Information Sciences 648 (2023) 119530

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Towards data security assessments using an IDS security model for cyber-physical smart cities

Arun Kumar Sangaiah [a,d], Amir Javadpour [b,c,*], Pedro Pinto [b]

[a] International Graduate Institute of AI, National Yunlin University of Science and Technology, Taiwan
[b] ADiT-Lab, Electrotechnics and Telecommunications Department, Instituto Politécnico de Viana do Castelo, Porto, 4900-347, Portugal
[c] Department of Computer Science and Technology (Cyberspace Security), Harbin Institute of Technology, Shenzhen, China
[d] Department of Electrical and Computer Engineering, Lebanese American University, Byblos, Lebanon

ARTICLE INFO

Keywords:
Smart operation systems
INTERACT
Smart cities
Intrusion detection system
Multilayer perceptron
KDD99

ABSTRACT

Technology has enabled many devices to exchange huge amounts of data and communicate with each other as Edge Intelligence in Smart Cities (EISC), as a result of rapid technological advancements. When dealing with personal data, it is paramount to ensure that it is not disclosed and that there is no disclosure of any confidential information. In recent decades, academics and industry have spent considerable time and energy discussing security and privacy. Other systems, known as intrusion detection systems, are required to breach firewalls, antivirus software, and other security equipment to provide complete system security in smart operation systems. There are three aspects to an intrusion detection system: the intrusion detection method, the architecture, and the intrusion response method. In this study, we combined linear correlation feature selection methods and cross-information. The database used in this article is KDD99. This paper examines applying two feature selection methods in predicting attacks in intrusion detection systems based on INTERACT and A multilayer perceptron (MLP). Since the number of records associated with each attack type differs, one of our suggestions is to continue using data balancing techniques. As a result, the number of records associated with each type of network status becomes closer together. The results in the categories can also be improved using information synthesis methods, such as majority voting.

1. Introduction

Recently, the issues of detection systems for preventing and not damaging the network were raised; a lot of research has been done in this field. A detection system is one or more systems that change the ability to detect specific behaviors in a host or network. Safety is synchronized when unwanted deeds are conducted during a system [1–3]. Users can benefit from the solitude with care and availability of smart operating systems. The current networks are holding their places as a significant phenomenon in modern societies and are being addressed and considered by more lawbreakers and antagonists. Beyond the approaches created to stop the disturbance, including applying various passwords and firewalls to safeguard facts and figures, other procedures are used, like confirming the user. The other way to shield the computer seems to codify and distinguish the intrusion. Identifying the interventions

* Corresponding author at: Department of Computer Science and Technology (Cyberspace Security), Harbin Institute of Technology, Shenzhen, China.
E-mail addresses: arunkumarsangaiah@gmail.com (A.K. Sangaiah), a.javadpour87@gmail.com (A. Javadpour), pedropinto@estg.ipvc.pt (P. Pinto).

https://doi.org/10.1016/j.ins.2023.119530
Received 29 January 2023; Received in revised form 8 August 2023; Accepted 10 August 2023

Available online 19 August 2023

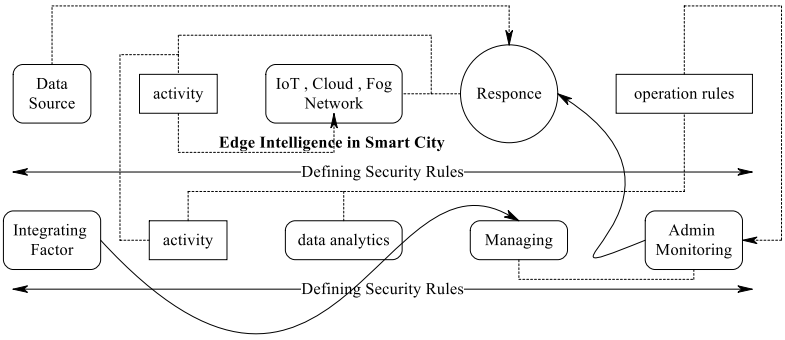


Fig. 1. Defined security rules and different IDS parts to build a monitoring system in EISC.

looks essential to categorize either internal or external practices by the unapproved users or possible misusers and cause harm to the computer networks and systems [4–6]. Among computer networks, the Edge Intelligence in Smart City (EISC), as the particular section, has recently reached a widespread status since they are exposed to almost all users, safe for even inexperienced persons, and reliable among proponents and opponents. They cause great development relevant to e-commerce, interests, hobbies, and social media. Modern market figures and businessmen have been applying such platforms to transact their goods and services. The citizens can reach this platform to embark on government services. Therefore, the users, based on intentions and determinations, tend to rely on various cyber sites by offering their financial and personal information to enable them to obtain market items, to involve in social media, to benefit from government services, and follow entertainment on certain sites. Since such computer-based interaction among people has increased, cyber-theft, cyber-attacks, and other cyber-crimes would be inevitable and numerous so the formal authorities and casual businessmen are worried about the safety of their affairs. Therefore, the researchers and the concerned figures in this field have suggested several prohibiting strategies to promote safety against the mentioned cyber risks [7–11]. It is certain that the main cause for the alleged and wide-used of wireless sensor networks appears its cost-effectiveness. However, much money normally should be used to uphold the security of hardware and software facilities. Regarding the research done in this field, it should be noted that the issue of cost and price has received less attention than computational load and such issues [12]. Therefore, it is necessary to reduce costs along with reducing computational load, reducing algorithm steps, increasing the life of nodes, and achieving a higher security factor [13,14].

The definition of hacking sounds to bring the secure status of a computer system to an insecure position to be arranged for illegal actions. In other words, it is considered a security system if it assures confidentiality, inclusiveness, and availability of the needed materials and sites for the target users. The following part will be oriented to describing the constituents of IDS Intrusion (Hacking) detection systems [1,15]. Activity is an action or event which is performed on the source; it is attractive and efficient for users. Activities can be both true and false, meaning that suspicious activity can be malicious and would be dangerous for the source, for example, a TCP connection request that is periodically sent from an IP address could be a sample of suspicious activity. An administrator is actually the person (individual) responsible for compiling security statements about the organization. These individuals are responsible for deciding about implementing and configuring IDSs. The manager makes decisions based on the level of alerts, log history, and session monitoring capabilities. They are also responsible for deciding about the response to intrusion and also a confidence about the effective response to attack [16]. A warning message (alert) is issued when an analyzer system detects a suspicious incident. This warning gives us information about the exact action that has been done along with an explanation of the exact kind of action taken: for example when there is a lot of huge data of ICMP protocols entering the server or a lot of unsuccessful login requests; it alerts by an analyzer system. There is always some usual traffic for a network. When this traffic passes the regular limits and gets abnormal; the analyzer is a parameter or an action that analyzes the data by a sensor [17]. This process analyzes the data for seeking suspicious activities. The analyzers monitor the actions and recognize if they are suspicious and if they work due to IDS terms by concerned processes. Data sources can include inspection or audit. Files, system logs or network traffic that consists of IDS' events is an assurance that happens in the data source that shows suspicious activity. An event can cause an alert. Events always log to refer in later. Events can report unusual network warnings. An IDS could start recording events when the internal connection of the server email got locked; an Event can be a determination of someone searching and discovering from your network. Eventually, it can alert that network traffic volume exceeds the normal limits and needs to check out. A manager is also a tool or process for the operator to manage the IDS. The IDS management console is the manager of it. The only way to make changes in the IDS setting is by connecting to the manager; the operator is a personal operator in overall charge of the IDS system. This person could be a manager, a network manager, or user or any other person, but should take responsibility for this position. As you see, an IDS consists of different parts and processes together so that they can monitor a correct image of the transferred traffic in your network at the moment. Fig. 1 shows the different parts of the system to make a complete IDS system. The data could gather from different sources and they should be analyzed completely to recognize what exactly happening in the network. The main purpose of an IDS system is not to block traffic in a network, although some IDSs have that capability. The IDSs monitors and inspects traffic and prosecution system naturally.

