INSTITUTE OF ENGINEERING & TECHNOLOGY

UGC Autonomous

Accredited by NAAC & NBA, Approved by AICTE & Permanently Affiliated to JNTUH

DECENTRALIZED INTRUSION PREVENTION (DIP) AGAINST CO-ORDINATED CYBERATTACKS ON DISTRIBUTION AUTOMATION SYSTEMS

UNDER THE GUIDANCE OF

DR. R.VIJAYANAND

ASSISTANT PROFESSOR

SUBMITTED BY

B.PRAVALLIKA(17671A0558)

B.BHARGAVI(17671A0563)

N.ESHWITHA(17671A0568)

RITIKA KALYANI(17671A0596)

ABSTRACT

- Integration of Information and Communications Technology (ICT) into the distribution system makes today's power grid more remotely monitored and controlled than it has been. Thus, research into intrusion detection systems at the distribution level is in critical need.
- This presents an approach toward intrusion prevention at the distribution system level. Simulations of the method have been performed on the dataset CICIDS2017.
- In this project, we are using Whale Optimization algorithm with KNN (K-Nearest Neighbor) classifier.
- The results have validated the performance of the proposed method for protection against cyber intrusions at the distribution system level with 98.42% accuracy.

INTRODUCTION

- Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity.
- Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because both IPS and IDS operate network traffic and system activities for malicious activity.
- Types of intrusion prevention systems

1. NIPS(network-based intrusion prevention system)
2. HIPS(host-based intrusion prevention system)

EXISTING METHOD

- PARTICLE SWARM OPTIMIZATION
- GENETIC ALGORITHM
- GREY WOLVES OPTIMIZATION
- FIREFLY ALGORITHM

DISADVANTAGES :

- Cannot work out problems of scattering
- Can converge prematurely and trapped into local minimum especially with complex problems
- Cannot give optimal solutions

PROPOSED METHOD

WHALE OPTIMISATION ALGORITHM WITH KNN CLASSIFIER:

- Novel Whale Optimization approaches are proposed for feature Selection .
- A superior performance of the proposed approaches is proved in the experiments by evaluating the fitness of each feature set.
- The KNN algorithm assumes that similar things exist in close proximity and is used for classification of trained data.
- The simulation results proved the suitability of the improved WOA-based feature selection method for the IDS.

