1. **Optimal Support Vector machine-based Intrusion detection system:**

Wireless Sensor Networks (WSNs) are typically less basic, distributed, and dynamic [1]. The best example of wireless sensor networks is computing. To meet the objectives of mobility support, geo-distribution, position details and a limited delay requirement for Internet of Things (IoT), Fog nodes must serve as users in IoT execution. The limitations of Wireless Sensor Networks (WSNs) make them vulnerable to a variety of factors which can impact their efficacy. Protocols that are authorized and have secure routing imply the use of cryptographic keys to ensure an efficient and effective transmission that is not vulnerable to passive attacks. Attack data from valuable sources is viewed as passive because nodes are always at the risk of being attacked.

In [2] a new support vector machine (SVM)-based intrusion detection system (IDS) is presented for wireless sensor networks (WSNs). This model involves the selection of optimal kernels in the SVM model using the whale optimization algorithm (WOA) for intrusion detection. Since the SVM kernel is altered using WOA, the application of OSVM model can be used to detect intrusions with proficient results. The OSVM model has been investigated on KDDCup 99 dataset.

1. **Working:**

Diagram

Description automatically generatedThe principle behind the working is illustrated in Figure 1 [1]. The OSVM model incorporates intrusion detection using three sub-processes: pre-processing, classification, and kernel selection. The input data is processed to make it more usable. The OSVM model is used to classify the intrusions. There is a new OSVM-based IDS that uses kernels tunes for specific applications. Thirdly, the model relies on the skilled selection of optimal kernels in a SVM.

Figure 1 Working of OSVM model [1]

Here, a machine learning algorithm is used to predict when a intruder will enter a specific area. The Modified Whale Optimization Algorithm (MWOA) was used to select the best kernel in a SVM classification model. A kernel function used in SVM, K (xn, xi) converted the actual data space into novel space with maximum dimension. The accuracy of WOA models can be improvised by assigning objective function values to randomly generated measures. The process is carried out in four phases as below:

1. Encircling Prey Phase

Here the whale examines the prey and finds actual location. It surrounds the prey as if it doesn’t want to escape from it which is measures by below equations [1]

Where A and C are coefficient vectors as shown below:

1. Exploitation Phase

It refers to the implementation of two models called shrink encircling technique and spiral updating position. Whales optimize the location defined in the following equation [1]:

Numerically the above expression is represented as

Where *p* belongs to [0,1].

1. Exploration Phase

The position is updated with respect to randomly selected reference whale that is decided using the below equations [1]:

WOA is modified by estimation of random measures r1 and r2  as shown in below equations[1] resulting in MWOA

Where fmx and fmn  denotes higher and lower values of fitness function (FF)

1. Objective function

Accuracy of WOA is improved by estimating objective function as shown in below equation [1]:

Where tp and tn denotes true positive and true negatives, fp and fn denotes false positive and false negatives.

1. **Evaluation:**

Table 1 [1] shows the different types of data that were collected for this study. The results of the OSVM model are compared with existing methods, and the OSVM model is found to be more accurate. The results show that the OSVM model is more effective than the other techniques in classifying data. It can be seen that the SVM and ELM methods have resulted in accuracy values of 88.20% and 87.90%, respectively. Both the HIDS and ML-ELM techniques have yielded acceptable accuracy rates of 91.26% and 92.10% [1], respectively. However, the OSVM model has achieved a high accuracy of 94.90%, The SVM method has resulted in a limited TPR value of 83.73%. The ELM model has been found to produce reasonable outcomes with a total positive rate of 83.84%. According to the MK-ELM method, its TPR is currently at 89.42%. OSVM has achieved a highest value of 95.53% TPR.

Table

Description automatically generated

Table 1 Comparison between OSVM and other models

1. **References:**

[1] Amaran, S., & Mohan, R. M. (2021). Intrusion Detection System using Optimal Support Vector Machine for Wireless Sensor Networks. *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, (pp. 1100-1104).

[2] Baraneetharan, E. (2020). "Role of Machine Learning Algorithms Intrusion Detection in WSNs: A Survey. *Journal of Information Technology 2, no. 03*, 161-173.

[3] Liang, D., & Pan, P. (2019). Research on Intrusion Detection Based on Improved DBN-ELM. *2019 International Conference on Communications, Information System and Computer Engineering(CISCE)*, (pp. 495-499).

[4] Smys, S., Basar, A., & Wang, H. (2020). Hybrid Intrusion detection System for Internet of Things (IoT). *Journal of ISMAC 2*, 190-199.