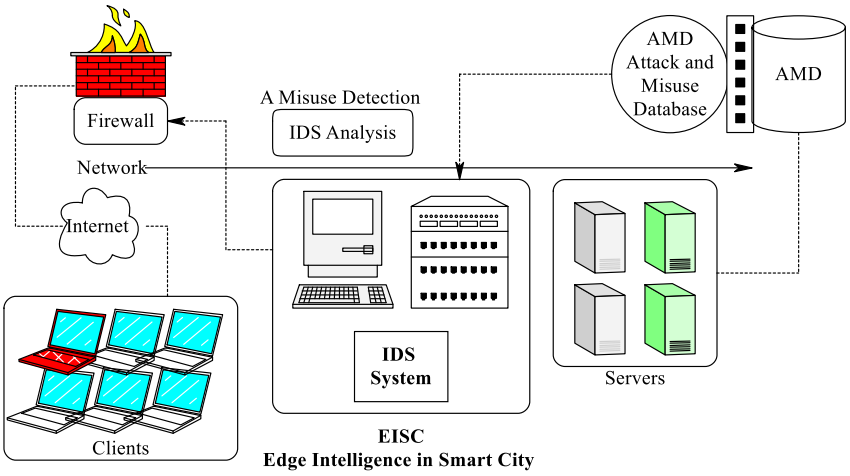


Fig. 2. A Misuse Detection – IDS in the operating environment.

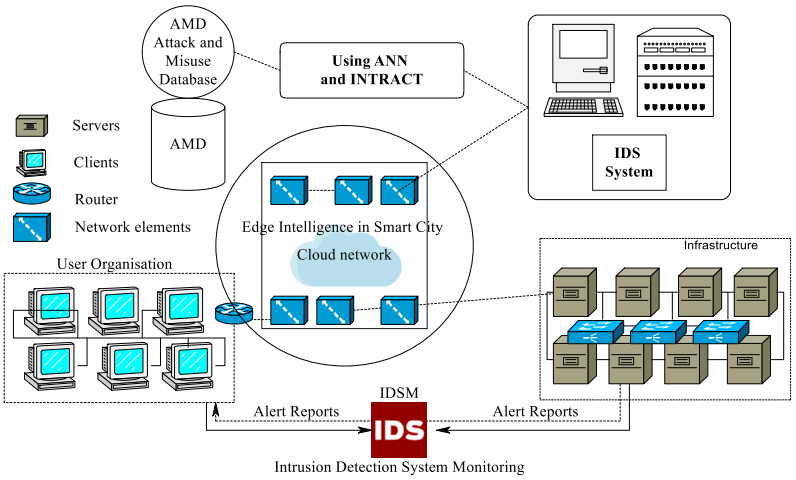


Fig. 3. An intrusion detection system using expert system technologies for intrusion detection.

1.1. Problem statement

IDSs generally are divided into two main kinds based on the capabilities they present to their operators: Intrusion detection systems and Misuse Detection IDS. This IDS mostly works due to attack analysis based on attack signatures and their effects (Audit–Trails) in the network. Attack IDs or Attack features are the ways invaders use to attack a system, e.g. a TCP Flood starts by sending multiple bogus TCP Sessions. If MD-IDS (Misuse Detection IDS) know how the TCP Flood attacks work, it can report or react properly to it by recognizing it. Fig. 2 shows you a complete map of how an MD-IDS act. Remember that these IDS's have a database of usual ways of making an attack or an Attack Signature Database to compare the attack way. This signature can be compared with antivirus structure [18,19]. Anomaly Detection IDS: This kind of IDS known as AD-IDS too refers to unusual behaviors on the network; that means that it works outside its database extent and has a kind of smart decision-making. This kind of IDS is actually a kind of educational program. First of all, it analyzes the usual actions of the network and the traffic, and then whenever the traffic causes systems to go out of this analysis status, it starts to alert and send it to the system operator.

IDSs generally focus on reports of network events that deviate from previous network patterns that contain routine network traffic and behaviors. Managers should be introducing a pattern from ordinary traffic and behaviors from a source of traffic and ordinary network behaviors as the source of IDS reviews. This source will be used as the main basis for comparisons and reports of this intrusion detection system in the future. For example, your IDS may report that you received more ICMP information packets at a specific time of day. This type of activity may be the beginning of a SYN FLOOD attack. The system will also report if a user who normally only accesses systems during daytime hours requests login with managerial access at night. Fig. 3 This AD-IDS system shows the track and report when there is a conflict from normal traffic. Process AD-IDS systems continuously are used artificial intelligence technologies and Expert Systems to analyze ordinary network traffic [9].

When dealing with personal data, it is paramount to ensure that it is not disclosed and that confidential information is not disclosed. In recent decades, academics and industry have spent considerable time and energy talking about security and privacy. Other systems known as intrusion detection systems are required to be able to breach firewalls, antivirus software, and other security equipment in order to provide complete system security. There are three aspects to an intrusion detection system: the intrusion detection method, the architecture, and the intrusion response method. In this study, we combined linear correlation feature selection methods and cross-information. The database used in this article is KDD99. This paper examines the application of two feature selection methods in predicting attacks in intrusion detection systems based on INTERACT and A multilayer perceptron (MLP). Since the number of records associated with each attack type differs, one of our suggestions is to continue using data-balancing techniques. As a result, the number of records associated with each network status type becomes closer. The results in the categories can also be improved using information synthesis methods, such as majority voting.

In most commercial systems, AD-IDS and MD-IDS are combined. They are the best opportunity to detect and deactivate the attacks and unauthorized (illegal) system access. Unlike firewalls, IDSs detect and report problematic and suspicious traffic instead of blocking it, and it also reports any suspicious activity on the network.

1.2. Motivations

The safety of the network depends on a set of instruments and approaches such as anti-virus software or preventive measures including firewalls deployed in companies [20]. One of the ways to prevent or at least detect malware or hackers is to apply intrusion detection to increase security along with other defense layers. The strategy of an intrusion detection system is to search, spot, and detect spasms or other bad behaviors by screening incoming traffic which may damage the network or host. Intrusion detection systems can be based on misuse based or anomaly-based or both methods according to the methods used to diagnose. Most intrusion detection systems such as Snort and Bro are based on abuse [21]. These systems maintain rules in a database that are actually known as signatures and attack patterns. In order to detect an attack in intrusion detection systems, it compares received packets from incoming traffic with these rules, and if the received package and rules are matched, it shows an appropriate reaction (e.g. SNORT features more than 9,000 rules, categorized into 51 detection libraries [22]). Anomaly-based intrusion detection systems learn the permissible and normal behaviors of the system over time and it compare any future system behaviors with these behaviors, and if they observe the anomalous behavior, they take the necessary operation [23]. Conventional intrusion detection systems operate in such a way that by detecting the attack, it alerts the network operator in order to take the necessary steps to prevent an attack. Also, some types of intrusion detection systems can perform the appropriate action automatically which previously have defined by the network administrator when detecting attacks. These systems are called Intrusion Prevention Systems (IPS). In general, the systems that have both diagnosis and prevention abilities are called Intrusion Detection/Prevention Systems (IDPS). In this article, “intrusion detection systems” means IDPSs which are based on dysfunction. We intend to increase the precision level of intrusion detection in clouds; therefore, a brand new method for intrusion detection is suggested pursuant to the intrusion diagnosis systems and different kinds of their architecture. After training and testing data are collected, NKDD99 will be used. The findings of this study and other conducted ones armed with updated features can be compared to clarify the results [2].