PROPOSED METHOD

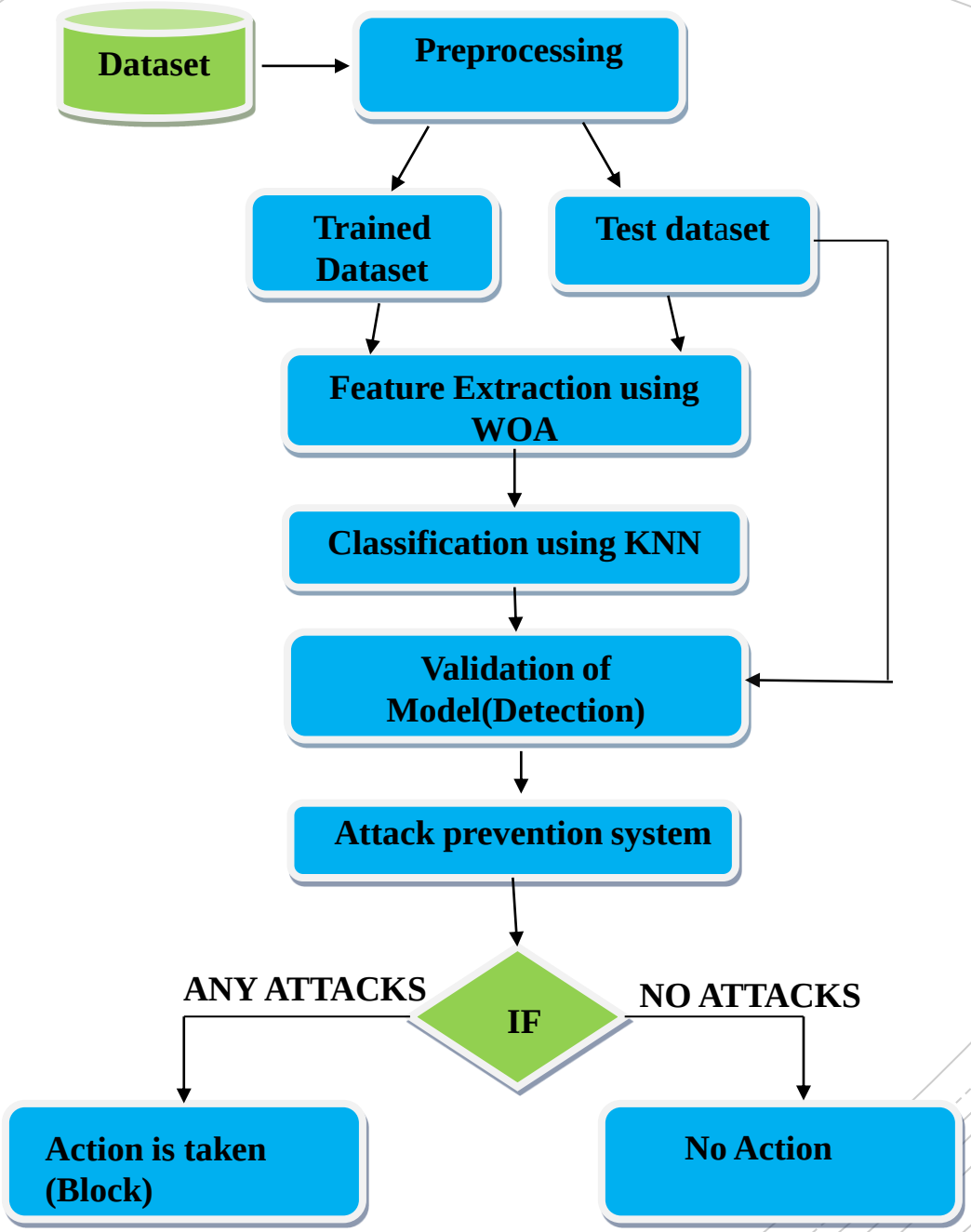
ADVANTAGES

- Appropriate for solving different optimization problems
- Helps to get global optimization solutions

APPLICATIONS

- Feature selection
- Optimal power flow problem
- 5G wireless networks
- Workflow planning of construction sites
- Neural Network training

PROPOSED ARCHITECTURE



SYSTEM REQUIREMENTS

SOFTWARE REQUIREMENTS

- Operating System : Windows10 (64 bit)
- Front End : Python
- Tool Used : Python IDLE 3.8
- Packages : Numpy, Pandas, Sklearn, Matplotlib

HARDWARE REQUIREMENTS

- Processor : Dual core
- Ram : 16 GB (minimum)
- Hard Disk : 20GB

MODULES

- PREPROCESSING
- FEATURE EXTRACTION
- CLASSIFICATION
- VALIDATION
- ATTACK PREVENTION

DATASET

- **CICIDS2017** dataset contains benign and the most up-to-date common attacks, which resembles the true real-world data (PCAPs). It also includes the results of the network traffic analysis using CICFlowMeter with labeled flows based on the time stamp, source, and destination IPs, source and destination ports, protocols and attack (CSV files).

PREPROCESSING

- Data preprocessor is concerned with collecting the data from the dataset provided and converting it into a format that is understandable by the intrusion detector.
- The dataset is passed through several preprocessing steps:

- The removal of labels
- Removing features
- Label encoding
- Data binarization

TRAINING AND TESTING

- The dataset after preprocessing is split into two sets.Trained data is used to train the model and the testing data is used to validate the model.

- We use ‘train_test_split’ function to split the data. Optional parameter ‘test_size’ determines the split percentage.

FEATURE SELECTION USING WOA

- Feature selection selects representative set of attributes from the set of original attributes. This representative set keeps only the relevant and important attributes, learning algorithm takes less time to learn and produces a more general classifier as it removes unnecessary and irrelevant attributes for the original set.

- Novel Whale Optimization approaches are proposed for feature Selection .

CLASSIFICATION USING KNN

- The k-nearest neighbors (KNN) algorithm is a simple, easy-to-implement supervised machine learning algorithm that can be used to solve both classification and regression problems.
- The KNN algorithm assumes that similar things exist in close proximity. In other words, similar things are near to each other.
- It keeps all the training data to make future predictions by computing the similarity between an input sample and each training instance.

