), Swarm intelligence - Chicken Swarm Optimization (CSO) by Xianbing Meng et al., (2014) and new reliable hybrid method designed by Mehrnaz Mazini et al., (2019). From the table value, it is illustrative that the time for detecting intrusion using HCSO-NB method is lower when compared to other existing methods. Based on obtained values, the performance analyzes is carried as shown in below figure.

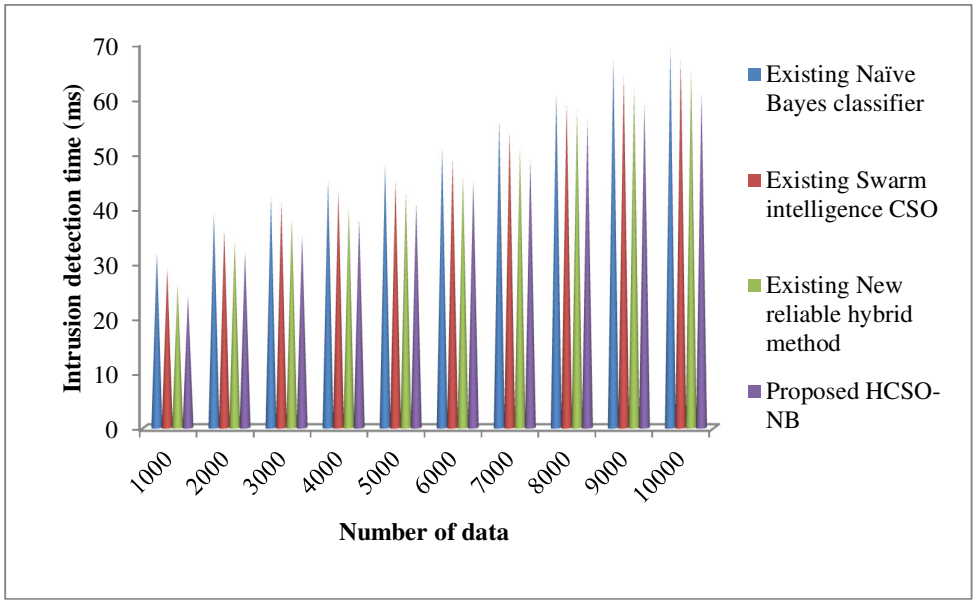


**Figure 2. Measure of intrusion detection time**

Above Figure 2 describes the measure of intrusion detection time with respect to the different number of data from dataset using proposed and existing methods. As shown in figure, proposed method provides minimized detection time on when compared to other existing methods namely Navies Bayes classifier, Swarm intelligence-Chicken Swarm Optimization and new reliable hybrid method. Besides, while varying the data for normal or anomalous data detection, the time taken for detection is also getting varied using all methods. As a result, proposed HCSO-NB method resulted with minimum intrusion detection time than the other methods.

The detection of incorrectly classified data as anomalous is detected with the use of Naive Bayes classifier. At each occurrence, the chicken swarm data is presented to differentiate the normal and anomalous data behaviour based on the optimization process. This helps for HCSO-NB method to attain minimum time to classify the anomalous data. As a result, time for intrusion detection is reduced by 15 %, 10% and 5% when compared to existing Navies Bayes classifier by Jaya Soni and Deepak Xaxa (2016), Swarm intelligence - Chicken Swarm Optimization (CSO) by Xianbing Meng et al., (2014) and new reliable hybrid method designed by Mehrnaz Mazini et al., (2019) respectively.

## 5 Conclusion

An efficient Hybrid module Chicken Swarm Optimization and Naive Bayes classifier (HCSO-NB) method is proposed for enhanced Anomaly Intrusion Detection in wireless ad-hoc network. The main objective of intrusion detection is obtained by monitoring the system activities which helps to classify the data as normal or anomalous data. It includes two different processes such as chicken swarm optimization and Naive Bayes classifier. At first, chicken swarm optimization is applied for selecting the chicken groups with attribute values for better detection of intrusion. This helps to improve the intrusion detection accuracy. After that, NB classifier is utilized on identified data groups to distinguish the malicious data and normal data. Based on the obtained data, more efficient detection on network intrusions is achieved. It classifies the nodes by monitoring chicken behaviour along with features. Hence, it effectively classifies the data and provides efficient detection of intrusion in network. Therefore, the performance results show that the HCSO-NB method improves the anomaly intrusion detection accuracy with minimum detection time than the state-of-art methods.

