**Feature Selection and Classification models of Intrusion Detection Systems -A Review on Industrial Critical Infrastructure Perspective**

Karthigha M1, Latha L2, Madhumathi R3

*1,3Sri Ramakrishna Engineering College, Coimbatore – 641 022, India*

*2Kumaraguru College of TechnologyCoimbatore – 641 022, India*

**Abstract**

Recently it is self-evident that humanity has entered the fourth industrial revolution. With the advent like Internet of things, cloud computing, Artificial Intelligence, the industrial critical infrastructures such as power plants, oil and gas plants, heavy industries, nuclear plants and water treatment facilities experiencing disruptive growth. This era of the industrialization, nevertheless, has carried with it its new myriad of issues, notably regarding cyber security threats. Nowadays industrial processes are openly connected to internet and internet-connected machines are almost always highly susceptible to security breaches by adversaries despite sufficient cyber security safeguards. Intrusion detection systems (IDS) are designed that employ classification models to detect malicious attacks such as service attack, probing attacks etc. In intrusion detection, phase which reduces the amount of similar traffic attributes while sustaining accuracy of classification is a requirement that considerably improves an intrusion detection system's overall efficacy. This chapter focuses on (i) various feature selection methods in IDS (ii) ML&DL classification models in IDS of industrial systems (iii) Various ensemble feature selection models are analysed and a novel ensemble feature selection model for IDS is proposed.

Keywords – Feature Selection, Intrusion Detection Systems, Classification, Machine Learning

1. **INTRODUCTION**

An Intrusion Detection gadget (IDS) can be network visitors monitors gadget that detects suspicious behaviour and send notifications.

The IDS is likewise a pay attention-handiest tool. The IDS monitors visitors and sends its findings to an administrator. IDS is not able to require movement automatically to save you an diagnosed exploit from seizing manipulate of the machine [1].

An IDS's only activity is to identify threats, thus it's hooked up out-of-band at the network, which indicates it is now not inside the proper real-time communique channel among the sender and receiver of statistics. Rather, IDS structures often use a faucet or SPAN port to have a look at a duplicate of the inline visitor’s circulation (and thus making sure that IDS does not effect inline network performance).

Any harmful interest is usually reports to gather a SIEM gadget. A SIEM system combines information from many resources and uses the alert filtering algorithms to shows differences among malicious and fake alarms. Despite the fact that intrusion detection structures hold an eye fixed fixed on networks for suspicious sports, they may be at risk of fake alarms. As a end result, whilst businesses first of all put into effect IDS merchandise, they need to great-tune them. It involves effectively configuring intrusion detection systems to differentiate among valid network site visitors and malicious activities.

This technology is used by IT departments in enterprises to get insight into potentially dangerous behaviours that occur in their technical settings. It also enables information to be shared across departments and organisations in a more secure and reliable manner. It is in many aspects, an advancement over conventional cybersecurity technologies such as firewalls, antivirus, and message encryption. The advantages and disadvantages of IDS is given in Figure1.

**1.1 IDS for Industrial Control Systems**

It can be a vast word that refers to a spread of manage structures and its related components which can be used to control industrial approaches. Actual-time statistics amassing, gadget tracking, and automated manipulate and management of commercial strategies are the major duties of ICS [2]. Finance, transportation, water remedy, manufacturing, and power manufacturing and distribution are just a number of the industries that employ ICS. They play a key element at some point of a country's crucial infrastructure and feature an immediate impact on the financial system. ICS have become more smart and open as they combine greater with pc and internet technology (IT).

The safety of ICS has sparked big public challenge in latest years, and therefore the frequency of cyber attacks in opposition to ICS is rapidly developing. In 2010, the infamous Stuxnet malware2 attacked Iran's Natanz nuclear enrichment complex, capture of several important structures and then unnaturally accelerating the uranium-enriched centrifuge, ultimately resulting inside the centrifuge's destruction. The plant had no preference however to close . BlackEnergy 33 hacked the Ukraine strength device in 2015 by means of infiltrating the power grid manage centre through VPN, tampering with the relay's control instructions, and separating the circuit. Concurrently, the system's community and manage software were broken, and a cellphone DDoS assault turned into initiated to forestall the manipulate gadget from recognising unusual situations after which resuming operation of the strength grid gadget. Dr. Staggs4 established the manner to bodily link unmanned wind generators inside the united states of america to compromise the wind farm control gadget at Black Hat 2017. Consistent with a succession of security events, ICS has turn out to be a well-preferred target for hackers. One most of the most urgent worldwide demanding situations is a way to protect the security of ICS.

IDS are intended to spot harmful attacks routinely. They accumulate and examine community site visitors, safety logs, audit information, and expertise from vital places on a laptop machine that allows you to decide whether or not the device has any security flaws. One among the maximum essential components of keeping the safety of ICS is intrusion detection. Intrusion detection technology for ICS is now a search hotspot that has attracted a whole lot of interest from academia and business. As a result, an awesome range of intrusion detection algorithms for ICS were evolved. The paper is to provide an explanation for intrusion detection strategies for ICS and propose a brand-new categorization of ICS IDS that takes under consideration the unique characteristics of ICS [3].

**Figure 1. Advantages and Disadvantages of IDS**

* 1. **Types of Intrusion Detection Systems**

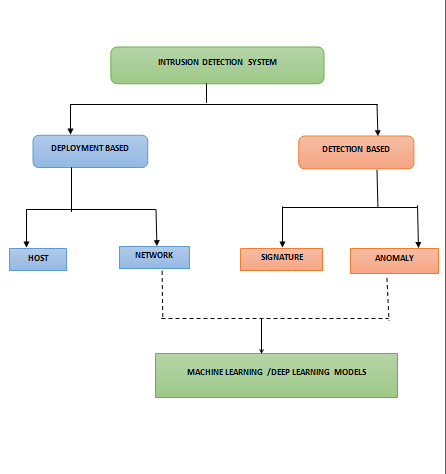
Different types of IDS are classified on different techniques and methods [4][5]

**1. Signature-based IDS**

With the growth of cyberattacks, it's more important than ever to protect your personal or company network from malware, viruses, Trojans, and other threats. Signature-based detection is a common method for detecting and identifying malicious software or assaults on your computer. It examines inbound network traffic and searches the signature database for known fingerprints (signatures) or susceptible patterns, also known as attack signatures. Signature-based IDS is used by antivirus developers to identify unusual behaviour in system files or databases. It, on the other hand, is unable to identify unidentified suspicious behaviour.

