International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Feature Vector Generation with Multi Level Classification using Particle Swarm Optimization Model for Intrusion detection

Battini Sujatha [1], Dr. Sammulal Porika [2]

Submitted:15/05/2024 **Revised:** 28/06/2024 **Accepted:** 05/07/2024

Abstract: The Network Intrusion Detection System (NIDS) is used to detect malicious activities on a network. Machine Learning (ML) techniques are heavily leveraged in the NIDS for intrusion detection. When it comes to enhancing NIDSs' functionality, feature selection is crucial. This is because intrusion identification uses numerous features, each of which must be processed individually. Therefore, the feature selection method impacts the time required to probe traffic behaviour and enhance accuracy. An Intrusion Detection System (IDS) with a powerful intrusion detection mechanism is highly desirable for preventing network intrusion. Despite all the effort put into them, intrusion detection systems are not very effective because of the frequent false positives they produce. Using a raw dataset with redundancy is a common source of false positives. Feature selection, which can boost intrusion detection performance, is required to fix this problem. In this research, we have used a Multi-Level Classification model using Feature Ranking Strategy to perform feature selection (FS) with the goal of eliminating superfluous features. The underlying process of intrusion detection is improved as a result. The false alarm rate was reduced, the detection rate was increased, and the accuracy of the IDS was improved when the Particle Swarm Optimization (PSO) algorithm was used to the selectable features of the NSL-KDD dataset. In order to manage numerous types of attacks, a Rational Multi Level Classification with Feature Ranking Strategy using PSO (RMLC-FRS-PSO) model is designed for accurate detection of intrusions in the network. The proposed model when contrasted with the existing models reduces the false alarms and enhances the network performance.

Keywords: *Intrusion Detection System, Feature Vector, Particle Swarm Optimization, Multi Level Classification, Attacks, False Alarms.*

1. Introduction

Identifying risks and irregularities in a data network and developing systems for IDS to promote cyber security [1]. A practical data-driven intrusion detection technique was developed using artificial intelligence (AI) [2], more especially ML techniques. In terms of business transactions, sources of information, networking, including socialization, to mention a few, cyberspace has completely changed the world [3]. Both the number of users of virtual networks and the economic prosperity of nations have benefited greatly from it. On the other hand, the increasing sophistication of information systems security is closely related to the development in internet accessibility [4]. Computer system competence is developing and getting better every day as a result of its increasing success. Blocking every security breach seems unfeasible right now, but attempts at intrusion may be detected, and precautions are taken to lessen the impact of the attack on the computer network [5].

An increasingly useful tool for keeping monitoring for unusual activity and alerting administrators to potential threats is the IDS [6]. Due to the nonlinear behavior caused by the intrusions, the system becomes unpredictable for network traffic. An IDS is necessary because intrusions and attacks, such as spoofing, traffic analysis, cyber-attacks [7], and other damaging vulnerabilities, threaten the security principles of availability, confidentiality, and integrity. When it comes to intrusion detection systems, there are essentially two main types: signature-based and anomaly-based [8]. Another name for the signature-based approach is misuse-based detection. This method checks for matches between the signatures of known harmful actions and sounds an alarm if one is detected [9]. As a result, these systems can accurately identify suspected assaults with few false positives. Systems based on anomalies can handle zero-day assaults with ease. This method keeps monitoring systems' patterns and sounds an alarm if any of them start acting strangely [10]. A high false-positive rate

1 Telangana Social Welfare Residential Degree College for women, Scholar of Computer science and Engg, JNTUH, battinisujata@gmail.com
2 Professor Department of computer science and Engg, JNTUH, College of Engineering, sam@jntuh.ac.in

(FPR) occurs with this method. Both host-based and network-based intrusion detection systems fall under the umbrella of NIDS. Based on the local host's system calls, log files [11], application logs, and other host actions, the HIDS monitors the individual hosts and issues alarms [12]. But NIDS watches every bit of data as it travels over the network, and it notifies the administrator anytime something suspicious that fits the profile of a known attack. As the number of features grows, so does the system's complexity [13].

Because of this, the IDS had a hard time processing the massive amounts of data. In order to detect intrusions in the sphere of information security, it is vital to pick helpful and critical features [14]. Prior to pre-processing, it is necessary to identify important traits in order to construct an acceptable and effective IDS [15]. Since the dataset is expressed by a variety of relevant, irrelevant, and extravagant features, which increase the complexity of computation for the analysis of incursions, it is challenging to identify the important features [16]. The primary goal of feature selection (FS) is to enhance the predictor's quality and performance. In order to improve the effectiveness of IDS with minimal computational complexity [17], this research recommends using a set of reduced features for optimal feature selection. Therefore, FS is employed to improve classifier performance and reduce irrelevant attributes [18].

Being scalable, dispersed, dynamic, fault tolerant, and having inadequate infrastructure makes wireless sensor networks (WSNs) susceptible to a wide range of security threats. These networks are thus vulnerable to a wide range of security risks [19]. Proposing effective and efficient feature selection technique and classification architecture for intrusion in WSNs is the main topic of this work. Intrusion detection systems rely on classification to determine if system behavior is normal or intrusive [20]. A classifier's or invasive analysis engine's performance is heavily influenced by the feature space of the classification task. In addition, there are many features in a dataset, including relevant, irrelevant, and duplicate ones, making it difficult to identify which ones are significant [21]. Classification isn't the place for irrelevant or superfluous features since they muddle up the system and impact the beneficial features. In order to improve the classifier performance, decrease the amount of features, and increase feature space quality, feature selection is essential [22]. The multi label classification general process is shown in Figure 1.

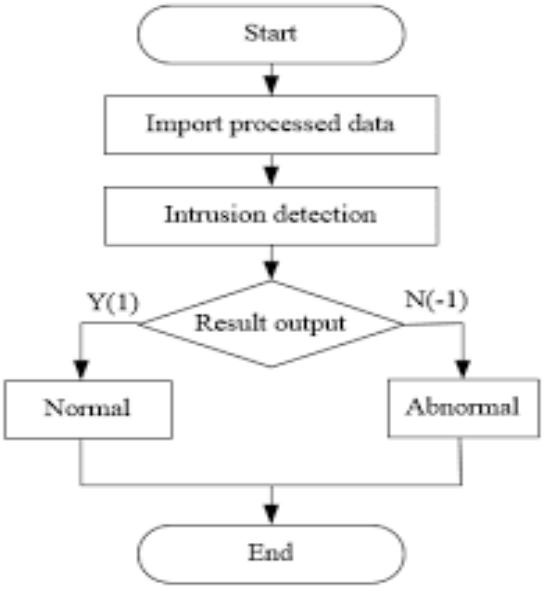

Fig 1: Multi Level Classification General Process

Consequently, intrusion detection has a significant challenge with feature selection. Although feature extraction and intrusion categorization have received considerable attention in the past, feature selection has received less attention [23]. Consequently, it is believed that improving the classifier's performance requires an ideal feature subset. Many different search strategies have been used to improve feature selection in order to circumvent this problem. However, there are a

number of issues with the current approaches, such as the high computational cost, increased memory utilization, and complexity of the classifier architecture [24]. IDS becomes essential when it is discovered that intrusion prevention mechanisms such as firewalls, admittance regulators, and encoding, to name a few are not enough to counter the danger to device and network security. It is important to stress the significance of IDS core design terminologies for performance and assessment [25]. By utilizing machine learning techniques, AI with intrusion aims to offer a smart IDS for network safety as an extra layer of defense. An approach to monitoring and analyzing events in a computer environment to identify signs of infiltration is called intrusion detection.