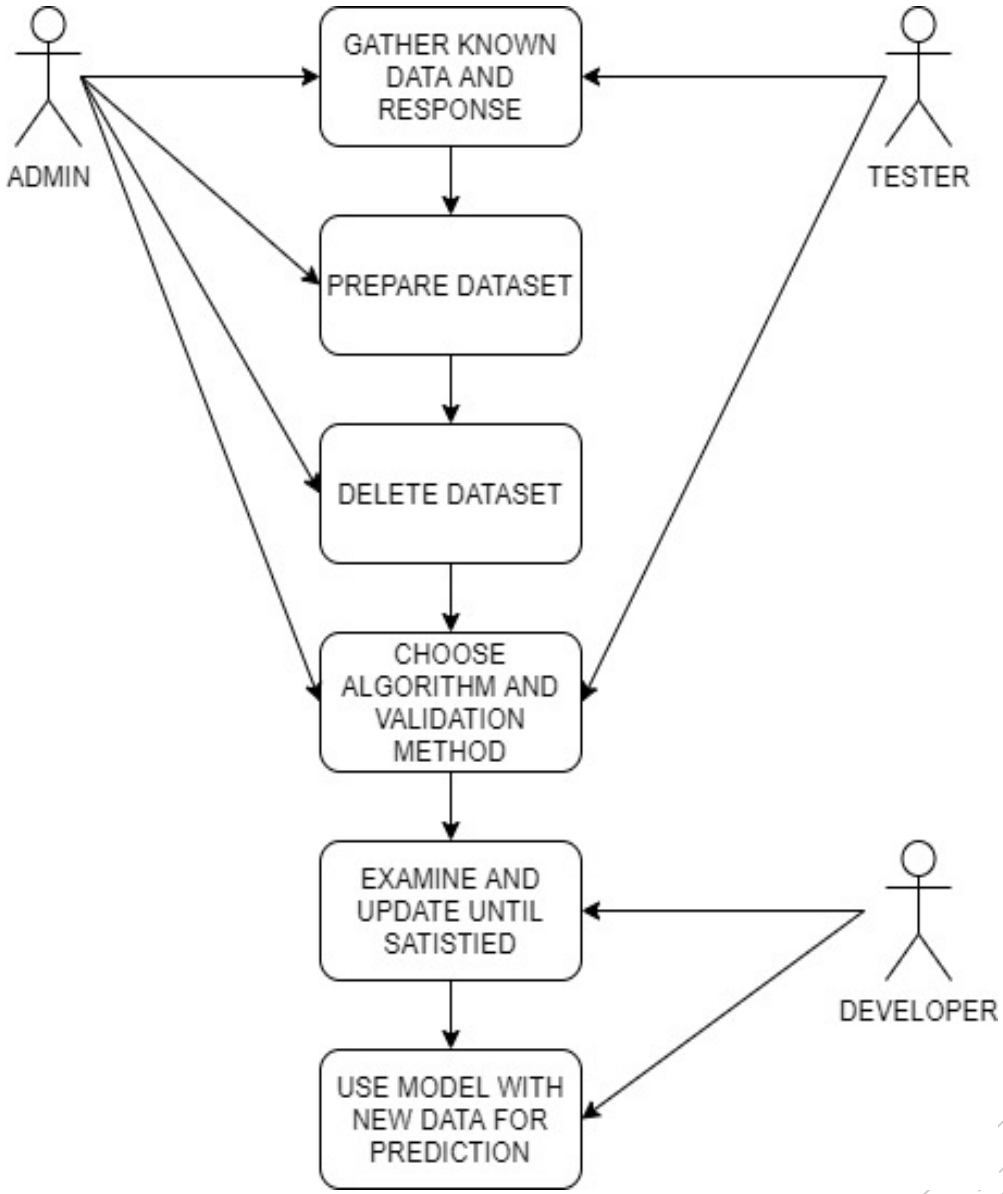
VALIDATION OF MODEL

- Model Validation is the task of confirming that the outputs of a statistical model have enough fidelity to the outputs of the data-generating process that the objectives of the investigation are achieved.
- Records matching to the normal class are considered as normal data, and the other records are reported as attacks.