**2. Anomaly or Behaviour-based IDS**

Signature-based detection systems are less successful than anomaly detection systems. The anomaly detection system, unlike signature detection, can monitor and analyse substantial network traffic and data to find abnormalities. It doesn't rely on known hallmark assaults to detect threats; instead, it searches for behaviours that might indicate a danger or attack. As a result, there are better odds of detecting and mitigating harmful assaults. To protect your network, anomaly-based IDS monitors network traffic using AI (Artificial Intelligence), statistical models, and machine learning.

****

**Figure 2. Types of IDS**

**1.3 Network IDS**

Network traffic monitors a cross platform and evaluates hosts to spot detectors is known as a (NIDS). NIDS analyses every traffic travelling through the network and compares it to packet information and content. An alarm is provided to the network administrator if any detection occurs. the simplest feature of NIDS is that it can detect whether someone is attempting to attack the firewall if it is put in the same area as the firewall.

A NIDS protocol may effectively monitor all network traffic while causing no performance degradation. Because it doesn't add to the traffic volume, it's no effect on network availability or performance. the kinds of intrusion detection systems are depicted in Figure 2.

**1.4 Host - Based Intrusion Detection System**

The whole system activity, including application logs and system calls, is analysed by a number Intrusion Detection System (HIDS). during this way, it varies from NIDS therein it monitors all system activity rather than only network activities. A (HIDS) may be a software agent that is placed directly on the host and detects malicious activity via system calls. It examines password credentials log attempts and compares them to known brute force to work out if they are attempts at a breach.

HIDS can identify assaults that an NIDS would miss since they monitor events local to hosts. HIDS can also be used to identify and prevent software integrity breaches. Making them perfect for safeguarding extremely sensitive data including legal papers, personal information, and property .

**1.5 Protocol - Based Intrusion Detection System**

It may be a machine or agent this is usually present at the server's front give up, regulating and decoding the protocol among the person/tool. It tries to shield the net server by means of checking the HTTPS protocol on a everyday foundation and accepting the associated HTTP protocol. Because HTTPS isn't secured until it reaches the net presentation layer, this approach might have to stay on this interface for you to use HTTPS.

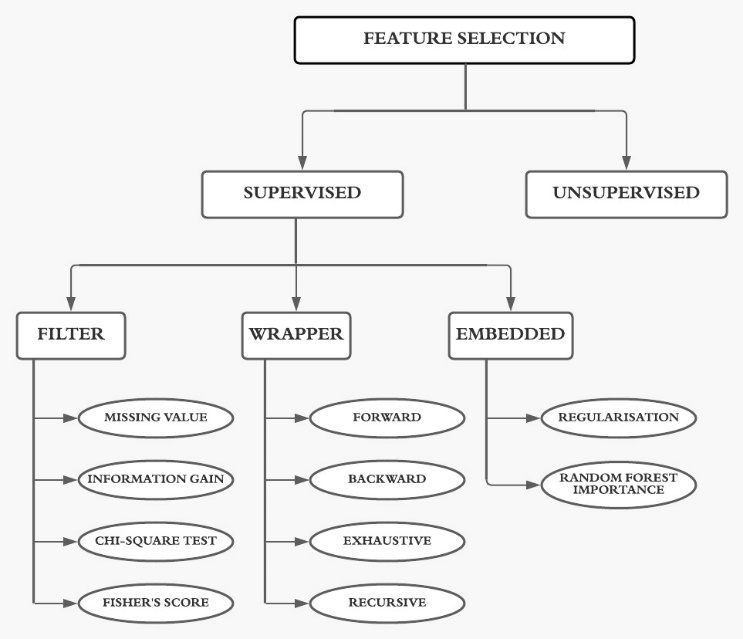
**1.6 Application Protocol-based Intrusion Detection System**

A system that lives during a collection of servers is known as an (APIDS). It detects intrusions by listening in on and deciphering application-specific protocols.Such as, because the middleware interacts with the database on the web, this is able to monitor the SQL protocol explicitly.

**1.7 Virtual Machine-Based Intrusion Detection System**

It is like one or more IDSs but it deployed remotely using a (VM). It is the most recent of the four IDS kinds, and it still being refined. VMIDS is employed by the majority of managed IT service providers (MSPs).

1. **FEATURE** **SELECTION**

Function choice is that the procedure of selecting a subset of applicable functions for use in model production. It is used to reduce the unwanted capabilities at the same time as training the dataset. Its aim is to are trying to find out the high-quality viable set of features for building a device mastering version [6]. Figure three suggests the forms of function selection.

**Figure 3. Feature Selection Types**

**2.1 UNSUPERVISED**

Unsupervised feature selection is the process which does not use a target variable. It is used for unlabelled dataset.

**2.2 SUPERVISED**

This techniques learn the variable and used for the labelled dataset [7][8][9].The three supervised selection method are,

* Filter method
* Wrapped method
* Embedded method

**2.2.1 FILTER METHOD**

Filter method is a pre-processing step. In this method features are selected based on statistics measures. It is independent on machine learning algorithms and it is used to filter the unwanted feature and columns. Advantage is that it does not overfit the data. The filter approach is shown in Figure 4.