PSO is employed in this research for the optimization of threshold to accomplish maximum class variance within normal and anomaly networks. PSO is an optimization technique that has strong comprehensive search capabilities and applicable for dimensional optimization. The expertise or expertise affects the particle moving inside the swarm [26]. The search is processed to return to earlier active provinces in the search space as a result of simulation for this social activity. In this research, PSO is proposed and implemented for optimal feature selection. PSO is an effective and efficient global search technique [27]. It is an appropriate algorithm to address feature selection problems due to better representation, capability of searching large spaces, being less expensive computationally, being easier to implement, and fewer parameters being required. The general process of PSO is shown in Figure 2.

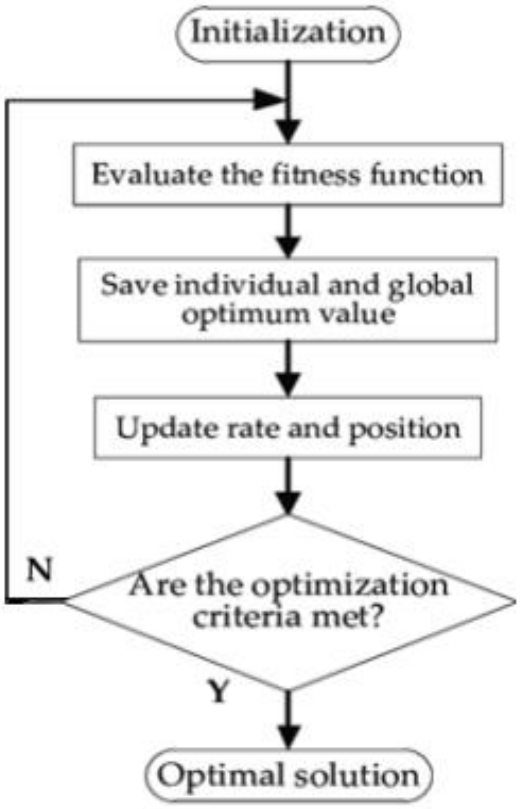

Fig 2: Flowchart for Particle Swarm Optimization

When data flows via the network systems, NIDSs label it as normal or abnormal and generate an alarm report accordingly. There have been numerous attempts by researchers to address the classification issue in IDS, however these methods still have a flaw in that they produce inaccurate attack classifications. Since they are the initial line of defense against cyber threats and are accountable for properly detecting any possible incursion in the network, IDSs are key components in an organization's network security [28]. The detection of possible threats is accomplished by many IDS implementations through flow-based network traffic analysis. There has been a lot of new thinking and development in the area of network security research recently, with a focus on IDS. In order to manage numerous types of attacks, a Rational Multi Level

Classification with Feature Ranking Strategy using PSO model is designed for accurate detection of intrusions in the network.

2. Literature Survey

As computer network technology advances and network systems expand, there is an increased risk of hacker attacks on sensitive data. An active defensive network security mechanism called intrusion detection is used to identify processes through attempted intrusions, current intrusions, or already-occurring intrusions. The intrusion detection method's detection rate is currently low, its false alarm and false alarm rate are high, and its real-time performance is subpar. Better detection performance requires a big number of complete data. The concept, traits, categorization, research topics, and challenges of conventional intrusion detection for large-scale multimedia data transmission networks are explained in this study by Guo et al. [1]. Next, the fundamentals of neural networks, the method known as PSO algorithm, and the algorithm for particle swarm optimization with quantum behavior (QPSO) are presented. It is highlighted that in global optimization problems, QPSO performs better at convergence than PSO method. This study presents the notion, properties, and architecture of neural networks along with the method and categorization of wavelet neural networks. The specific operating procedure is then provided, utilizing the QPSO method as the training method and the wavelet neural networks for the object.

Numerous issues with network security have arisen as a result of the network's quick development and growing popularity. Network protection frequently use intrusion detection technology as an efficient security tool. As a traditional deep learning model, a deep belief network (the DBN) performs well in classification and is frequently applied to intrusion detection. On the other hand, DBN's network structure is typically determined by actual usage. In order to optimize the DBN's network topology, Wei et al. [2] presented a new joint optimization approach for the intrusion detection and classification model (DBN-IDS) optimization problem. Initially, the author created a form of PSO using the learning factor and adaptive inertia weight. Second, the author optimized the PSO in order to identify the initial optimisation solution by utilizing the cluster, scavenging and other behaviors of fish swarms. Next, the author enhanced the PSO to search for the global optimization result using genetic operators having self-adjusting crossing probability as well as mutation probability based on the first optimization solution. Lastly, the network topology of the malware detection classification model is derived from the global optimization approach created by the aforementioned joint optimization technique.

The World Wide Web of Things, or IoT for short, is progressively encroaching into a variety of fields with the arrival of the "Internet plus" era, and the size of its technology is also exhibiting a rapid expansion trend. The Internet of Everything era is rapidly approaching. IoT is more susceptible to different types of intrusion assaults because of its integration as well as diversification of terminals and apps. Designing a system for intrusion detection that ensures the security, integrity, and dependability of the Internet of Things is therefore very crucial. The limitations of traditional intrusion detection technologies include low detection rates and limited scalability, making it unable to adjust to the dynamic and complex IoT environment. In this article, Liu et al. [3] proposed a gradient descent method for intrusion detection based on particle swarm optimization (PSO-LightGBM). This method uses one-class SVM to find and identify harmful data after PSO-LightGBM is applied to extract the distinctive characteristics of the data. The intrusion detection algorithm is validated using the UNSW-NB15 dataset.

Because of the high dimensional features and high noise levels in power system measurement data, it is challenging to use this information for direct intrusion detection. Conventional data mining techniques applied to the area of network for intrusion detection employ feature analysis for an initial processing phase and execute separate from the learning process, which makes the characteristics not well fitted to the training. Han et al. [4] offered a unique binary particles swarm-wrapped selection of features optimization framework (BPSWO) to enhance the coupling between feature selection and training, hence increasing the accuracy with which machine learning systems identify intrusions. The approach first uses the enhanced transfer function to arrive to the globally optimal particle. Second, the conventional particle swarm optimization's early difficulty is addressed with the help of the stochastic conversion and the Hamming distance. Particle swarm training can then incorporate the various classifiers. While picking features, the BPSWO

educates the classifier, and the resulting classifier is then used for detection of intrusions. The Oak - Ridge -National Laboratory public electricity system and the IEEE 57-bus system are used to test the suggested solution.