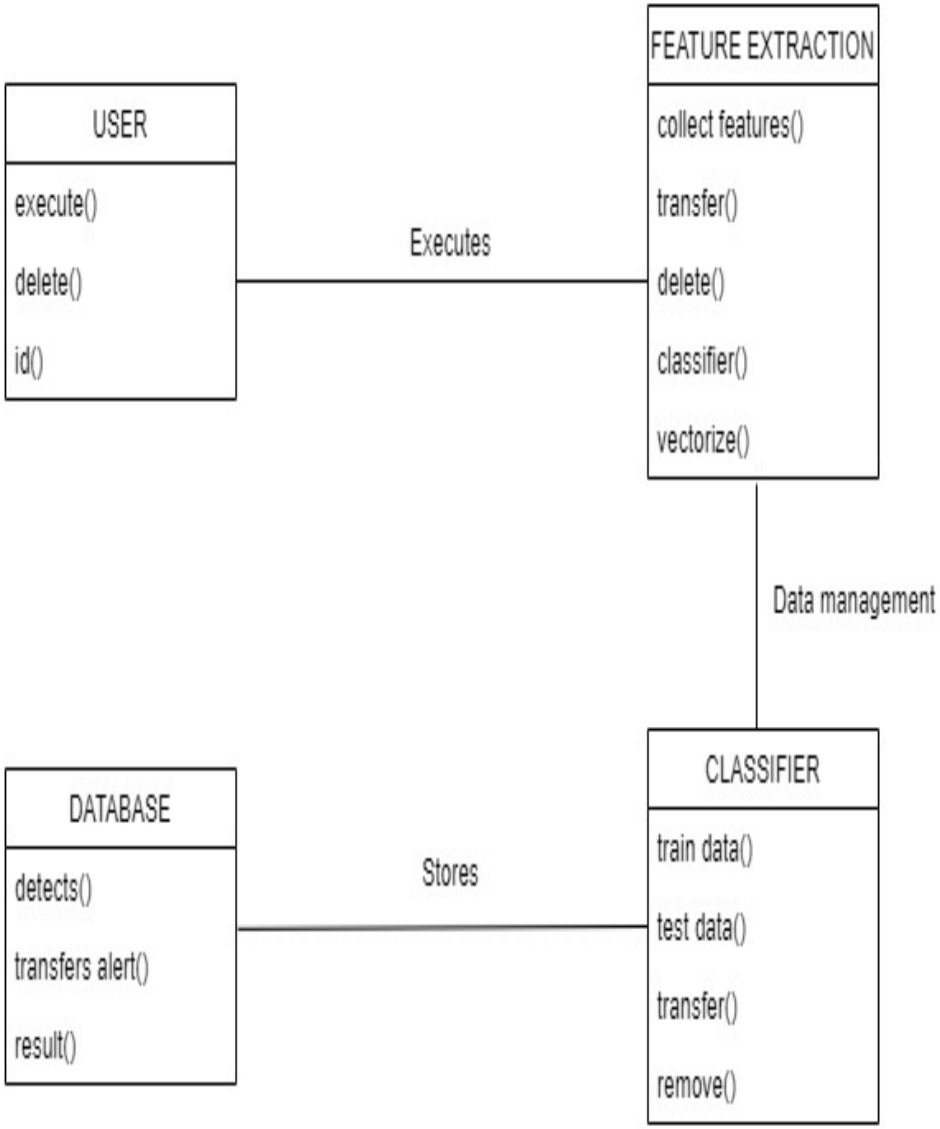
ATTACK PREVENTION:

- Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.
- If there is any malicious activity encountered then the system is blocked and shares that information to the other system.
- In this way the anomaly/intrusion can be prevented. And if there are no malicious traffic the system performs no action and allows good traffic to pass through.