2. Work background

2.1. IPS and IDS techniques

Some factors should be considered for the efficiency of IPS and IDS in the cloud to solve many threats. These features include the techniques utilized to promote the IDS, the related status within the network, the pertinent combination, etc. It is worth noticing that the old IDS and IPS can be tapped as beneficial means for cloud security since they are practically applied in artificial intelligence as a signature or a diagnosis aspect [14].

2.2. Recognition based on signature

The IDS brings about high levels of accuracy and the least false positives according to the signature. The known attacks have affected the dissimilarities in the study. Therefore, it can be concluded that the identification method cannot differentiate between unknown and known attacks. One of the causes for applying this method is to deal with the perpetuation and utilization of the updates easily. The useful leads related to intrusion prevention systems are attainable [24] due to the signatures and potential outlines.

2.3. Identification of anomaly

Anomality identification is related to identifying events associated with the anomalous normal behavior of a system. An extensive type of these techniques comprises data mining, statistical modeling, and Markov concealed models that are presented in various methods to meet anomaly identification problems. Statistical tests for identifying anomalies have been employed to analyze activities and information about approved users’ behavior over some time. This is used in identifying previously known attacks [25].

An anomaly-based solution to prevent real-time intrusion was proposed that analyzed protocol-based attacks and multimodal traffic [26]. However, there is an optimal area for reducing the number of IPS. Pranto et al. in 2022 introduced the intrusion detection

system to be able to detect the intruder in real-time effectively. Behavioral profiles and information extraction techniques are used to detect a coordinated attack and anomaly with basics features selections in IDS [27]. By applying cloud anomaly detection techniques, spotting and finding the unidentified cloud risks can be pursued at different stages. Since there are many events that may happen on the network and system, it seems hard to notice or govern the intrusions in the Cloud just through the use of anomaly detection techniques mentions the approaches to detect anomaly at diverse stages of the Cloud that inspect intrusion detection [28]. Intrusion detection is a good application of soft computing techniques because it can deal with unknown and somewhat realistic information. Numerous gentle computational methods exist, including artificial neural networks (ANNs) [29], ambiguous logic relational laws, support vector machines (SVMs), and genetic algorithms (GAs) [30]. IDS-based anomaly detection or signature-based IDS can be corrected by using the algorithms.

2.4. Neural network-based IDS

The plan consists of nine features: Protocol IDs, source ports, destination ports, source IP addresses, destination IP addresses, ICMP types, raw data lengths, and raw data. Nevertheless, it seems that there is inaccuracy in Intrusion detection. Javadpour et al. [2] (2017), for example, improved an MLP. The results of their study portrayed that higher layers functioned superior at finding hidden information. MLP and self-organization maps (SOM) were employed and the details of the success rates for penetration were presented in [31]. The study's findings showed that SOM is more precise than ANN at detecting penetration. To prevent the rate of most network attacks, Distributed Time Delay Neural Networks (DTDNN) are assumed to bear a better detection accuracy. Considering the great speed and high conversion rate, classifying data can well be done with this useful and simple method. By merging this method with the other gentle computational techniques described above, the preciseness of the method got developed [32]. Ahmed et al. suggested the usage of artificial neural networks (ANNs) to identify cloud anomaly spasms. Yet, by using this approach, training samples and longer periods of time are needed to identify intrusions [33].

2.5. IDS based on Fuzzy logic

Fuzzy logic can be used to control the normal explanation of intrusions [17]. A fuzzy IDS system called the Fuzzy Intruder Detection System (FIDS) is suggested to identify intrusions like SYN, UDP streams, FTP/Telnet passwords, and port scanning [33]. Decreasing the time of training an ANN, Chavan et al. (2004) created Entangled Fuzzy Neural Networks (EFuNN). Both controlled and uncontrolled processes are needed for training. The finding of the research proposes the idea that applying a reduced number of EFuNN inputs causes a better classification accuracy for IDS than employing ANNs [34]. Because of the extended training period, it seems difficult to follow the suggested approaches [35] and [36] to identify network intrusions in real time. In this regard, Su et al. (2022) planned fuzzy rules to identify intrusions in a timely manner. Two online sets of data were hired to clarify the results. This method is widely used to involve DoS and DDoS attacks. In order to minimize the consumed time to identify the unidentified attacks in the cloud, fuzzy logic, and ANN are used [37].

2.6. Association rule based on IDS

According to the recognized attacks or kinds of them, some of them are invented. An algorithm that identifies a subset of such attacks can be used to detect them (by detecting some of their main features). The researchers apply data extraction to identify intrusions in this study. They also use a signature-based algorithm to detect abuse. It is certain that it is time-consuming to make a decision and to create signatures. The postponement in perusing dates has been removed in [38]. Such an algorithm has been offered to shape more useful signatures relevant to formerly recognized attacks. Then the new signatures in the Cloud have been built up by the rules. Then, the identification of every recognized attack in real time will be possible by creating new signatures.

2.7. IDS based on support vector machine (SVM)

The researchers employed a fixed data sample SVM to identify intrusions in [39]. With no regard to the scope of the data, this looks accurate. When SVM was used, the rate of false positives became reduced in [40] when it was compared to ANN. SVM needs merely a few factors against ANN, which needs many samples. This is a result of the usage of SVMs with binary data. Apart from this concern, SVM can be associated with further procedures to advance detection precision. On the condition that the sample data is restricted to intrusion detection in the cloud, SVM seems a very useful answer. For this reason, SVM-based identifiers do not suffer from the size of the data [41].