A supervised system for intrusion detection is one that can identify new assaults by using instances of past attacks as a source of learning. Because artificial neural networks (ANNs) can learn from real-world instances, using ANN-based intrusion detection holds potential for lowering the frequency of false positives or false negatives. Ali et al. [5] proposed PSO-FLN, an established learning model for rapid learning networks (FLN) based on the optimization of particle swarms (PSO). The model has been used to solve the intrusion detection problem and has been verified using the well-known KDD99 dataset. A common tool for protecting networks and detecting intrusions is the network attack detection system (NIDS), yet one of its main drawbacks is the false positive problem. Jiang et al. [6] suggested the PSO-Xgboost models based on the comparative experiments as well as evaluation of the features of Xgboost and PSO. Its overall classification accuracy is higher than that of other alternative models, including Xgboost, Random Forest, Bagging, and Adaboost. Xgboost is first utilized to build a classification model, and then PSO is employed to adaptively seek for Xgboost's ideal structure. The suggested model is assessed using the standard NSL-KDD dataset.

As computer network technology advances and network systems expand, there is an increased risk of hacker attacks on sensitive data. An active defensive network security mechanism called intrusion detection is used to identify processes through attempted intrusions, current intrusions, or already-occurring intrusions. The intrusion detection method's detection rate is currently low, its false alarm and false alarm rate are high, and its real-time performance is subpar. Better detection performance requires a big number of complete data. The concept, traits, categorization, research topics, and challenges of conventional intrusion detection for large-scale multimedia data transmission networks are explained in this study. Next, the fundamentals of neural networks, the particle swarm optimization (the method of PSO) algorithm, and the algorithm for particle swarm optimization with quantum behavior (QPSO) are presented. It is highlighted that in global optimization problems, QPSO performs better at convergence than PSO method. Guo et al. [7] presented the notion, properties, and architecture of neural networks along with the method and categorization of wavelet neural networks. The specific operating procedure is then provided, utilizing the QPSO method as the learning algorithm and a wavelet neural network to be the object.

The Internet and computer networks are vulnerable to several security risks these days. It is difficult to introduce adaptable and adaptable security-related techniques because of the new kinds of threats that happen often. Similar to other security tools designed to improve communication and information security, such as firewalls, antivirus programs, and access control models, is an IDS. One essential tool for protecting the systems and networks of computers is the NIDS. However, modern networks face a number of challenges regarding the viability and sustainability of current methods. These issues are closely linked to the increasing numbers of human interactions that are required and the declining degree of detection accuracy. Numerous methods exist for identifying and controlling different security risks within a network. The intrusion detection method designed by Deore et al. [8] employed Deep Short-Term Long-Term Memory (ChCSO-driven Shallow LSTM) powered by Chimp Chicken Swarm Optimization. Effective intrusion detection requires a CNN extraction of features procedure. In this case, the Deep LSTM is used to detect network intrusions, and its detection performance is improved through training it with a specially created optimization technique.

The location of intrusions is important for perimeter systems. Chen et al. [9] proposed an accurate incursion localization technique utilizing fiber Bragg diffraction (FBG) sensors. The penetration deflection distribution is established using FBG strain measurements, which are based across the fixed-simply unsupported beam theory. Deflection curve analysis is used to identify the force and localize the incursion. An enhanced particle swarm optimization approach is presented to optimize the identification result.

Network security is vital to our everyday lives due to the ever-increasing dangers and cyberattacks to which we are vulnerable. Different protection plans and techniques must therefore be created. Using detection and prevention systems, or NDSs, is one method of identifying malicious network intrusions. Many scholars have focused on building NIDS that

use ML techniques to identify different types of attacks. By examining the characteristics of a sizable dataset, machine learning techniques may automatically identify the key distinctions between normal and aberrant data. Since multiple traits are typically taken for this reason without discriminating, the difficulty of computation is raised. To improve the efficacy of machine learning-based identification techniques, the next step is to select a subset of characteristics from the total feature set using an attribute selection methodology. The salp swarm method (SSA), an optimization method inspired by nature, has demonstrated efficacy in minimizing processing barriers that arise during feature selection optimisation. Zheng et al. [10] investigated how the SSA improves ML-based network detection of anomalies using a range of ML classifiers, including the extreme gradients boost (XGBoost) and Naïve Bayes (NB) algorithms. The use of standard datasets in the experiments allowed for comparability. The two datasets that were explicitly used were UNSW-NB15 and NSL-KDD because they are both focused on network intrusion efforts.

3. Proposed Model

A number of challenges, such as attacks on networks, have accompanied the expansion of network applications across many industries. Cybercriminals use a wide variety of techniques, including worms, viruses, and denial of service attacks, to breach computer systems. Viruses and worms come in a wide variety, and each kind has its own unique set of tricks that it uses to legitimately infiltrate various services. There are many different kinds of attacks, which can be categorized as either active or passive. Denial of service, probing, user-to-root, and remote-to-local assaults are the four categories of known cyber attacks. Among these, the first is an aggressive attack and the others are passive. In order to accomplish their goals, attackers employ a wide variety of viruses and worms in each assault. As a result, the security system needs attack type detection capabilities so it can choose the most effective countermeasures.

Firewalls, antivirus software, encryption, and intrusion detection systems are just a few of the security measures that researchers have been working to address this issue. Any kind of IDS, be it software or hardware, uses its analysis engine's criteria to determine whether a threat is typical or out of the ordinary. A wide variety of methods, including soft computing, statically modules, and others, can be used to construct an IDS analysis engine. There are numerous facets to soft computing approaches, including swarm intelligence, GA, and artificial neural networks (ANN). The use of standardized international datasets for training and evaluation, including IDS KDD99 and NSL-KDD, and the combination of various methodologies can lead to efficient IDS.

There are features in the datasets whose magnitudes, ranges, and units are very variable. Some algorithms, like the Multilayer Perceptron, make inaccurate predictions because of the datasets' extremely variable characteristics. On top of that, a lot of computer power is needed. Thus, feature scaling is a popular approach to reducing the dispersion of independent variables. In order to determine the distance between data points, certain machine learning models require feature scaling. In machine learning, two commonly used feature scaling methods are standardization and normalization. In this research, the data was normalized between 0 and 1 using normalization. An issue with network traffic classification has been the presence of redundant and irrelevant features in the data, which hinders the classification process and makes accurate classifications impossible. Finding the best feature subset that produces high accuracy and gets rid of diversions is a major concern.