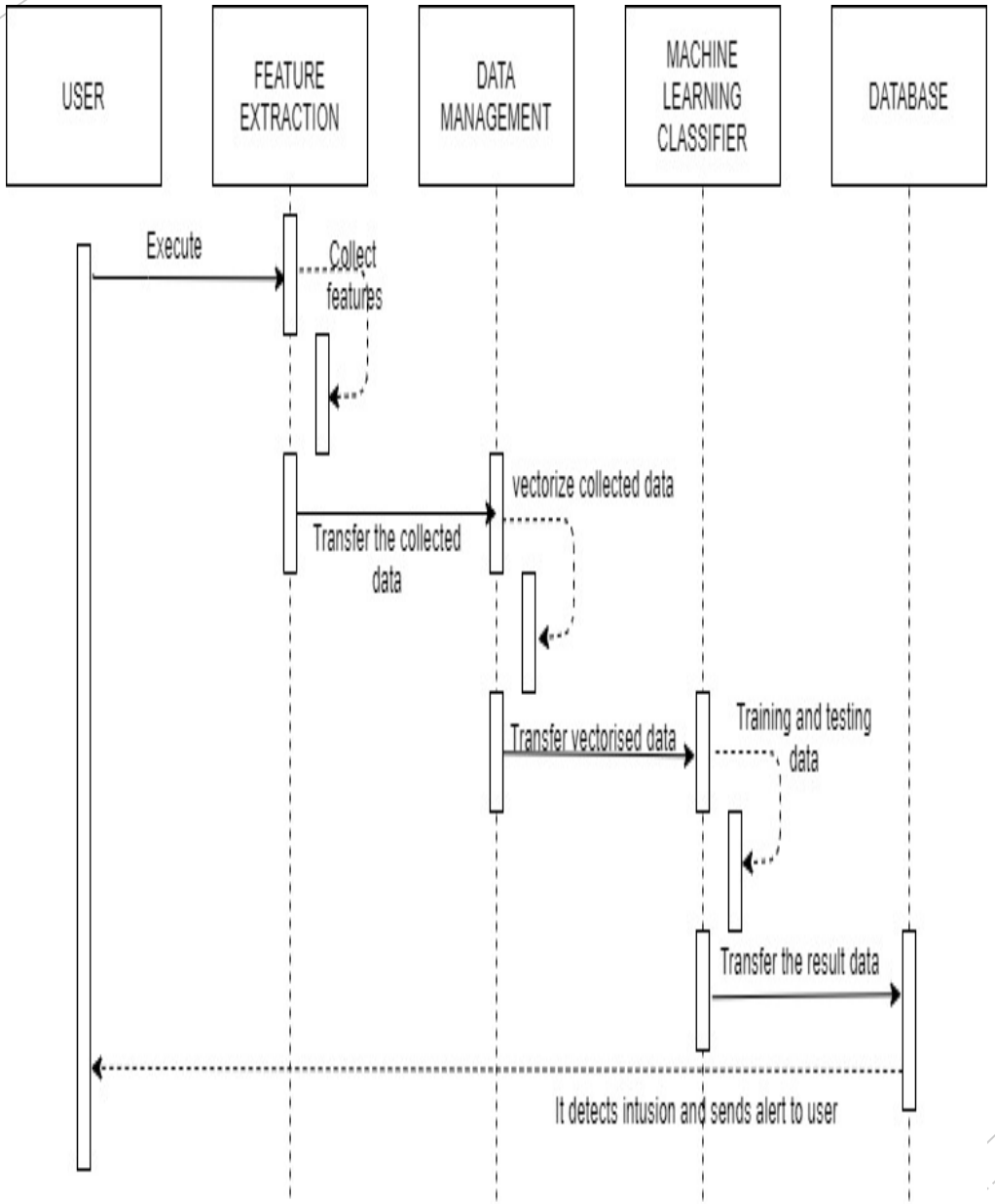
USE CASE DIAGRAM



CLASS DIAGRAM



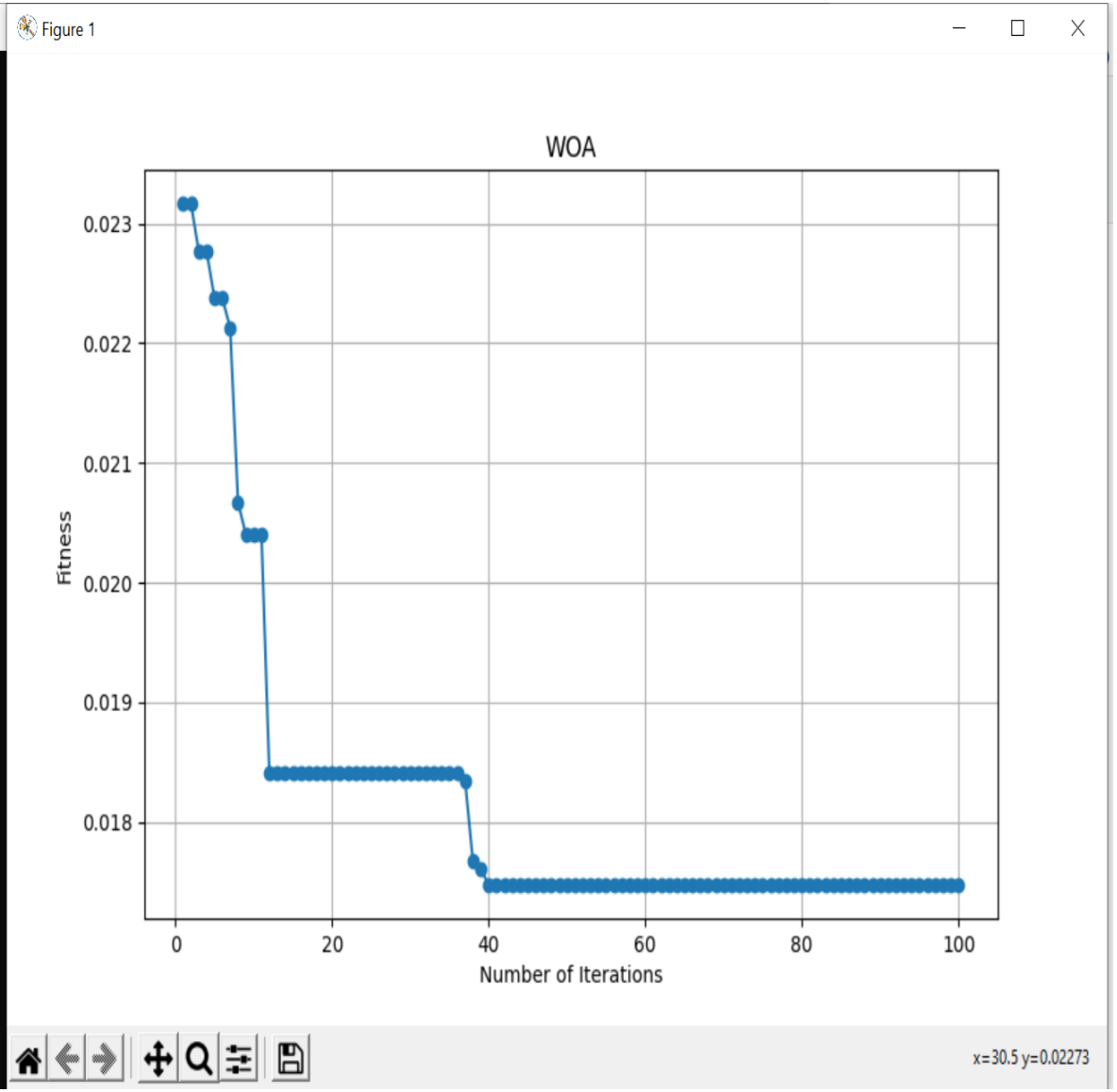
SEQUENCE DIAGRAM



OUTPUT SCREEN

C:\WINDOWS\py.exe

```
Generation: 83
Best (WOA): 0.017477185908319145
Generation: 84
Best (WOA): 0.017477185908319145
Generation: 85
Best (WOA): 0.017477185908319145
Generation: 86
Best (WOA): 0.017477185908319145
Generation: 87
Best (WOA): 0.017477185908319145
Generation: 88
Best (WOA): 0.017477185908319145
Generation: 89
Best (WOA): 0.017477185908319145
Generation: 90
Best (WOA): 0.017477185908319145
Generation: 91
Best (WOA): 0.017477185908319145
Generation: 92
Best (WOA): 0.017477185908319145
Generation: 93
Best (WOA): 0.017477185908319145
Generation: 94
Best (WOA): 0.017477185908319145
Generation: 95
Best (WOA): 0.017477185908319145
Generation: 96
Best (WOA): 0.017477185908319145
Generation: 97
Best (WOA): 0.017477185908319145
Generation: 98
Best (WOA): 0.017477185908319145
Generation: 99
Best (WOA): 0.017477185908319145
Generation: 100
Best (WOA): 0.017477185908319145
Accuracy: 98.42069892473118
Feature Size: 14
```



CONCLUSION

- In this project, we proposed a novel feature selection method using WOA feature selection.