**Features**

**Subset**

**Performance**

**Model**

**Figure 4. Filter approach**

Filter method or Feature selection can be divided into four categories:

**Information Gain**

It is employed in reduce while the dataset is transformed. It are often calculated by comparing with before and after of information gain**.**

**Chi-square Test**

It is one of the way to know the difference of the categorical variables. The calculated value among feature, target variable and chosen features with the selected value.

**Fisher's Score**

It represents the quantity of information of one variable that provides some unknown parameter. It calculates the difference of the variance of the expected value and the observed value. It returns the rank in high-low order. Then we will select the variables.

**Missing Value Ratio**

The missing value can be calculated by this missing value ratio. The formula is difference between number of the missing value divided by the total number of observations.

**Missing Value Ratio=**

**2.2.2 WRAPPER METHOD**

This technique by using comparing a subset of features employing a gadget mastering set of rules over and over is shown in discern five. Choice of functions is completed by way of thinking about it as a search problem.

• Wrapper method are supported grasping search algorithms so these strategies are known as greedy algorithms due to the fact they intention to find the pleasant feasible aggregate of capabilities that result in the satisfactory overall performance model.

• The features decided on through filter out strategies won't be the maximum top-rated set of features for that precise set of rules.

|  |
| --- |
| FEATURES  SUBSET |

|  |
| --- |
| ML  ALGORITHM |

|  |
| --- |
| ALL  FEATURES |

|  |
| --- |
| PERFORMANCE |

**REPEAT UNTIL OPTIMUM)**

**Figure 5: Wrapper approach**

Wrapper method can be divided into four types:

* Recursive Elimination
* Exhaustive selection
* Step forward selection
* Step backwards selection

**Forward selection**

It is an iterative process where beginning stage of the step forward feature selection, it is evaluated by the performance of the classifier. The method continues until the specified features is selected. The primary feature is combination of other features. This is often given in figure 6.

**Step backwards feature selection**

It is also known as an iterative approach. The feature selection of round-robin is removed.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  | | --- | | Sequential  forward |   addition   |  | | --- | | Sequential  Selection |  |  | | --- | | Sequential  backward |  |  | | --- | | Candidate set |  |  | | --- | | Candidate set |   return |

**Figure 6. Sequential feature selection**

**Exhaustive Feature Selection**

It is a fine characteristic method that evaluates every characteristic set as brute force. It creates all of the subsets of capabilities from 1 to N, with N being the complete variety of capabilities, and for each subset, it builds a device mastering set of rules and selects the subset with the handiest performance. It approaches this approach attempts and makes every feasible mixture of capabilities and returns the handiest appearing characteristic set.

**Recursive Feature Elimination**

Recursive characteristic removal can be a recursive grasping optimization approach, wherein functions are decided on via way of means of recursively. Now, an estimator is skilled with every function, and consequently the significance of every characteristic is decided the use of characteristic or thru a characteristic significance characteristic.

**2.2.3 EMBEDDED METHOD**

It combines the wrapper and filter methods which is given in Figure 7. This processing method is quicker. These processing method also are iterative. After each iteration, it evaluates and find the foremost important feature which has contributed the most to training for a particular iteration.

**GENERATE SUBSET**

**ALGORITHM & PERFORMANCE**

**Figure 7. Embedded Approach**

Embedded method divided into two categories:

* Regularisation
* Random forest importance

**Regularisation**

Regularization adds a penalty to various parameters model in order to avoid overfitting. Then penalty terms are added to the coefficients. There are two types of regularization techniques. They are:

1. L1 regularisation (LASSO)
2. L2 regularisation (Ridge)

Some coefficients are shrink to zero and those zero coefficients are removed from the dataset.

**Random Forest Importance**

Random forest method uses combination of the decision trees. This method is so successful as it provides a good predictive performance, low over-fitting and easy interpretability.

**INPUT**

**DECISION TREES PREDICTIONS**

**TREE 1 :**

**TREE 2 :**

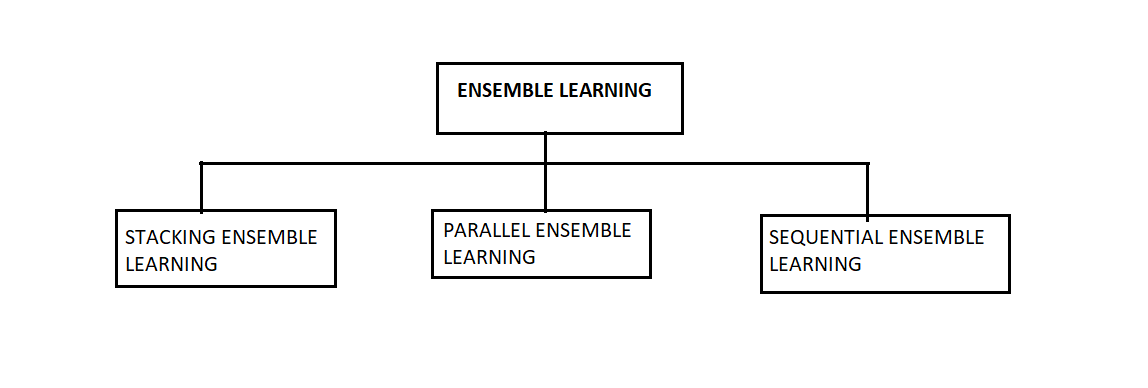
**TREE 3 :**

**RANDOM FOREST PREDICTS**

**Figure 8. Random Forest Importance**

This method may be bagging algorithm as it aggregates a different decision trees. The nodes of all the trees are ranked by their performance.Then the nodes are assembled as impurity values, which helps to make a subset of the most features. Random Forest Importance is shown in Figure 8.

**Ensembling**

This technique to produce one optimal predictive model of several base model that combines together [10][11] shown in Figure 9.