2.8. IDS based on genetic algorithm (GA)

The Genetic algorithm-based feature is used to select the network properties in determining the optimal parameters. Therefore, this technique can be used for other techniques to achieve optimal results and improve results. The suitable purpose was planned through tractability and a modest safety structure. Network intrusions are identified over widespread guidelines. This article uses numerical and qualitative features to generalize the classified rules, which improves the identification and accuracy of the results. A method for identifying abuse and anomalies through a combination of fuzzy and genetic algorithms was introduced in [24]. To identify invasions, fuzzy algorithms are applied to present qualitative factors and genetic algorithms are employed to control the

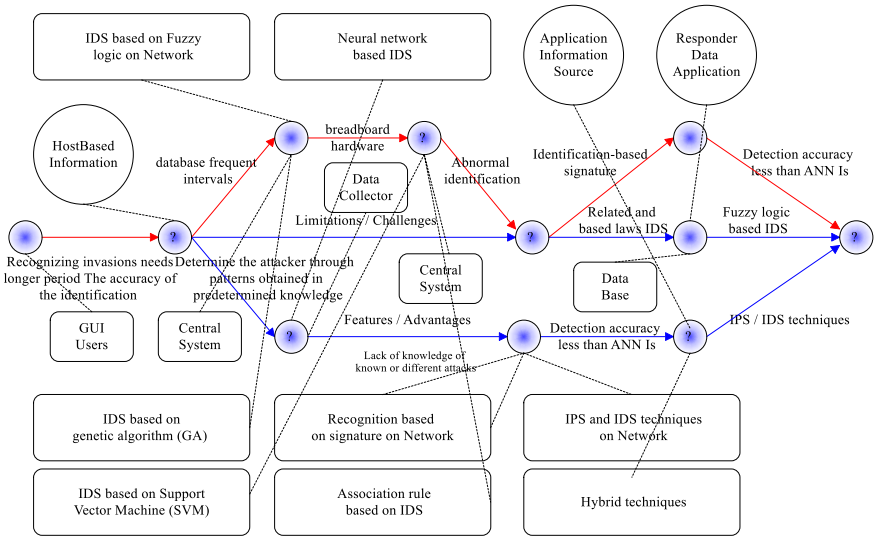


Fig. 4. An intrusion detection system using expert system technologies for intrusion detection [9].

factors that look most suitable for numerical fuzzy purposes. In the cloud environment, selecting the optimal parameters (network properties) to detect intrusion increases the accuracy of IDS. IDA-based GA genetic algorithm is used in the Cloud.

2.9. Hybrid techniques

These techniques use a combination of two or more of the above techniques. As shown in Fig. 4, NeGPAIM Is a combination of two low-level components in hybrid techniques consisting of Fuzzy logic to detect abuse and neural networks to detect abnormalities. It also has a high-level component and the central analyzer motor is the result of two low-level components. This is an effective model that does not require updating of dynamic rules.

To modify IDS performance, in [42] proposed a procedure in which a combination of Naïve Bayes, ANN, and the DT decision tree is classified into three separate data sets. The independent outputs of each classifier were combined by using multiple fuzzy methods. This process has used the advantage of each class and modifies the overall performance of IDS.

There are so many benefits in soft computing methods over outdated IDSs in the Cloud environment. Nevertheless, each method bears pros and cons that influence the presentation of the IDS. There are two shortcomings in an ANN; for example, it involves longer training time and a low level of flexibility. As fuzzy logic was added to data mining methods, flexibility got increased. Since GA's fuzzy logic increases IDS function, GA indicates the most suitable guidelines on behalf of IDS. As it is employed when used by means of a particular scheme, GA seems more beneficial due to the combined designs than as it is conducted with a common scheme. Applying SVMs to run several network sorts can be desirable. The pertinent law should be applied based on IDS according to particular risks. Yet, the success of a rule connected to IDS hinges on the application of knowledge. IDS / IPS techniques indicating their advantages and disadvantages are summed up in the Table 1 [43,44].

3. Proposed method

Some simulated computers can be linked to one another to declare that cloud computing functions as a sort of circulated, analogous computing scheme. When the service providers and service users hold the bond negotiations, such computers come extremely into use and are measured as one of the several incorporated computing assets. When an extremely interacted simulated machine prepares services, an original set of data centers by which the users can reach the services from various sites can be shaped by the cloud computing process. Because the Cloud platform still keeps its evolution and plays a role as an essential portion of our lives, a Cloud IDS shows its role and significance more around us. Nevertheless, there are some challenges and flaws with the current intrusion detection techniques as they come into use in the Cloud platform. This chapter inspects the feasibility and practicality of a neural network-based intrusion detection system that applies feed-forward algorithms to identify invasions in cloud computing environments. In this case, MLP is used as an algorithm to help to learn through neural networks. Such architecture can help to approach so much data in a precise attempt. Neuronal networks (MLP) include a kind of disorder in layers of neurons arranged in a row. First, the input values step in the next layer and gather there. They become increased through the loads in the directions between the layers, and following the transient stop, they move via the matching network function, and finally, they are produced as the output. When the output is computed and compared with the anticipated output as well as a correction of the related weights in case of significant differences, a neural network can be well accomplished. The performance of both monolayer Perceptron and multilayer Perceptron seem to be conducted similarly. Consequently, the calculation of the output of a model is done according to an offered model for the network. By comparing the actual and desired outputs, there appears to be a change in the weight coefficients

Table 1
Summary of techniques used in IDS/IPS technologies for intrusion detection.

IPS/IDS techniques	Features/Advantages	Limitations/Challenges
Identification-based signature	⋄ Determine the attacker through patterns obtained in predetermined knowledge ⋄ Identifies earlier recognized invasions through excellent precision ⋄ As needing little computational properties	⋄ Lack of knowledge of known or different attacks ⋄ Unidentified invasions increase wrong warnings in top level
Abnormal identification	⋄ Employing numerical tests to pinpoint invaders pursuant to gather data and decrease wrong warnings as of unidentified invasions	⋄ Recognizing invasions needs longer period The accuracy of the identification depends on the amount of behavior collected or its characteristics
ANN Based on IDS	⋄ Proper classification of unstructured network packets ⋄ Multiply hidden layers in ANN The rate of efficiency increases the classification	⋄ More experimental phase time and samples are required ⋄ It has little flexibility
Fuzzy logic based IDS	⋄ Employed to safeguard quality ⋄ Presents superior adaptability when involving in undetermined concerns	⋄ Detection accuracy less than ANN
Related and based laws IDS	⋄ To identify signatures of known attacks or attacks related to misuse in identification	⋄ Unidentified invasions keep unrecognized forever ⋄ Formed rules are required to get monitored via database frequent intervals ⋄ Employed merely to misdirect Sensei
SVM Based on IDS	⋄ If limited examples are given, it can accurately classify attackers ⋄ May offer a large number of features	⋄ It only categorizes the attributes of the author, so the pre-processing of these attributes is necessary
GA Based on IDS	⋄ Used to select the best feature for identification ⋄ It has better performance	⋄ It is a complex method ⋄ It is a special method compared to the general type
Hybrid methods	⋄ An efficient way to classify rules correctly	⋄ The computational cost is very high

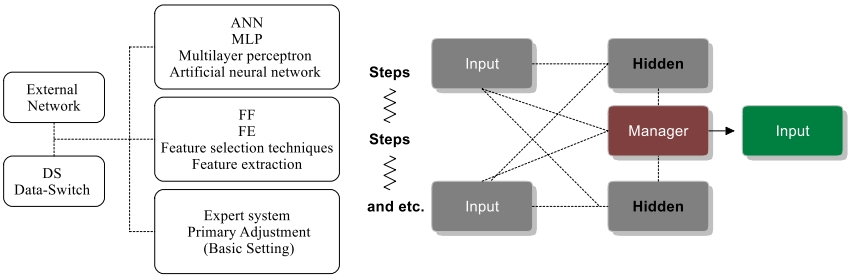


Fig. 5. Proposed IDS architecture in this research.

of the network. When we provide a model to an untrained network, it produces random outputs that define the difference between the actual output and the desired output by defining the error function [31]. This type of learning is called "Learning with the supervisor".