- The proposed method selects the most informative features from the network data. The selected informative features help to improve the accuracy of the KNN-based IDS.
- We evaluated the performance of the proposed method by using CICIDS2017 dataset.
- A comparison of the proposed method with the other feature selection algorithms on the basis of detection rate, execution time, and computational complexity proved the efficiency of the proposed method.

REFERENCES

- [1] Ahmad, I.; Abdullah, A.; Alghamdi, A.; Alnfajan, K.; Hussain, M. Intrusion detection using feature subset selection based on MLP. Sci. Res. Essays 2011, 6, 6804–6810.
- [2] Syarif, I. Feature selection of network intrusion data using genetic algorithm and particle swarm optimization. EMITTER Int. J. Eng. Technol. 2016, 4, 277–290.
- [3] Devi, E.M.; Suganthe, R.C. Feature selection in intrusion detection grey wolf optimizer. Asian J. Res. Soc. Sci. Humanit. 2017, 7, 671–682.
- [4] Selvakumar, B.; Muneeswaran, K. Firefly algorithm based feature selection for network intrusion detection. Comput. Secur. 2019, 81, 148–155.
- [5] S. Mirjalili and A. Lewis, "The whale optimization algorithm", *Adv. Eng. Softw.*, vol. 95, pp. 51-67, May 2016.

THANK YOU