**Figure 9. Ensemble Methods**

**Parallel ensemble learning (bagging)**

It is an ensemble learning method that seeks a various group of ensemble members by varying the data. Short form for boots trap aggregation is bagging. Decision trees is employed to increase the accuracy of models [9].

Eg: Random Forest and additional tree

**Stacking Ensemble Learning (Stacking)**

Stacked Generalization, or stacking for brief , is an ensemble approach that seeks a numerous institution of participants through various the version kinds match at the schooling records and the use of a version to mix predictions.

Eg: balloting ensemble

Sequential Ensemble Learning (boosting)

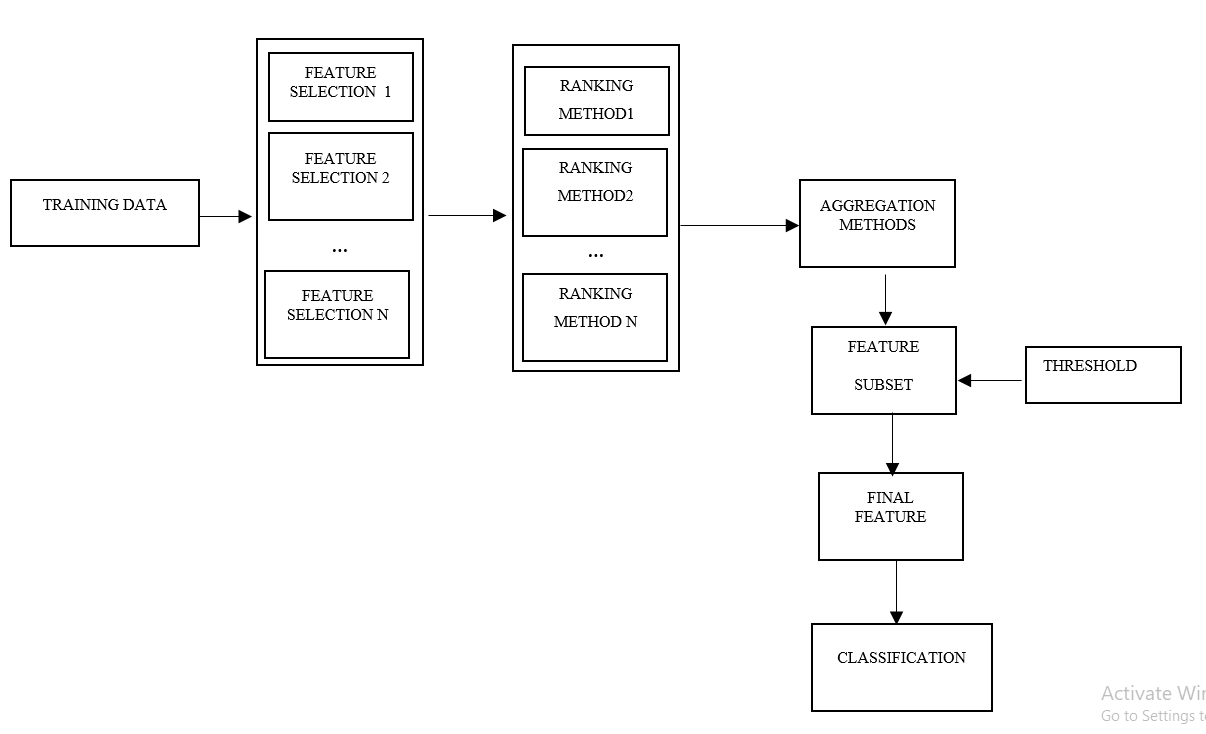
Boosting is an ensemble approach that seeks to differ the schooling records to attention interest on examples that preceding match fashions at the schooling dataset are becoming wrong.

Eg: Ada Boost, Gradient Boosting are examples of Boosting Techniques.

Different fashions of ensembling may be done. In this chapter, six ensembling fashions primarily based totally were proposed.

**Model I**

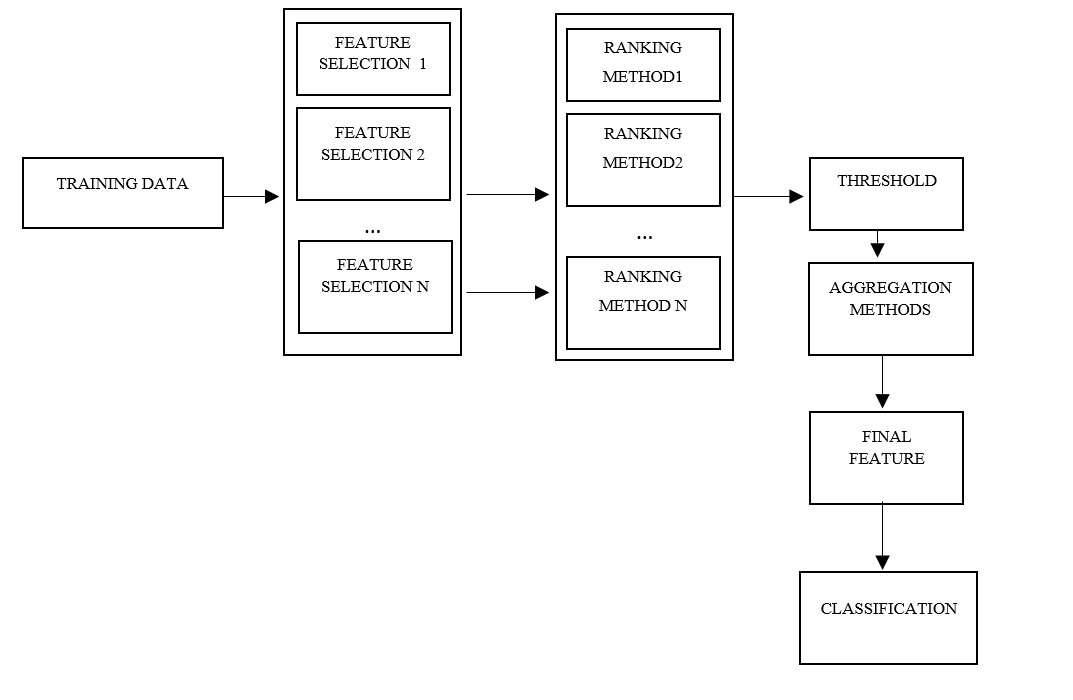
In model I the training data’s significant features are selected by ensembling various feature selection algorithm shown in Figure 10. The feature selection can be done with the selection of diverse base selectors which gives feature importance score for each selector. Different ranking algorithms could be used to rank the scores. The features with ranks can be aggregated using various aggregation techniques like mean, borda etc. The final features can be selected by applying threshold to the feature subset. The threshold can be 10,25,50 percent and log2 n of the original dataset.