By following the configuration of the planned ANN, there is a kind of accountability meant for the input layer to handle the data collection procedure from the network. In order to stop any harmful functions in the process, the network is planned so carefully that it enables the researchers to deal with all requests and data flow and an input device is employed to input the data and then send them via the neural networks. By using ANN mechanisms, the hidden layers obtain raw data from the input layer and process it, sending it to the output layer to be evaluated there. Furthermore, such a layer updates the weight values of the input layer every time iterations are performed. The ultimate findings can be reached through the output layer by hiring the mean of the results established from the hidden layer (Fig. 5).

3.1. Primary adjustment (basic setting)

In the following, a network based on neural IDS is considered. According to the ability of machine learning in neural networks, the proposed IDS can detect a new type of attack with relatively accurate results (Fig. 5). Some of the parameters used in this research are as follows. The variables X, Y, and W are used as the input, the output, and the weight of the edge of the network, respectively. A complete list of these parameters is given in Table 2. To better illustrate how to replace variables, the architecture of a network which backward with the introduced variables is shown in Fig. 6. The steps are as follows (Fig. 6):

- Randomly set all weights and network threshold levels in the range $(\frac{-2.4}{F_i}, \frac{2.4}{F_i})$.

Table 2
The parameters used in this research and their description.

Parameter	Description
x	Network Inputs
y	Network Outputs
w	The weights of edges
θ	Correction required in the middle and output layers
e	Error value
σ	gradient error value
p	The number of repetitions
F_i	The total number of neuron inputs i in the network
n	Number of neuron inputs j in the middle layer
m	Number of neuron inputs k in the output layer
α	Training rate

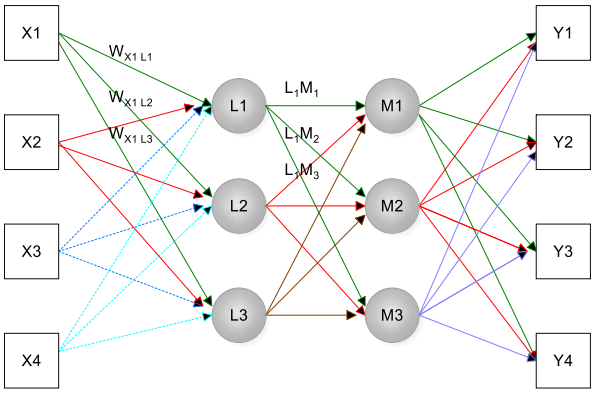


Fig. 6. Proposed Backward Neural Network Architecture for IDS.

- Calculate the output of neurons in the middle layer $y_j(p) = sigmoid \sum_{i=1}^{n} [x_i(p) \times w_{ij}(p) - \theta_j]$, where the Sigmoid function is an activation function and is calculated according to Equation (1). In this regard, the number e is the basis of the natural logarithm.

$$sigmoid(s) = 1 + \frac{1}{e^{-s}} \tag{1}$$

- Calculate the output of neurons obtained from the outer layer as Equation (2).

$$y_k(p) = sigmoid \sum_{j=1}^{m} [x_{jk}(p) \times w_{jk}(p) - \theta_k] \tag{2}$$

- Calculate the error gradient for output layer neurons as Equation (3), where $y_{d.k}(p)$ is the optimal value is at the output.

$$\begin{aligned} \sigma_k(p) &= y_k(p) \times [1 - y_k(p)] \times e_k(p) \\ e_k(p) &= y_{d.k}(p) - y_k(p) \end{aligned} \tag{3}$$

- Modify and update weights as Equation (4).

$$\begin{aligned} \Delta w_{jk}(p) &= \alpha \times y_j(p) \times \sigma_k(p) \\ w_{jk}(p+1) &= w_{jk}(p) + \Delta w_{jk}(p) \end{aligned} \tag{4}$$

- Calculate the gradient error for neurons in the middle layer based on Equation (5).

$$\sigma_j(p) = y_j(p) \times [1 - y_j(p)] \sum_{k=1}^{I} w_{jk}(p) \times \sigma_k(p) \tag{5}$$

- Modify and update weights as Equation (6).

$$\begin{aligned} \Delta w_{ij}(p) &= \alpha \times x_i(p) \times \sigma_j(p) \\ w_{ij}(p+1) &= w_{ij}(p) + \Delta w_{ij}(p) \end{aligned} \tag{6}$$

- End the loop and repeat from step 2 until the amount of error obtained is acceptable.

3.2. Feature selection

High-dimensional data platforms provide ample opportunities, along with various computational challenges. One of the main problems in these datasets is that not all features are often crucial for extracting the knowledge buried in the dataset [2]. Therefore, dimension reduction is still receiving considerable attention in various fields. Dimension reduction techniques can be divided into two main categories:

3.2.1. Feature extraction techniques

A lower-dimensional map is created from a higher-dimensional space. By means of joining the current structures and stabilizing the enclosed data, a slight collection of traits is shaped. The kinds of feature extraction techniques include linear and non-linear. Relevant to the common linear method, DFT, DWT, PCA, and FA can be mentioned. Self-Organizing Maps is the eminent extracting features-related technique.

3.2.2. Feature selection techniques

A subgroup of the unique features is designated in order to diminish the dimension. Classification, for example, acts better with condensed feature space than it does with unique space in some cases.

Feature selection is one of the problems discussed in machine learning and statistical pattern recognition. It is an essential part of various applications such as classification. Because these applications usually work with numerous features, most of which are either useless or provide little information. Keeping these features is not problematic in an informatics sense but imposes a considerable computational cost.

In this paper, two feature selection techniques, Pearson's linear correlation and Mutual Information (MI), are used to eliminate redundant and irrelevant features. In the proposed method, first, we use the linear correlation algorithm to reduce the feature space dimension. Then, the MI-based feature selection algorithm is applied to the features that were not selected in the previous stage. Calculating the shared data of any feature including the class label appears as the first step in this algorithm. The features are organized according to their shared data holding their own class label. Following the process of ranking for the features, the shared data between the feature including the highest MI and the other features in the dataset are calculated. The features with the slightest shared data and the feature of our interest are selected. We encompassed the designated features for each phase in the last set.

3.3. Detection and classification of attacks using data mining techniques

Various data mining techniques are used in attack classification. These techniques create more efficient support systems for AI services. Artificial Neural Networks (ANNs) are one of the most popular techniques used for this purpose. A trained neural network obtains the knowledge representing normal activities and different attacks to detect abnormal activities. In this research, we used the KDD dataset for training. Various qualitative and quantitative features are selected and analyzed for each network connection. Once trained, the neural network learns the different values of the features in normal and penetration situations. When an event is given to the network as input, the selected features will be fed to the input layer. From there, the learned values would travel through the hidden and output layers. The output layer would raise the alarm and prevent the activity's execution if a sabotage event is detected. The cloud environment manager would extract this information from the output layer. As the output layer exists in cluster masters, they seem the mere tools allowed to cooperate with the outside world.

Random Forest is another algorithm considered in this paper that has two inputs. A set of training records (E) and the features set (F). The algorithm uses a recursive approach for feature selection. The selected features are used to partition the feature space and create the internal nodes of the decision trees until the stopping criterion is met. Once the decision trees are created, a post-pruning step can be used to reduce the size of the trees. Too large decision trees are prone to over-fitting. Pruning can improve the decision trees' generalization capabilities by removing the initial tree's redundant branches.