This research used supervised machine learning model to complete a binary classification challenge. In supervised machine learning, binary classification occurs when a discrete value is asked to predict whether an instance is normal or attack. This research makes use of a huge dataset with a high feature space dimension. If users working with a big dataset, they need to pick a feature selection approach that will help to remove superfluous features before training and testing. When developing a predictive model, feature selection is essential for narrowing down the available input variables to a manageable subset of useful features. Improving the accuracy of prediction models is usually the goal. The efficiency of the model is also diminished by superfluous features. On the other hand, the detection accuracy score drops and the computational cost goes up because the IDS processes a lot of data instances with irrelevant or redundant features. In order to solve some of the most common problems with intrusion detection systems, feature selection is used to find the features

that are most important to the classification task at hand.

Separating malevolent activity into internal and external sources is a good starting point for any useful categorization. People can better comprehend it because of this. The IDS itself can work with many kind of classifications. However, the IDS have to interact with a system administrator about the identifications. The difference between malevolent actions coming from inside and those coming from outside makes more sense. Every sort of malicious activity is identified by different features. It is helpful to know these features so that users may adjust the IDS for better identification. The Proposed Model for feature selection and Evaluation is depicted in Figure 3.

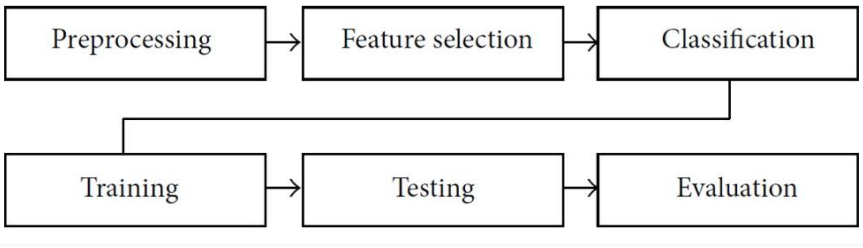

Fig 3: Proposed Model for feature selection and Evaluation

PSO optimization technique development was predicated on a straightforward principle borrowed from the behavior of schools of fish and flocks of birds. Several interpretations were made using computer simulations before it was finally developed. PSO makes use of a wide array of agents, or particles. In order to discover the optimal solution, this swarm explores the search space. To accommodate its own and other particles' flying experiences, each particle in the search space adjusts its flying relative to the others. A random number generator launches PSO, and the search speed is indicated by the velocities of the created particles. Afterwards, the particles are assessed for fitness value. Two primary tests follow this examination. Personal best (pbest) is the initial test that compares a particle's experience with itself. In the second evaluation, a single particle performed relative to the overall swarm is analyzed. The term for it is global best (gbest). The proposed model framework is shown in Figure 4.

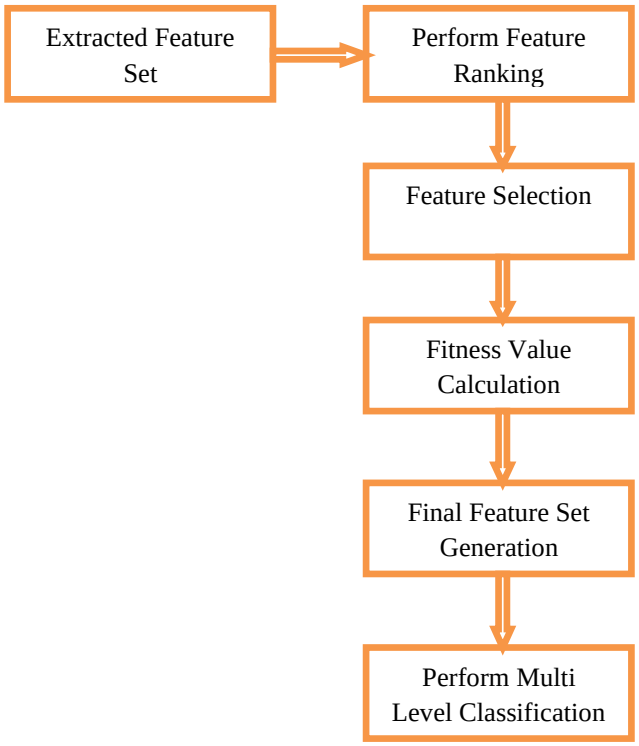

Fig 4: Proposed Model Framework

For feature selection problems, PSO approach is a good fit because it is simple to encode features, has a global search facility, is computationally reasonable, uses few parameters, and is easy to apply. Through PSO's exploration and selection of a subset of principal components or features, a search space known as the principle space was utilized. PSO uses a population of particles, sometimes called a swarm, to represent potential solutions in the search space. The distribution of 1's and 0's is randomly generated to produce the swarm of particles. If a particle's principal component is 1, it is chosen; otherwise, the component with a value of 0 is disregarded. Therefore, several subsets of the principal components are indicated by each particle. After a random initialization, the particles swarm updates its position and velocity as it moves around the search space or principal space, searching for the ideal subset of features. In order to manage numerous types of attacks, a Rational Multi Level Classification with Feature Ranking Strategy using PSO model is designed for accurate detection of intrusions in the network.

Algorithm RMLC-FRS-PSO

{

Input: Feature Set {FeSet}

Output: Multi Level Classification Set {MLCset}

Step-1: Initially the feature set is considered and these features are analyzed and feature ranking is performed. The feature ranking is the process of allocating a rank to the features based on the feature importance. The feature ranking helps to select the highest ranked features. The feature ranking is performed as

$$rank[M] = \sum_{i=1}^{M} getDefaultValue(i)$$

$$Frank[M] = \sum_{i=1}^{M} maxVal\big(FeSet(i)\big) + \tau\big(FeSet(i, i+1)\big) + \min\,(\text{simm(FeSet(i, i + 1))} - minVal\big(FeSet(i)\big)\begin{cases} Frank(i) \leftarrow \max\big(rank(i)\big)\; if\; simm\big(FeSet(i, i+1)\big) < Th \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad Otherwise \end{cases}$$

$$rank[M] = \sum_{i=1}^{M} rank(i) + \gamma(\min\,(simm\big(FeSet(i, i+1)\big))$$

Here default value is considered from the user, τ is used to consider the features that has high similarity, Th is the threshold value, γ is the model used to identify the highest rank with minimum similarity.

Step-2: Feature selection is performed on the ranked feature set for selecting a subset of features from a larger set of characteristics with highest ranks in order to minimize the feature space as much as possible while still meeting some predetermined criteria. Feature selection is a method for selecting useful, consistent, and non-redundant features for use in building models. Improving a predictive model's effectiveness while decreasing the computational cost of modelling is the primary objective of feature selection. The feature selection is performed as

$$Fselect[M] = \sum_{i=1}^{M} \frac{\max\,(Frank\big(FeSet(i)\big))}{len(FeSet)} + \beta\big(Frank(i.\,i+1)\big) + \frac{\sum_{i=1}^{\beta} \min\,(simm\big(FeSet(i, i+1)\big))}{\gamma(FeSet(i, i+1))}$$

β is the count of total features with highest rank greater than threshold value.