**Figure 10. Model I-Ensemble Feature Selection Approach**

**Model II**

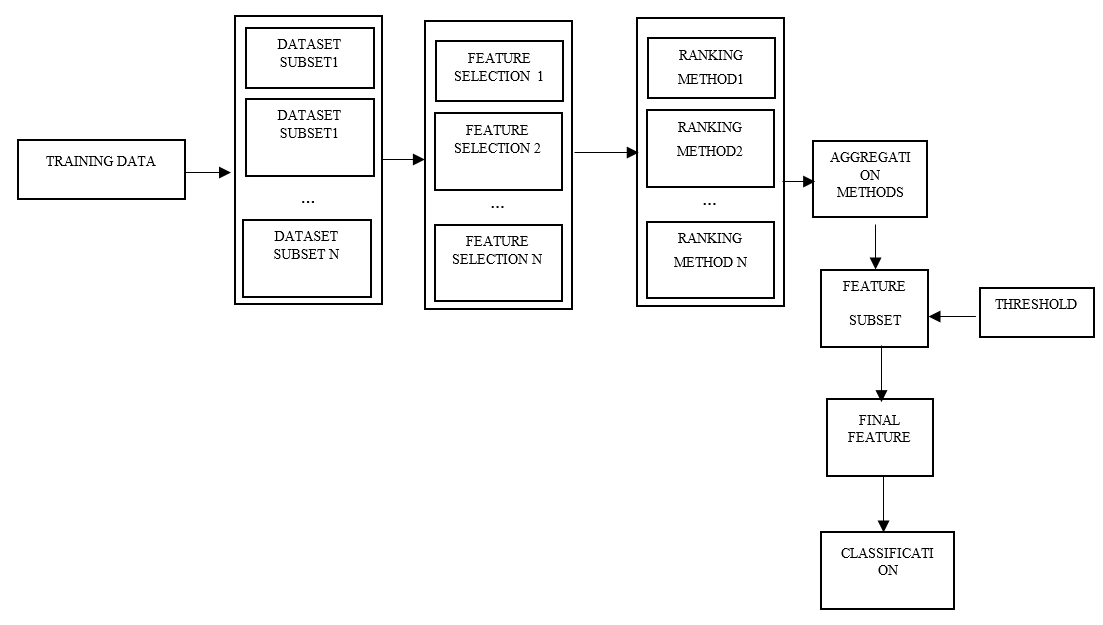
In model II the training data’s significant features are selected by ensembling various feature selection algorithm shown in Figure 11. The feature selection can be done with the selection of diverse base selectors which gives feature importance score for each selectors. Different ranking algorithms could be used to rank the scores. Threshold is applied to the feature list and the features with ranks can be aggregated using various aggregation techniques like mean, borda etc.



**Figure 11. Model II-Ensemble Feature Selection Approach**

**Model III**

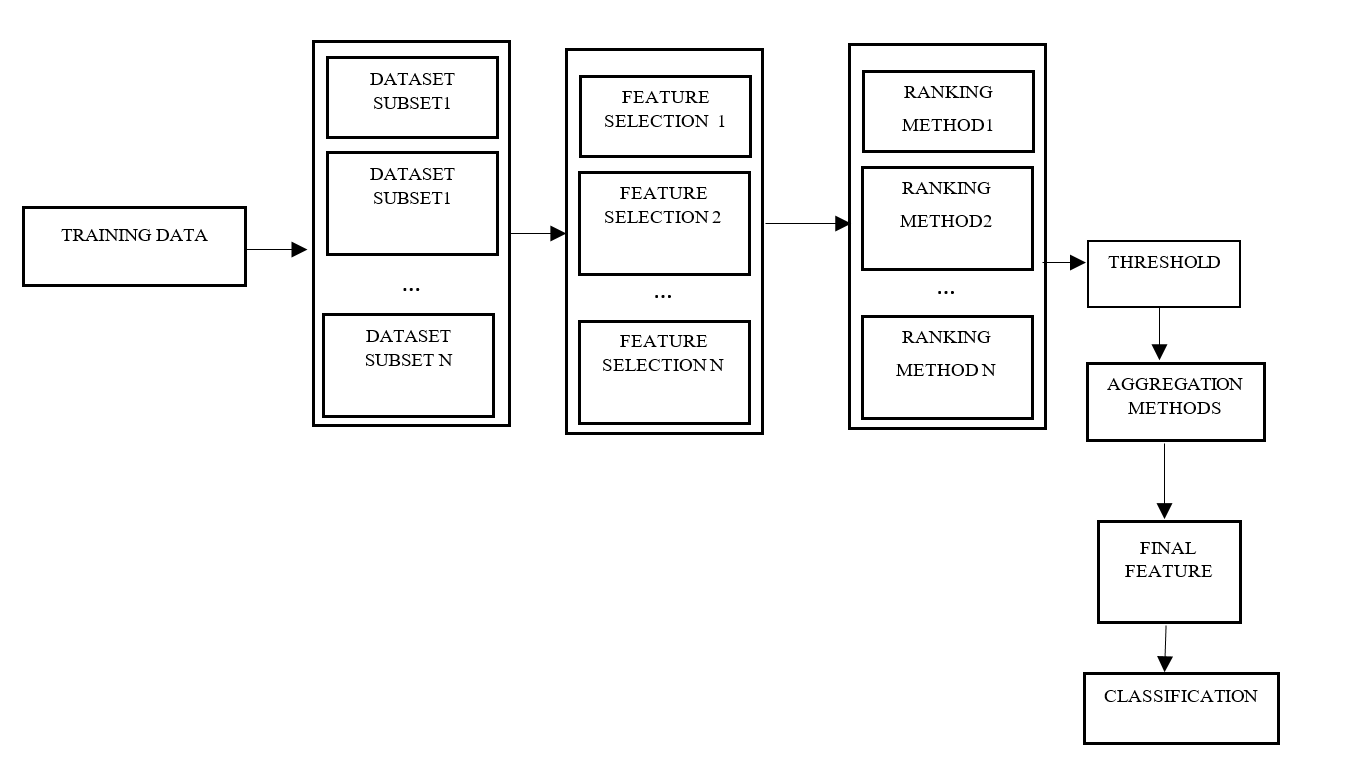
In model III the dataset split into different data subsets shown in Figure 12. Each data subsets are applied with different base selectors for feature selection. Different ranking algorithms could be used to rank the scores. The features with ranks can be aggregated using various aggregation techniques like mean, borda etc. The final features can be selected by applying threshold to the feature subset.