4. Evaluation and results

In this paper, in order to evaluate the proposed method, several evaluation methods and criteria are used. The most common method is to draw an interference matrix (Fig. 7). The following is an overview of the interference matrix. The evaluation criteria which are considered in this article include Accuracy, Recall, and Precision results. Each number of the matrix is as follows:

- Precision

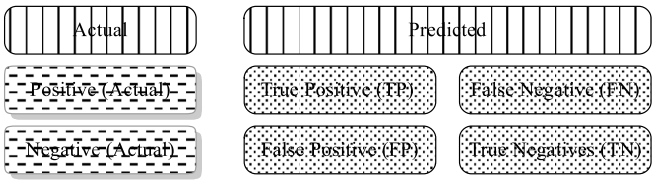
$$\text{Precision} = \frac{TP}{TP + FP} \tag{7}$$

- Recall

$$\text{Recall} = \frac{TP}{TP + FN} \tag{8}$$

- Accuracy

$$\text{Accuracy} = \frac{TP}{TP + FP + TN + FN} \tag{9}$$



"TN: Displays if the suggested system has properly recognized accounts for which the real sort is negative.
"TP: Assesses many accounts with a positive real sort and have been properly recognized through the offered algorithm because it includes a positive real sort.
"FP: Relevant to the outcome of the suggested algorithm, some accounts that are mistakenly recognized as positive pursuant to the actual data has been considered as positive.
"FN: Some accounts consist of the positive real data, but characterized as negative by the offered algorithm.

Fig. 7. Exponential of the interference matrix.

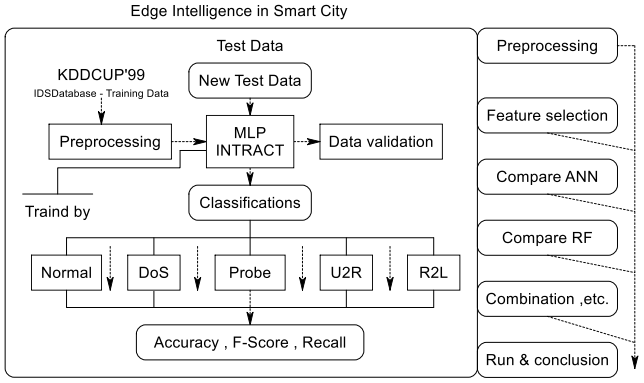


Fig. 8. The details of implementation HABCO method.

4.1. Maltab software

One of the most distinguished languages and ubiquitous environments is the statistical calculation, professional sketch, and software design, MATLAB. Many deeds such as the analysis of data, the creation of algorithms, and the creation of models and applications can be handled via it. When it is compared with its traditional counterparts such as C, C++, and Java, its capabilities to manage compound approaches and to detect quicker solutions would be illuminated [2].

4.2. Weka tools

To detect the data mining algorithms, a module called the Weka data mining system with the help of Java was improved by the University of Waikato in New Zealand. The challenges in the real world can be addressed when machine learning techniques are used. Data sets are run directly using this algorithm. Data preprocessing and classification tools, regression, clustering and dependency rules are also among these tools. The system includes tools for illustration as well. The package also develops machine learning algorithms. There is no licensing involved with this tool, and it uses an open-source data file format called ARFF, which consists of special tags to show different parts of the data file (Fig. 8).

4.3. Database used

The database of this study is considered as KDD. There are 42 features in the UCI Machine Learning dataset representing the regularity of the accounts or attacks in the data set. On the other hand, it shows the last features of the data class. This file inspects spasms such as dos and r2l, prop, and u2r. There are 10,000 records in total. There are no missing values in this database. In Fig. 9, the number of normal records and various attacks in the database is shown as a histogram [2].

4.4. Pearson correlation feature selection method

The approaches employed in this research include linear correlation and mutual information thanks to the feature selection for the achievement of the perfect precision oriented to the classification algorithms. A pack of prediction data about attacks and their types, KDD99 was hired. The researchers compare the values of the variables to be able to measure predictability through correlation-based criteria. Coefficients are identified as classical dependency criteria to detect the correlation between a property and a class. In the presence of a correlation between an X feature and class C that exceeds the correlation between an Y feature and class C, the X

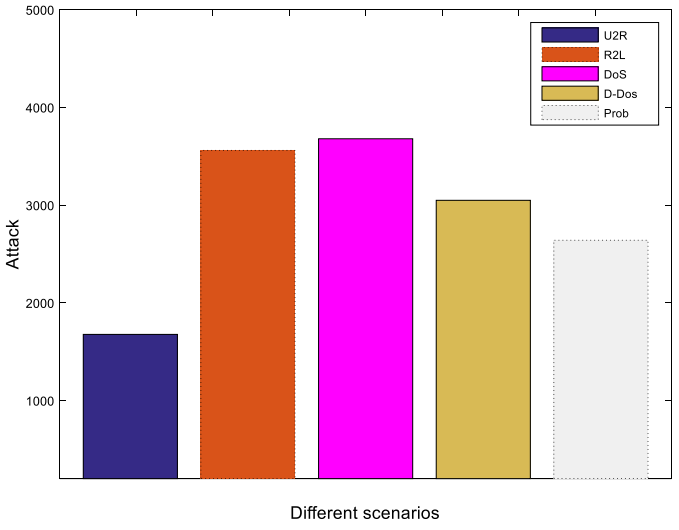


Fig. 9. Histogram of the number of normal conditions and different types of attacks in the database (Fig. 10).

Attacks	Descriptions	Sub Class
NORMAL KDD	Based on the **DARPA'98** Intrusion Detection System Evaluation Program. DARPA'98 consists 5 million records of various connections, each of which is about 100 bytes in size. The KDD training suite contains a total of 4900000 vectors of various connections, each vector consisting of 41 features and is categorized as usual or attack.	- **DARPA'98**
PRB KDD	PRoBing Investigation attacks (PRB): An attempt is made to obtain information on a computer network with the purpose of network security threats.	ipsweep, nmap, portsweep, satan **DARPA'98**
DOS KDD	Denial of Service (DoS) Attack: In this type of attack, an attacker is busy or filling a processor or memory source that cannot handle legitimate requests.	back, land, neptune, pod, smurf, teardrop **DARPA'98**
R2L KDD	Remote to Local Attack (R2L): This attack occurs when the attacker can send the packet over the network, but has no account on one of the network machines and accesses the system by checking the vulnerabilities of the system as the user of the system.	buffer_overflow, l oadmodule, multihop, perl, rootkit **DARPA'98**
U2R KDD	The user of Root Attack (U2R): In this attack, a bunch of attacks that an attacker begins by accessing a regular user account on the system (usually through password hearsay, dictionary attack, or social engineering)	ftp_write, guess_passwd, imap, phf, spy, warezclient, warezmaster **DARPA'98**

Fig. 10. The different attack applied to KDD99 in the database.

feature is superior to the Y feature. A correlation-based analysis method is used; this means different classifiers can be used with the selected subset. Furthermore, the methods require a relatively low amount of time. On the basis of the data presented in [45], these researchers chose features based on Pearson linear correlation. To figure out which features correlate, they examined the Pearson correlation. This feature selection method produces a symmetric correlation matrix. Fig. 11 shows the correlation between attribute 2 and other attributes. It can be seen that the correlation value can be negative. Therefore, by decreasing one feature the value of another feature will be increased. Fig. 11 also shows the maximum numerical value of the dependence of all features on other features. For example, as shown in Fig. 12, feature number 2 is highly correlated with feature numbers 27, 32, and 33. Therefore, the presence of these features does not affect the detection methods. Thus, it can prevent duplicate data. In this research, the correlation of each feature with other features is calculated and the maximum value is obtained from the absolute value of the correlation of one feature with other features.