## References

[1] Yuk Ying Chunga, Noorhaniza Wahid, “A hybrid network intrusion detection system using simplified swarm optimization (SSO), Applied Soft Computing 12 (2012) 3014–3022

[2] A.Shanthi Sona, N. Sasirekha, “An Enhanced Hybrid Intrusion Detection Mechanism Based on Chicken Swarm Optimization and Naïve-Bayes Method”, International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-3, September 2019

[3] Fadi Salo, Ali Bou Nassif, Aleksander Essex, Dimensionality Reduction with IG-PCA and Ensemble ClassiƤer for Network Intrusion Detection, Computer Networks (2018), doi: https://doi.org/10.1016/j.comnet.2018.11.010

[4] Alaa O. Khadidos, Hariprasath Manoharan, Shitharth Selvarajan, Adil O. Khadidos, Khaled [5] H. Alyoubi, Ayman Yafoz, “A Classy Multifacet Clustering and Fused Optimization Based Classification Methodologies for SCADA Security”, Energies 2022, 15, 3624. https://doi.org/10.3390/en15103624

[5] Beatriz Flamia Azevedo, Ana Maria A. C. Rocha, Ana I. Pereira, “Hybrid approaches to optimization and machine learning methods: a systematic literature review”, Machine Learning Springer 2023 https://doi.org/10.1007/s10994-023-06467-x

[6] Zhenwu Wang, Chao Qin, Benting Wan, William Wei Song, Guoqiang Yang, “An Adaptive Fuzzy Chicken Swarm Optimization Algorithm”, Mathematical Problems in Engineering, Volume 2021, Hindawi, Article ID 8896794, 17 pages https://doi.org/10.1155/2021/8896794

[7] M. Bakro et al.: Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms, IEEE Access Volume 12, 2024

[8] Mohammad Azmi Ridwan, Nurul Asyikin Mohamed Radzi, “A New Machine Learning-based Hybrid Intrusion Detection System and Intelligent Routing Algorithm for MPLS Network”, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 14, No. 4, 2023

[9] Mr Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kishan, “International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com, Volume 5, Issue 2 (March - April 2017), PP. 38-44

[10] Dr.A.Shanthisona & Dr.A.Krishnaveni, “Analysis of Intrusion Detection Based On Swarm Intelligence And Classifier Techniques” GIS SCIENCE JOURNAL, VOLUME 10, ISSUE 4, PP.269-281, 2023

[11] F. Cauteruccio, L. Cinelli, E. Corradini, G. Terracina, D. Ursino et al., “A framework for anomaly detection and classification in multiple IoT scenarios,” *Future Generation Computer Systems*, vol. *114*, pp. 322–335, 2021.

[12] M. N. U. Islam, A. Fahmin, M. S. Hossain and M. Atiquzzaman, “Denial-of-service attacks on wireless sensor network and defense techniques,” *Wireless Personal Com.s*, vol. *116*, pp. 1993–2021, 2020.

[13] X. Lu, D. Han, L. Duan and Q. Tian, “Intrusion detection of wireless sensor networks based on IPSO algorithm and BP neural network,” *International Journal of Computational Science and Engineering*, vol. *22*, no. *2–3*, pp. 221–232, 2020.

[14] K. Khan, A. Mehmood, S. Khan, M. A. Khan, Z. Iqbal et al., “A survey on intrusion detection and prevention in wireless ad-hoc networks,” *Journal of Systems Architecture*,vol. *105*, no. *September 2019*, pp. 101701, 2020.

[15] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," *Telecommunication Systems*, vol. *73*, no. *1*, pp. 3–25, 2020.

[16] W. Zhang, D. Han, K. C. Li and F. I. Massetto, "Wireless sensor network intrusion detection system based on MK-eLM," *Soft Computing*, vol. *24*, no. *16*, pp. 12361–12374, 2020.

[17] D. Praveen Kumar, T. Amgoth and C. S. R. Annavarapu, "Machine learning algorithms for wireless sensor networks: A survey," *Information Fusion*, vol. *49*, pp. 1–25, 2019.

[18] J. Cheng, J. Zhou, Q. Liu, X. Tang and Y. Guo, "A DDoS detection method for socially aware networking based on forecasting fusion feature sequence," *Computer Journal*, vol. *61*, no. *7*, pp. 959–970, 2018.

[19] T. Kaur, K. K. Saluja and A. K. Sharma, "DDOS attack in WSN: A survey," in 2016 Int. Conf. on Recent Advances and Innovations in Engineering, Jaipur, Rajasthan, India, pp. 23–27, 2016.

[20] I. Almomani, B. Al-Kasasbeh and M. Al-Akhras, "WSN-Ds: A dataset for intrusion detection systems in wireless sensor networks," *Journal of Sensors*, vol. *2016*, pp. 41525–41550, 2016.

[21] O. Can and O. K. Sahingoz, "A survey of intrusion detection systems in wireless sensor networks," in 2015 6th Int. Conf. on Modeling, Simulation, and Applied Optimization (ICMSAOIstanbul, Turkey, pp. 1–6, 2015.

[22] W. Li, P. Yi, Y. Wu, L. Pan and J. Li, "A new intrusion detection system based on knn classification algorithm in wireless sensor network," *Journal of Electrical and Computer Engineering*, vol. *2014*, pp. 1–8, 2014.

[23] L. Coppolino, S. DAntonio, A. Garofalo and L. Romano, "Applying data mining techniques to intrusion detection in wireless sensor networks," in 2013 Eighth Int. Conf. on P2P, Parallel, Grid, Cloud and Internet Computing, Compiegne, France, pp. 247–254, 2013.

[24] A. Garofalo, C. Di Sarno and V. Formicola, "Enhancing intrusion detection in wireless sensor networks through decision trees," In: Vieira, M., Cunha, J. C. (Eds.*Dependable Computing*, Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 1–15, 2013.