Step-3: Evolutionary computation has previously dealt with this issue of overly lengthy fitness function computations, successfully predicting a new individual's fitness without actually calculating it using various methods. In principle, the PSO could keep track of all the positions that have been investigated and how fit they were, and it could check this list every time a particle was relocated. Use the corresponding fitness if the particle's new location in the list is found. However, the list will grow quite vast very quickly, and the number of hits may be minimal because the algorithm's goal is to

discover new and interesting regions of the problem space. Time savings for all but the most insignificant issues are highly unlikely due to the low number of hits and the expense of list maintenance. The PSO model is applied for fitness value calculation that is performed as

Phase1: Initialize Swarm population of M particles P_i (i=1, 2, …, M)
Phase 2: Perform selection of hyper parameter attributes as velocity V, w,S1 and S2,R1,R2 and tot_iter
Phase 3: For i in range(tot_iter):
For i in range(M):
a. Calculate new velocity of i^{th} particle
S[i].V = w*S[i].V+ R1*S2*(S[i].bestPos - S[i].position) +R2*S2*(best_pos_swarm - S[i].pos+Fselect[i])
b. Calculate new position of i^{th} particle using its new velocity
S[i].pos += S[i].V
c. If the calculated position of particle is out of range [minx, maxx] then clip it
if S [i].pos < minx:
S[i].pos = minx+Fselect[i]
Else if S[i].pos > maxx:
S[i].pos = maxx
S[i].fit = i
d. Update the best values calculated
S[i].bestFit = S[i].fit
S[i].bestPos = S[i].pos
if S[i].fitness < best_fitness_swarm
best_fit_swarm = S[i].fit
best_pos_swarm = S[i].pos
End for
End for
Phase 4: Return best particle of Swarm

Step-4: The best fitness value is considered and the final feature set is generated. The final feature set is used for training the model and the final classification will be performed. The final feature set is generated as

$$Fset[M] = \prod_{i=1}^{M} \frac{\max\left(Frank\left(Fselect(i,i+1)\right)\right) + \max\left(S[i].Fitness\left(FeSet(i)\right)\right)}{len(Fselect)} + \max\left(Fselect(i,i+1)\right) + \max\left(best\_fitness\_swarm(i) + \max\left(best\_pos\_swarm\ (i)\right)\right)$$

Step-5: The supervised learning problem known as Multi-Level classification occurs when a single occurrence can have more than one label that occurs as intrusions in the network. In a variation of the classification problem known as multi level classification, each instance can be given numerous nonexclusive labels. The single-label problem of assigning instances to one of several classes is known as multi level classification. The instances can be allocated to an unlimited number of classes in the multi-label problem, and the labels are not exclusive. The multi level classification of intrusions in the network is performed as

$$MLclass[M] = \sum_{i=1}^{M} \frac{\max\left(Fset(i,i+1)\right)}{len(Fset)} + \max\left(Frank\left(Fselect(i,i+1)\right)\right) + \max\left(S[i].Fitness(Fset(i))\right) \begin{cases} MLclass \leftarrow Normal\ \ if\left(\max\left(Fset(i)\right) < nTh\right) \\ MLclass \leftarrow Attack\ \ if\ \left(\max\left(Fset(i)\right) < aTh\right. \\ MLclass \leftarrow minuteAttack\ \ if\ \left(\max\left(Fset(i)\right) < oTh\right) \end{cases}$$

nTh is the normal transaction threshold range, aTh is the attack transaction threshold range and oTh is the other transaction minute attack threshold range.

4. Results

Because IDSs are the initial line of defense against cyber threats and are tasked with properly detecting any possible intrusion into the network, they are key components in an organization's network security. The detection of possible threats is accomplished by many IDS implementations using flow-based analysis of network data. There has been a lot of new thinking and development in the area of network security research recently, with a focus on IDSs. One crucial instrument in cyber security for monitoring and determining intrusion threats is the IDS. The purpose of this research is to examine recent work in IDS that makes use of ML techniques, paying close attention to datasets, ML algorithms, and metrics and to design an efficient model that overcomes the traditional models limitations. To make sure the model is fit for IDS application, dataset selection is crucial. Moreover, the structure of the dataset can impact the efficacy of the ML algorithm. So, the structure of the dataset is crucial when choosing an ML algorithm. Then, metrics will quantitatively assess ML algorithms' performance on a given dataset.

Anomaly intrusion detection, which includes new or modified intrusion attacks, could be hindered by IDS. An important part of machine learning's pre-processing is feature selection. It improves classification efficiency by reducing data dimensionality. Several feature selection strategies for intrusion detection systems were suggested by scholars. Important features are proposed to be classified using those methods according to many criteria. More and more sensitive data is being stored and handled online, making network security a top priority. Attack prevention via passive security rules, firewalls, and other methods is challenging. As a result, IDS have grown in importance as a tool for proactive system security.

In order to detect an attack, a IDS can gather data on system and network activities and analyze it. The primary goal of this research is to provide a security architecture for computer networks, namely a IDS. In order to identify questionable connections, this suggested system should be installed at the network server and watch all data packets as they pass through. In this way, it can alert the system administrator to the specific kind of attack that seems suspect. In order to manage numerous types of attacks, a Rational Multi Level Classification with Feature Ranking Strategy using PSO (RMLC-FRS-PSO) model is designed for accurate detection of intrusions in the network. The proposed model is contrasted with the traditional models like Optimization Method for Intrusion Detection Classification Model Based on Deep Belief Network (OM-IDC-DBN) and Network Intrusion Detection Based on PSO-Xgboost Model (NID-PSO-XGB) models. The results represent that the proposed model performance is high in feature vector generation that is used for intrusion detection in the network.

Feature extraction is a method for mining current features for new ones, with the goal of reducing the amount of features in a dataset. Once these features have been reduced, the original collection of features should be able to be summarized to a large extent. By combining the original set of features in this way, a condensed version of the original set can be constructed. The Feature Extraction Accuracy Levels of the proposed and existing models are represented in Table 1 and Figure 5.