Recognizing a principle to eliminate plugin features seems vital as it is needed to employ as a method under the title of the feature selection method. The findings of this study are analyzed based on the possible standard deviation of 0.5. On the other hand, in case an association between two variables moves further than 0.5, there would be an extra variable. So, it can be concluded that the objectives of this research are not affected by this extra variable. The further phase of the study includes the application of the

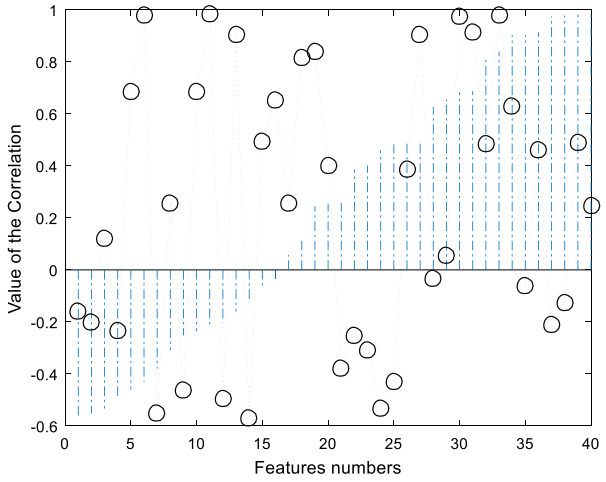


Fig. 11. Correlation between feature numbers 2 to other features. The horizontal axis shows the feature numbers and the vertical axis shows the correlation value.

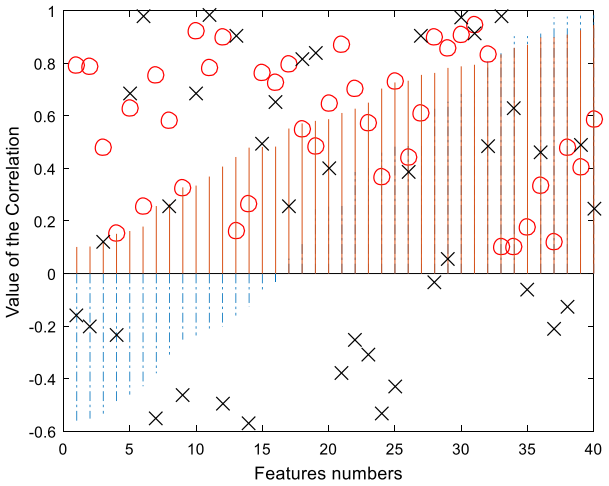


Fig. 12. Maximum numerical value of the dependence of all properties. The horizontal axis shows the properties and the vertical axis shows the maximum correlation value for each feature.

left 25 features when involved with the feature selection method at a threshold of 0.5. During this research phase, the researchers withdraw 14 features from the data set.

4.5. Reciprocal feature selection method

In the following, feature selections a method is used to measure the information in this research. These criteria consider the amount of information that can be obtained from a feature. For example, the X features in these methods have priority over the Y feature, if the information which is obtained from the X feature is greater than the information obtained from the Y feature. The method which is used in this research to select the feature of mutual information is obtained from [46,2].

First, the Joint Entropy formula is employed for every single feature to be compared with the target feature in the line of controlling its shared data. After computing the probability of the occurrence of each feature by connecting each feature to the target feature, the joint entropy is calculated. $I(X;Y)$ displays the data shared in both features. In the case of observing the adjacent association between X and Y, then $I(X;Y)$ shows a superior position.

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \Longrightarrow$$
$$I(X;Y) = -\sum_{y\in Y}\sum_{x\in X} p(x.y)log(\frac{p(x.y)}{p(x)p(y)}) \tag{10}$$

By performing this algorithm, some features may be irrelevant and some may contain duplicate information. This means that the information which obtained by this feature is available in other features and these extra features increase the computation time in creating the classification model. In addition, it can affect the accuracy of the classification which has been created. Fig. 13 shows

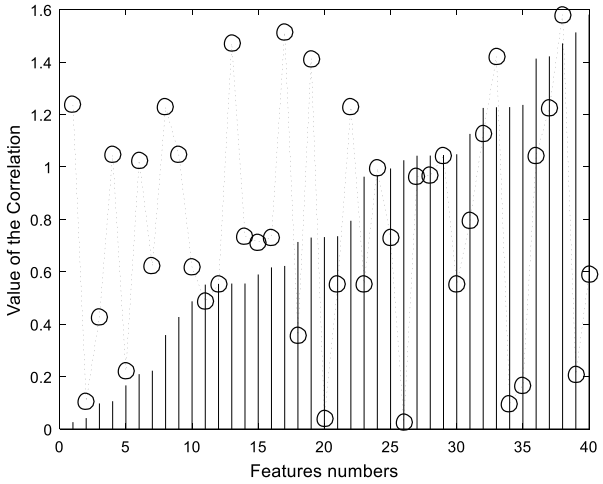


Fig. 13. Common information between feature selections with data class.

Table 3
Comparison of classification methods which is applied.

Method	Explanation
Neural Network	It takes a long time to network training data. For this reason, paying for this work is appropriate in most cases. Moreover, it is suitable for responding to changing circumstances.
CART	Used for discrete variables. A decision tree with binary divisions. The Gini Index is the criterion for selecting the appropriate variable [47].
Decision Tree	To build a classification tree with divisions. Multiple in each node is very convenient. This algorithm was designed for qualitative variables. The criterion for deciding on that is the entropy index [48].
Random Forest	The random tree forest produces many decisions. Large data sets are used. Provides a rough estimate of which variables are the most important [49].

the numerical value of the information shared between all the features selected in the previous step with the data class. For example, it can be seen in this figure that features 12 and 13 have almost nothing in common information with the target class. Therefore, the classes of using data are irrelevant to identify attacks.

Describing criteria related to the algorithm sounds vital to enable the researchers to access its concluding findings. Due to the threshold principles, it is certain to eliminate the divergent features to the target feature (data class). Since the thresholds address 0.01, the data related to a feature class should be more than 0.001, otherwise, it is considered irrelevant and should be omitted. By using such kind of threshold, four more features should be sent out of the consideration set. The next part is oriented to the process of utilizing the classification algorithms for the selected features and the final data class.

4.6. Actions classification methods

Following the application of multiple classification methods on the preprocessed data, the features were designated to benefit from their positive points. As shown in Table 3, different classification methods are compared, and a short description is provided for each.

Through the application of the Weka tool, the applied methods have been applied. Both the trend of preprocessing and conducting the feature selection methods was followed. Then, the researchers used the classification algorithms for the complete feature collection process and for the collection of the selected features at the start of the season, and the comparison of the findings was conducted. To validate the results, we used the 10 Fold Cross Validation method. In the following, we will explain the confusion matrix (Table 4) consequence from the application of different methods on the data with the validation criteria of the results.