**Figure 12. Model III-Ensemble Feature Selection Approach**

**Model IV**

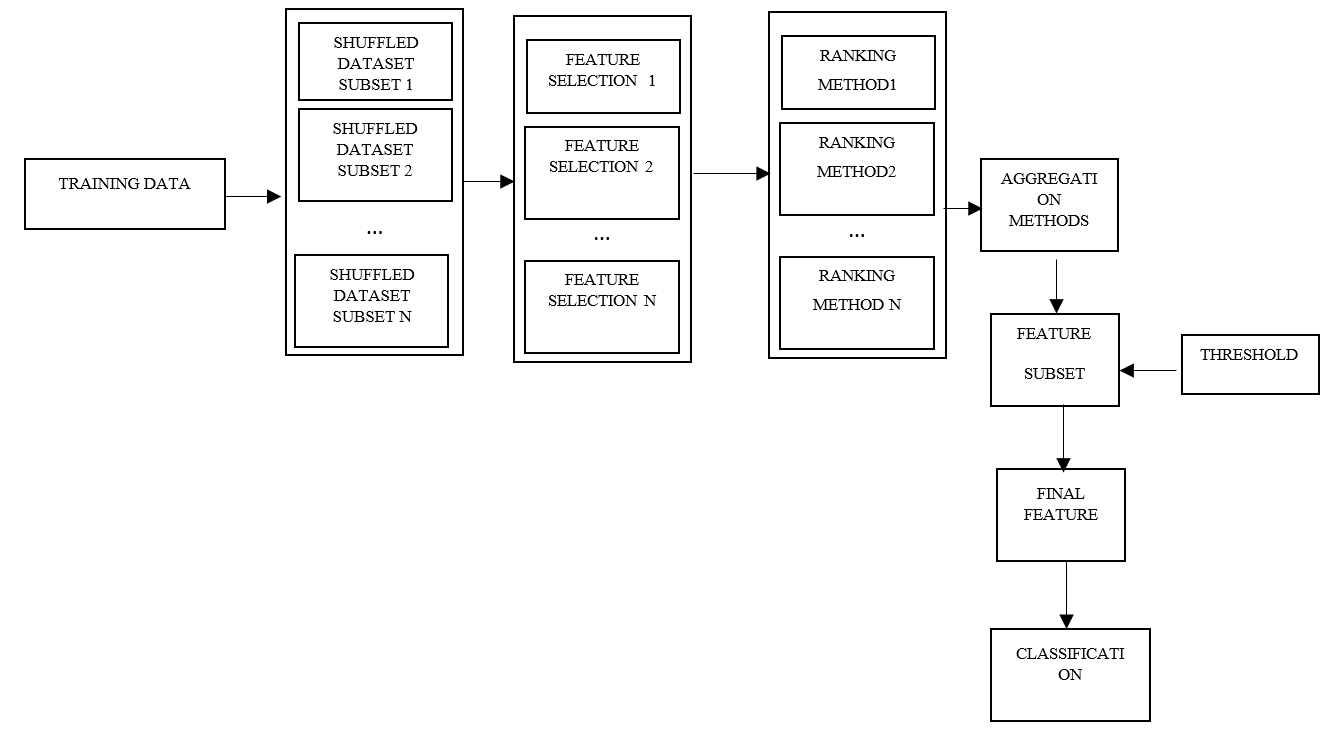
In model IV the dataset split into different data subsets shown in Figure 13. Each data subsets are applied with different base selectors for feature selection. Different ranking algorithms could be used to rank the scores. Threshold is applied to the feature list and the features with ranks can be aggregated using various aggregation techniques.