Table 1: Feature Extraction Accuracy Levels

Nodes in the Network	Models Considered		
	RMLC-FRS-PSO Model	OM-IDC-DBN Model	NID-PSO-XGB Model
10000	97.6	94.0	91.9
20000	97.9	94.1	92.1
30000	98.0	94.3	92.3
40000	98.2	94.5	92.5
50000	98.3	94.7	92.7
60000	98.5	94.8	92.8

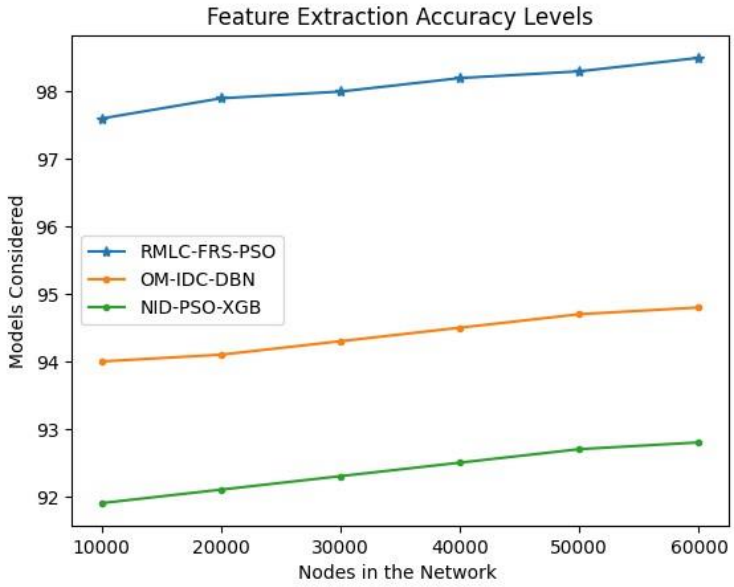

Fig 5: Feature Extraction Accuracy Levels

One machine learning task that ranks the relevance of input features in relation to their impact on a supervised learning model's performance is feature importance ranking. When constructing a predictive model in machine learning, feature importance scores are utilized to ascertain the corresponding significance of every feature within a dataset. The Feature Ranking Accuracy Levels of the existing and proposed models are represented in Table 2 and Figure 6.

Table 2: Feature Ranking Accuracy Levels

Nodes in the Network	Models Considered		
	RMLC-FRS-PSO Model	OM-IDC-DBN Model	NID-PSO-XGB Model
10000	97.1	93.9	92.7
20000	97.4	94.1	92.9
30000	97.6	94.4	93.1
40000	97.8	94.6	93.3
50000	98.0	94.8	93.7
60000	98.2	95	93.8

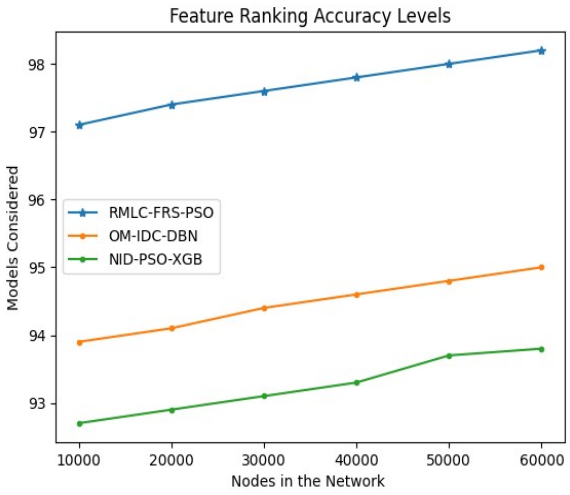

Fig 6: Feature Ranking Accuracy Levels

By extracting just the most pertinent information and excluding any irrelevant or noisy details, Feature Selection allows to decrease the number of input variables into the model. It is the method of selecting appropriate features for a machine learning model autonomously according to the problem type. In order to accomplish this, the main features are considered when adding or removing them. It aids in decreasing the amount of input data and the amount of noise in the data. The Table 3 and Figure 7 shows the Ranked Feature Selection Time Levels of the existing and proposed models

Table 3: Ranked Feature Selection Time Levels

Nodes in the Network	Models Considered		
	RMLC-FRS-PSO Model	OM-IDC-DBN Model	NID-PSO-XGB Model
10000	15.2	21.0	19.8
20000	15.4	21.2	20.1
30000	15.6	21.4	20.3
40000	15.7	21.6	20.6
50000	15.8	21.8	20.8
60000	16	22	21

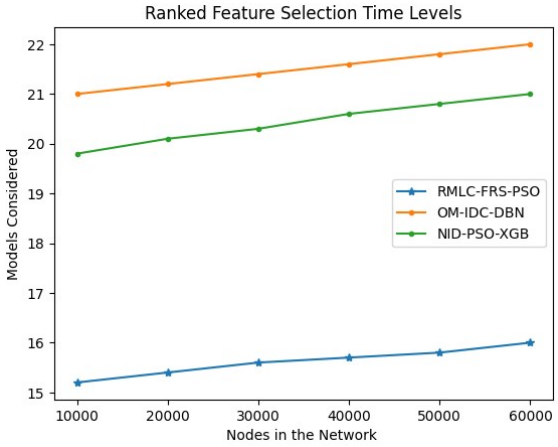

Fig 7: Ranked Feature Selection Time Levels

Fitness measures the degree to which natural selection favors a certain genotype. Values for fitness range from zero to one. A fitness of 1 indicates the healthiest member of a population, and fitness of the remaining individuals can be calculated as 1 - s, where s is the selection coefficient. After being initialized with a set of solutions, PSO iteratively searches for optimum values by updating generations. Each particle is updated in each iteration by comparing two best values. So far, the first one has proven to be the most effective solution in terms of fitness. The Fitness Value Calculation Time Levels of the proposed and existing models are shown in Table 4 and Figure 8.

Table 4: Fitness Value Calculation Time Levels

Nodes in the Network	Models Considered		
	RMLC-FRS-PSO Model	OM-IDC-DBN Model	NID-PSO-XGB Model
10000	17.1	23.0	26.9
20000	17.3	23.2	27.1
30000	17.5	23.5	27.3
40000	17.7	23.7	27.5
50000	17.9	23.9	27.8
60000	18	24	28

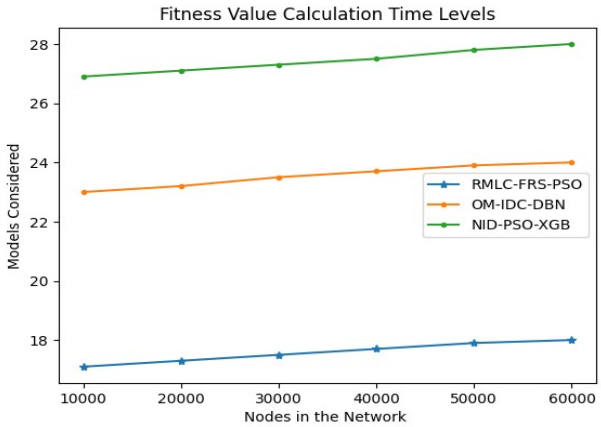

Fig 8: Fitness Value Calculation Time Levels

When developing ML models, feature selection is crucial. In addition to increasing the training time required to construct the model, irrelevant elements in the data impact the model's accuracy. An essential step in developing a IDS is feature selection. The purpose of feature selection in machine learning is to improve the accuracy of the process. By identifying the most important factors and removing the unnecessary ones, it improves the algorithms' ability to make predictions. This highlights the significance of feature selection. The Final Feature Vector Generation Accuracy Levels of the proposed and existing models are indicated in Table 5 and Figure 9.