**Figure 13. Model IV-Ensemble Feature Selection Approach**

**Model V**

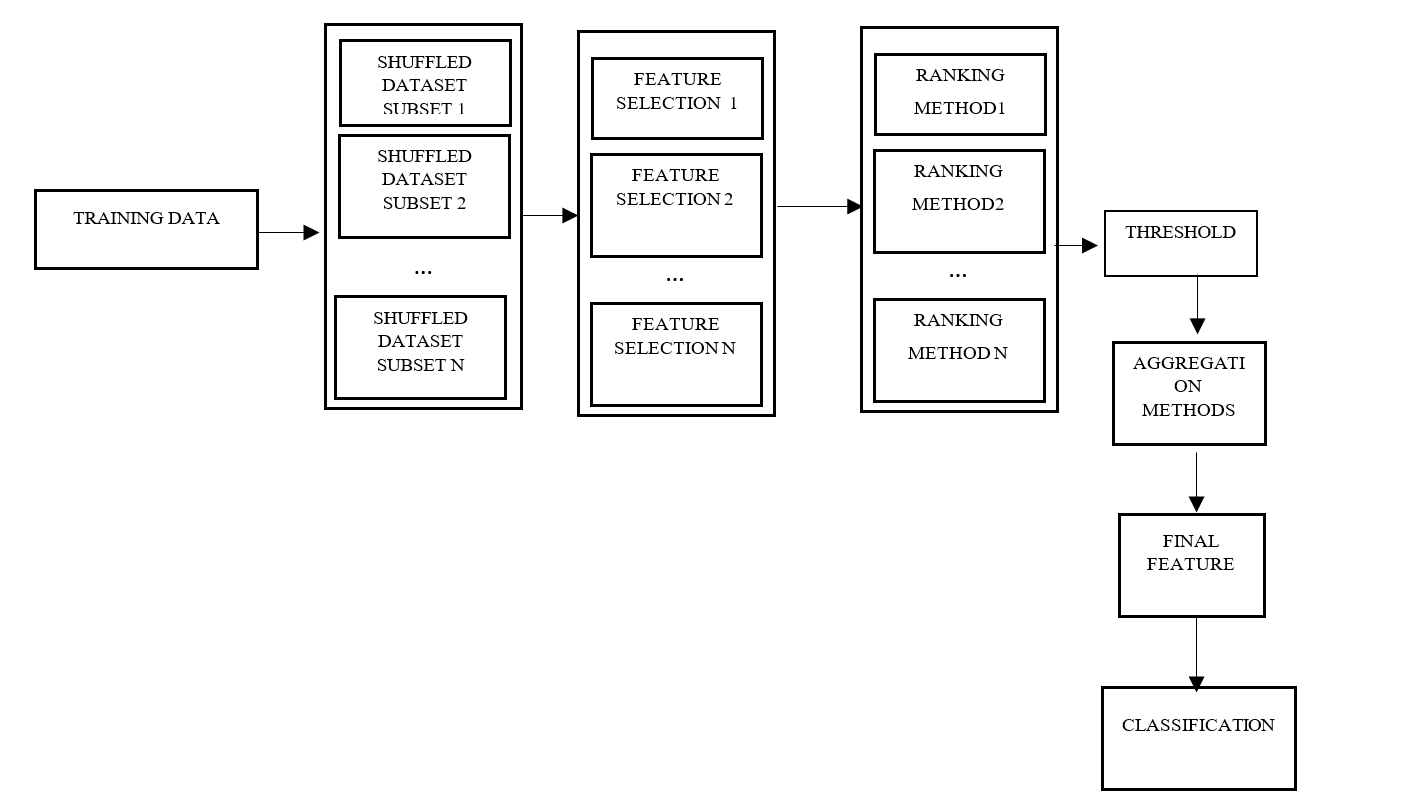
In model V the dataset split into different data subsets. The data subsets are shuffled to form a new data subset shown in Figure 14. Each shuffled data subsets are applied with different base selectors for feature selection. Different ranking algorithms could be used to rank the scores. The features with ranks can be aggregated using various aggregation techniques. The final features can be selected by applying threshold to the feature subset.



**Figure 14. Model V-Ensemble Feature Selection Approach**

**Model VI**

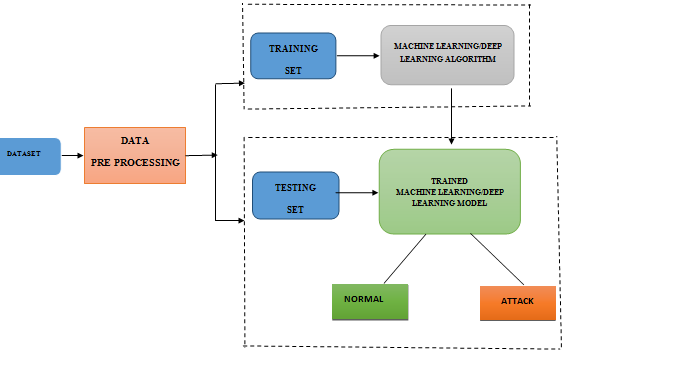
In model V the dataset split into different data subsets. The data subsets are shuffled to form a new data subset. Each shuffled data subsets are applied with different base selectors for feature selection shown in Figure 15. Different ranking algorithms could be used to rank the scores. Threshold is applied to the feature list and the features with ranks can be aggregated using various aggregation techniques.

****

**Figure 15. Model VI-Ensemble Feature Selection Approach**

1. **CLASSIFICATION MODELS**

It tries to reduce something from given data. A classification model will try and predict the value of one or more outputs given one or more inputs. Labels which may be appended to a dataset are called outcomes. IDS are investigated for use in a variety of approaches, including ML &DL. These approaches are wont to evaluate IDS performance, also as to define many elements and properties, like intrusion detection, positioning of IDS devices within the network, and methods for IDS evaluation. With the labelled dataset, classification-based approaches classify the info into recognized classifications [13] [14]

[15]. The Classification process is depicted in figure in 16

**Figure 16. Classification Model**

Decision Tree, ANN, SVM, Fast Learning Network, and Ensemble Methods are some of the techniques utilized in IDS. The algorithm and methodology used in the literature are:

**Table 1 ML/DL intrusion studies**

|  |  |  |
| --- | --- | --- |
| **Literature** | **Algorithm** | **Methodology** |
| Shen et al[16] | Machine Learning | Ensemble with BAT |
| Ali et al [17] | Fat learning network |
| Yao et al [18] | K-means |
| Gao et al [19] | Ensemble method |
| Karatas et al [20] | ML algorithm with SMOTE |
| Yin et al [21] | Deep Learning | RNN |
| Jia et al [22] | DNN |
| Xu et al [23] | GRN |
| Xiao et al [24] | Convolutional neural network |
| Malaiya et al [25] | Fully connected network |
| Andresini et al [26] | Multistage Autoencoder and CNN |

1. **CONCLUSION**

This survey paper goal is to provide a thorough overview of (IDS) in industrial control systems and how attack detection has been accomplished using it. Taxonomy of Intrusion Detection System, approaches to feature engineering selection, computational intelligence methods utilized for IDS, and datasets created and used for IDS measuring performance is studied. Various hybrid feature selection models are proposed for intrusion detection system which improves the overall performance of industrial systems. In the future, the proposed feature selection models will be implemented and compared with other existing models.

[1] Colbert, Edward JM, and Steve Hutchinson, "Intrusion detection in industrial control systems", Cyber-security of SCADA and other industrial control systems. Springer, Cham, 2016. 209-237.

[2] R. Mitchell and I.-R. Chen, "A Survey of Intrusion Detection Techniques for Cyber-Physical Systems", *ACM COMPUTING SURVEYS*, vol. 46, no. 4, MAR 2014.

[3] S. V. B. Rakas, M. D. Stojanovic and J. D. Markovic-Petrovic, "A Review of Research Work on Network-Based SCADA Intrusion Detection Systems", *IEEE ACCESS*, vol. 8, pp. 93 083-93 108, 2020.

[4] Sajith, P. J., and G. Nagarajan, "Optimized Intrusion Detection System using computational intelligent algorithm", *Advances in electronics, communication and computing*. Springer, Singapore, 2021. 633-639.

[5] Khraisat, Ansam, and Ammar Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges", *Cybersecurity* 4.1 (2021): 1-27.

[6] Cai, Jie, et al. "Feature selection in machine learning: A new perspective", Neurocomputing 300 (2018): 70-79.

[7] Di Mauro, Mario, et al. "Supervised feature selection techniques in network intrusion detection: A critical review" Engineering Applications of Artificial Intelligence 101 (2021): 104216.

[8] Nimbalkar, Pushparaj, and Deepak Kshirsagar, "Feature selection for intrusion detection system in internet-of-things (IoT)", ICT Express 7.2 (2021): 177-181.

[9] Krishnaveni, S., et al. "Efficient feature selection and classification through ensemble method for network intrusion detection on cloud computing", Cluster Computing 24.3 (2021): 1761-1779.

[10] Jaw, Ebrima, and Xueming Wang, "Feature selection and ensemble-based intrusion detection system: an efficient and comprehensive approach", Symmetry 13.10 (2021): 1764.

[11] Herrera-Semenets, Vitali, et al. "A multi-measure feature selection algorithm for efficacious intrusion detection", *Knowledge-Based Systems* 227 (2021): 107264.

[12] Safaldin, Mukaram, Mohammed Otair, and Laith Abualigah. "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks", *Journal of ambient intelligence and humanized computing* 12.2 (2021): 1559-1576.

[13] Kunang, Yesi Novaria, et al. "Attack classification of an intrusion detection system using deep learning and hyperparameter optimization", *Journal of Information Security and Applications* 58 (2021): 102804.

[14] Yousefnezhad, Maryam, Javad Hamidzadeh, and Mohammad Aliannejadi. "Ensemble classification for intrusion detection via feature extraction based on deep Learning", *Soft Computing* 25.20 (2021): 12667-12683.

[15] Ge, Mengmeng, et al. "Towards a deep learning-driven intrusion detection approach for Internet of Things", *Computer Networks* 186 (2021): 107784.

[16] Shen Y, Zheng K, Wu C, Zhang M, Niu X, Yang Y, “An ensemble method based on selection using bat algorithm for intrusion detection”, Comput J. 2018;61(4):526-538.

[17] Ali MH, Al Mohammed BAD, Ismail A, Zolkipli MF, “A new intrusion detection system based on fast learning network and particle swarm optimization”, IEEE Access. 2018;6:20255-20261.

[18] Yao H, Fu D, Zhang P, Li M, Liu Y, “MSML: a novel multilevel semi-supervised machine learning framework for intrusion detection system”, IEEE IoT J. 2018;6(2):1949-1959.

[19] Gao X, Shan C, Hu C, Niu Z, Liu Z “An adaptive ensemble machine learning model for intrusion detection”, IEEE Access. 2019;7:82512-82521.

[20] Karatas G, Demir O, Sahingoz OK, “Increasing the performance of machine learning-based IDSs on an imbalanced and up-to-date dataset”, IEEE Access. 2020; 8:32150-32162.

[21] Yin C, Zhu Y, Fei J, He X, “A deep learning approach for intrusion detection using recurrent neural networks”, IEEE Access. 2017;5:21954-21961.

[22] Jia Y, Wang M, Wang Y “Network intrusion detection algorithm based on deep neural network”, IET Inf Secur. 2018;13(1):48-53.

[23] Xu C, Shen J, Du X, Zhang F “An intrusion detection system using a deep neural network with gated recurrent units”, IEEE Access. 2018;6:48697-48707.

[24] Xiao Y, Xing C, Zhang T, Zhao Z “An intrusion detection model based on feature reduction and convolutional neural networks”, IEEE Access. 2019;7:42210-42219.

[25] Malaiya RK, Kwon D, Suh SC, Kim H, Kim I, Kim J “An empirical evaluation of deep learning for network anomaly detection”, IEEE Access. 2019;7:140806-140817.

[26] Andresini G, Appice A, Di Mauro N, Loglisci C, Malerba D, “Multi-channel deep feature learning for intrusion detection”, IEEE Access. 2020;8:53346-53359.