Table 5: Final Feature Vector Generation Accuracy Levels

Nodes in the Network	Models Considered		
	RMLC-FRS-PSO Model	OM-IDC-DBN Model	NID-PSO-XGB Model
10000	96.8	91.6	93.1
20000	96.9	91.8	93.3
30000	97.1	92.0	93.5
40000	97.3	92.1	93.7
50000	97.5	92.4	93.9
60000	97.8	92.5	94

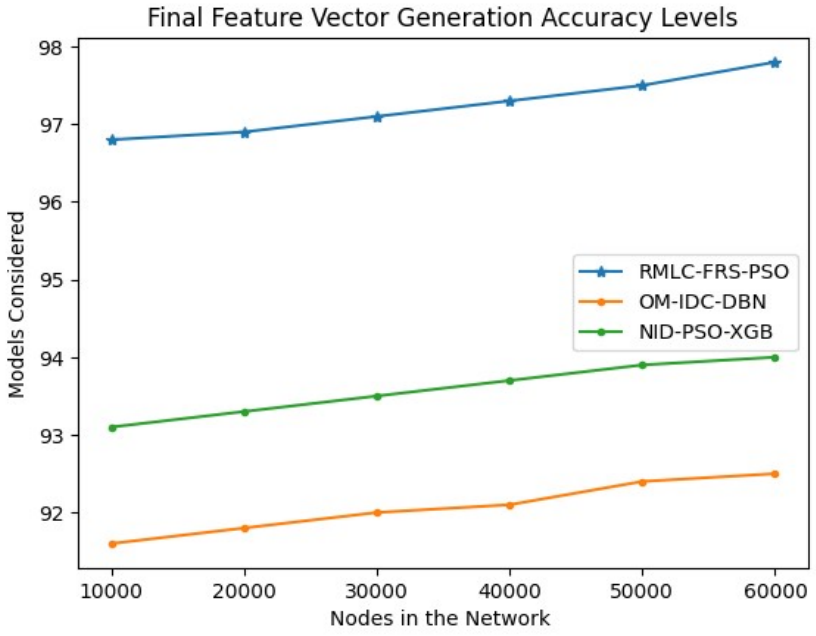

Fig 9: Final Feature Vector Generation Accuracy Levels

When there are more than two categories to be classified, the process is called multiclass classification. No more than one class can be assigned to any given sample. The goal of multi-label classification is to anticipate the labels of at least two classes. Specialized machine learning algorithms are needed for multi-label classification in contrast to traditional classification problems where class labels are mutually exclusive. These algorithms may predict numerous classes or labels that are mutually non-exclusive. The Multi Level Classification Accuracy Levels of the proposed and existing models are indicated in Table 6 and Figure 10.

Table 6: Multi Level Classification Accuracy Levels

Nodes in the Network	Models Considered		
	RMLC-FRS-PSO Model	OM-IDC-DBN Model	NID-PSO-XGB Model
10000	97.3	93.7	94.3
20000	97.6	93.9	94.6
30000	97.9	94.1	94.8
40000	98.1	94.3	95.0
50000	98.4	94.7	95.2
60000	98.7	94.8	95.4

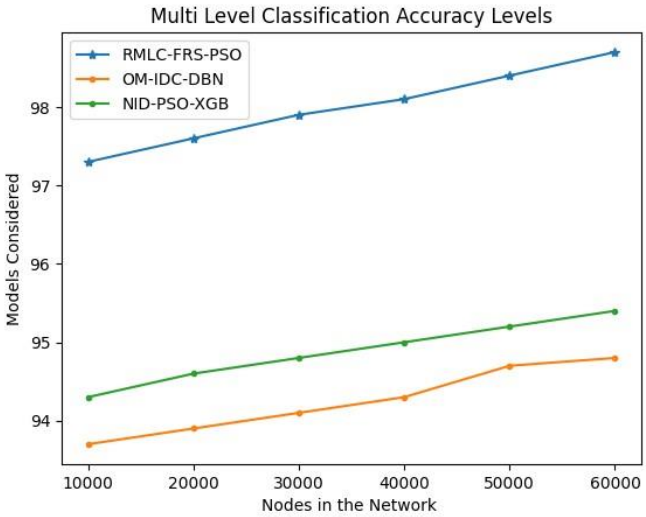

Fig 10: Multi Level Classification Accuracy Levels

5. Conclusion

WSNs lack any kind of protection, leaving them vulnerable to a wide range of security risks. Consequently, to counteract these dangers, a robust security mechanism is required. The performance of the various intrusion detection algorithms is an issue. Suggestions for better feature selection and categorization methods can boost performance. Therefore, this research proposes a feature selection approach for intrusion detection in wireless sensor networks based on PSO, which selects the optimal subset of characteristics. Nowadays, the biggest problem with network communications is interference. There is a growing danger to network networks from the increasing frequency of network attacks. Finding a suitable and trustworthy method to prevent network interference and safeguard network security and privacy has also been the subject of numerous studies. An essential research tool for identifying any instances of unusual network traffic flow is machine learning. Providing a synopsis of intrusion detection systems' benefits and requirements is the major objective of this research. An intrusion detection technique based on feature optimization and classification is proposed in this paper. To get the most out of the recovered direct and indirect trust, PSO method is applied. This research delves into how the PSO approach, when combined with FS, might enhance the intrusion detection accuracy of the IDS. In order to manage numerous types of attacks, a Rational Multi Level Classification with Feature Ranking Strategy using PSO model is designed for accurate detection of intrusions in the network. This research achieves 98.7% accuracy in multi level classification of

intrusions that accurately generates the class labels in the network that enhance the quality of service levels of IDS. In future, hybrid optimization techniques can be applied on the IDS models for feature dimensionality reduction and also for enhancing the intrusion detection rate.

References

[1] L. Guo, "Research on Anomaly Detection in Massive Multimedia Data Transmission Network Based on Improved PSO Algorithm," in IEEE Access, vol. 8, pp. 95368-95377, 2020, doi: 10.1109/ACCESS.2020.2994578.

[2] P. Wei, Y. Li, Z. Zhang, T. Hu, Z. Li and D. Liu, "An Optimization Method for Intrusion Detection Classification Model Based on Deep Belief Network," in IEEE Access, vol. 7, pp. 87593-87605, 2019, doi: 10.1109/ACCESS.2019.2925828.

[3] J. Liu, D. Yang, M. Lian and M. Li, "Research on Intrusion Detection Based on Particle Swarm Optimization in IoT," in IEEE Access, vol. 9, pp. 38254-38268, 2021, doi: 10.1109/ACCESS.2021.3063671.

[4] Y. Han, Y. Wang, Y. Cao, Z. Geng and Q. Zhu, "A Novel Wrapped Feature Selection Framework for Developing Power System Intrusion Detection Based on Machine Learning Methods," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 53, no. 11, pp. 7066-7076, Nov. 2023, doi: 10.1109/TSMC.2023.3292110.

[5] M. H. Ali, B. A. D. Al Mohammed, A. Ismail and M. F. Zolkipli, "A New Intrusion Detection System Based on Fast Learning Network and Particle Swarm Optimization," in IEEE Access, vol. 6, pp. 20255-20261, 2018, doi: 10.1109/ACCESS.2018.2820092.

[6] H. Jiang, Z. He, G. Ye and H. Zhang, "Network Intrusion Detection Based on PSO-Xgboost Model," in IEEE Access, vol. 8, pp. 58392-58401, 2020, doi: 10.1109/ACCESS.2020.2982418.

[7] L. Guo, "Research on Anomaly Detection in Massive Multimedia Data Transmission Network Based on Improved PSO Algorithm," in IEEE Access, vol. 8, pp. 95368-95377, 2020, doi: 10.1109/ACCESS.2020.2994578.

[8] B. Deore and S. Bhosale, "Hybrid Optimization Enabled Robust CNN-LSTM Technique for Network Intrusion Detection," in IEEE Access, vol. 10, pp. 65611-65622, 2022, doi: 10.1109/ACCESS.2022.3183213.

[9] Y. Chen, L. -X. Zhou and H. -L. Liu, "A Fiber Bragg Grating Sensor Perimeter Intrusion Localization Method Optimized by Improved Particle Swarm Optimization Algorithm," in IEEE Sensors Journal, vol. 18, no. 3, pp. 1243-1249, 1 Feb.1, 2018, doi: 10.1109/JSEN.2017.2773631.

[10] Z. Zheng, A. K. Sangaiah and T. Wang, "Adaptive communication protocols in flying ad hoc network", IEEE Commun. Mag., vol. 56, pp. 136-142, Jan. 2018.

[11] Saheed, Y.K.; Arowolo, M.O. Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. IEEE Access 2021, 9, 161546–161554.

[12] Nandy, S.; Adhikari, M.; Khan, M.A.; Menon, V.G.; Verma, S. An intrusion detection mechanism for secured IoMT framework based on swarm-neural network. IEEE J. Biomed. Health Inform. 2021, 26, 1969–1976. Hady, A.A.; Ghubaish, A.; Salman, T.; Unal, D.; Jain, R. Intrusion detection system for healthcare systems using medical and network data: A comparison study. IEEE Access 2020, 8, 106576–106584.

[13] Gupta, K.; Sharma, D.K.; Gupta, K.D.; Kumar, A. A tree classifier based network intrusion detection model for Internet of Medical Things. Comput. Electr. Eng. 2022, 102, 108158.

[14] Saba, T. Intrusion detection in smart city hospitals using ensemble classifiers. In Proceedings of the 2020 13th International Conference on Developments in eSystems Engineering (DeSE), Liverpool, UK, 14–17 December 2020; pp. 418–422.

[15] Kumar, P.; Gupta, G.P.; Tripathi, R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. Comput. Commun. 2021, 166, 110–124.

[16] Chaganti, R.; Varadarajan, V.; Gorantla, V.S.; Gadekallu, T.R.; Ravi, V. Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture. Future Internet 2022, 14, 250.

[17] Li, M.; Liu, Y.; Tian, Z.; Shan, C. Privacy Protection Method Based on Multidimensional Feature Fusion Under 6G Networks. IEEE Trans. Netw. Sci. Eng. 2022, 1–14.

[18] Yaacoub, J.P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. Future Gener. Comput. Syst. 2020, 105, 581–606.

[19] Zachos, G.; Essop, I.; Mantas, G.; Porfyrakis, K.; Ribeiro, J.C.; Rodriguez, J. An anomaly-based intrusion detection system for internet of medical things networks. Electronics 2021, 10, 2562. Thamilarasu, G.; Odesile, A.; Hoang, A. An intrusion detection system for internet of medical things. IEEE Access 2020, 8, 181560–181576.

[20] Binbusayyis, A.; Alaskar, H.; Vaiyapuri, T.; Dinesh, M. An investigation and comparison of machine learning approaches for intrusion detection in IoMT network. J. Supercomput. 2022, 78, 17403–17422. Awotunde, J.B.; Abiodun, K.M.; Adeniyi, E.A.; Folorunso, S.O.; Jimoh, R.G. A deep learning-based intrusion detection technique for a secured IoMT system. In Proceedings of the International Conference on Informatics and Intelligent Applications, Ota, Nigeria, 25–27 November 2021; pp. 50–62.

[21] Khan, S.; Akhunzada, A. A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT). Comput. Commun. 2021, 170, 209–216.

[22] Ravi, V.; Alazab, M.; Selvaganapathy, S.; Chaganti, R. A Multi-View attention-based deep learning framework for malware detection in smart healthcare systems. Comput. Commun. 2022, 195, 73–81.

[23] Radoglou-Grammatikis, P.; Sarigiannidis, P.; Efstathopoulos, G.; Lagkas, T.; Fragulis, G.; Sarigiannidis, A. A self-learning approach for detecting intrusions in healthcare systems. In Proceedings of the ICC 2021-IEEE International Conference on Communications. IEEE, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6.

[24] Saheed, Y.K.; Arowolo, M.O. Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. IEEE Access 2021, 9, 161546–161554. Nandy, S.; Adhikari, M.; Khan, M.A.; Menon, V.G.; Verma, S. An intrusion detection mechanism for secured IoMT framework based on swarm-neural network. IEEE J. Biomed. Health Inform. 2021, 26, 1969–1976.

[25] Hady, A.A.; Ghubaish, A.; Salman, T.; Unal, D.; Jain, R. Intrusion detection system for healthcare systems using medical and network data: A comparison study. IEEE Access 2020, 8, 106576–106584.

[26] Gupta, K.; Sharma, D.K.; Gupta, K.D.; Kumar, A. A tree classifier based network intrusion detection model for Internet of Medical Things. Comput. Electr. Eng. 2022, 102, 108158.

[27] Saba, T. Intrusion detection in smart city hospitals using ensemble classifiers. In Proceedings of the 2020 13th International Conference on Developments in eSystems Engineering (DeSE), Liverpool, UK, 14–17 December 2020; pp. 418–422.

[28] Kumar, P.; Gupta, G.P.; Tripathi, R. An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. Comput. Commun. 2021, 166, 110–124.