When the features selection method is employed based on the kind of data, better precision is achieved (Fig. 14). Table 5 indicates the judgment over the precisions between methods according to the features selected and the other features minus features selection. When a test is conducted on the Fig. 15 diagram, an important growth relevant to the precision can be seen that is attained by using the methods of the features selection. Based on the findings of the research, the suggested process of the random forest classification method displays better precision than other procedures.

4.7. Comparison of other criteria for evaluating results

In this section, the results which are obtained from the various criteria are evaluated in order to consider the proposed method. The results which have been archived in this section are obtained by Weka software (Table 6).

Table 4
Confusion matrix of different methods.

Method	Confusion matrix					
		DoS	**Normal**	**Probe**	**r2l**	**u2r**
Neural Network	**DoS**	4993	4	2	1	0
	Normal	3	2425	0	0	4
	Probe	1	1	1518	0	0
	r2l	0	0	0	1000	0
	u2r	0	5	1	1	42
		DoS	**Normal**	**Probe**	**r2l**	**u2r**
Decision Tree	**DoS**	4992	4	3	1	0
	Normal	3	2414	2	9	4
	Probe	2	3	1515	0	0
	r2l	1	2	0	997	0
	u2r	1	3	2	2	41
		DoS	**Normal**	**Probe**	**r2l**	**u2r**
Random Forest	**DoS**	4997	1	1	1	0
	Normal	0	2428	2	0	2
	Probe	0	0	1516	2	2
	r2l	1	0	2	995	2
	u2r	0	4	1	0	44
		DoS	**Normal**	**Probe**	**r2l**	**u2r**
CART	**DoS**	4992	3	3	2	0
	Normal	3	2411	4	10	4
	Probe	2	3	1515	0	0
	r2l	1	2	0	997	0
	u2r	1	2	3	2	41

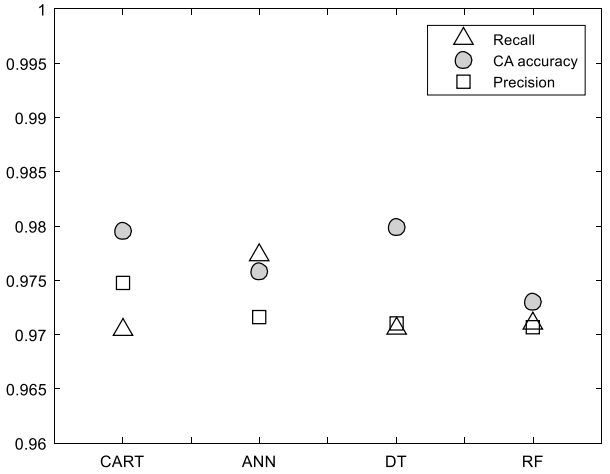


Fig. 14. Accuracy of different results of applied classification on data with the features selection method.

Table 5
Comparison of numerical values of accuracy obtained in classification methods.

Method	No feature selection	Proposed feature selection method	The method of selecting the similarity ratio attribute
Neural Network	99.53	99.55	99.54
CART	99.80	99.88	99.61
Decision Tree	99.54	99.58	99.4
Random Forest	99.66	99.65	99.68

5. Conclusion

In addition to firewalls and other intrusion equipment, other systems called Intrusion Detection Systems (IDS) are required to provide complete security to a computer system. Therefore, it can recognize and find a way to deal with if there is Intruder from the firewall. Intrusion detection systems can be classified into three aspects: method of detection, architecture, and response to an intrusion. Types of intrusion detection methods include detecting abnormal behavior and detecting abuse (signature-based detection). There are several types of intrusion detection systems architecture that can generally be divided into three categories: HIDS, NIDS, and DIDS. Apart from linear correlation and cross-information selection methods that were applied in the present

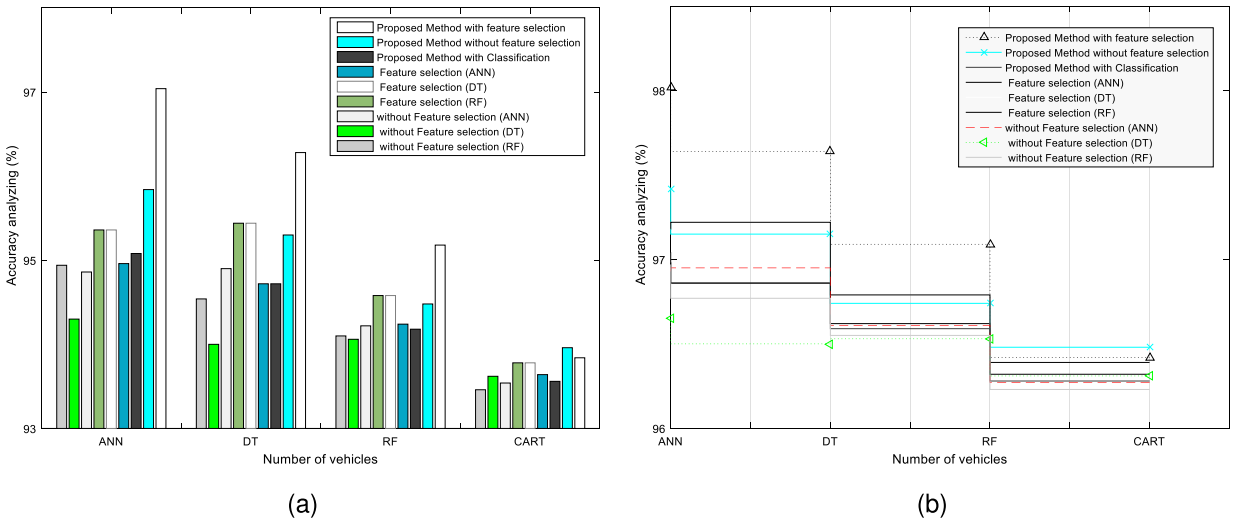


Fig. 15. Analyzing the accuracy obtained with and without feature selection in classification methods.

Table 6
Validation criteria with applied methods by feature selection.

Method	Random Forest	Decision Tree	Neural Network	CART
CA accuracy	98.3509	98.1807	98.523	98.7356
	98.8234	98.2177	99.0659	98.9668
	98.5389	98.2969	98.6277	98.6339
	98.9340	98.2427	98.8191	98.8019
Precision	0.9723	0.9799	0.9790	0.9745
	0.9696	0.9716	0.9836	0.9648
	0.9810	0.9727	0.9719	0.9778
	0.9874	0.9704	0.9819	0.9792
Recall	0.9756	0.9719	0.9850	0.9851
	0.9745	0.9760	0.9841	0.9870
	0.9760	0.9794	0.9864	0.9835
	0.9799	0.9785	0.9801	0.9807
EA classifier error	0.3429	0.4175	0.1932	0.4428
	0.3438	0.4136	0.3983	0.4810
	0.3491	0.4174	0.3870	0.4847
	0.3375	0.4162	0.2906	0.5487
DR Accuracy	0.9595	0.9574	0.9627	0.9612
	0.9531	0.9585	0.9647	0.9608
	0.9590	0.9547	0.9611	0.9600
	0.9593	0.9544	0.9641	0.9620
FAR false alarm rate	0.0044	0.0055	0.0033	0.0047
	0.0042	0.0057	0.0033	0.0045
	0.0044	0.0057	0.0032	0.0048
	0.0043	0.0056	0.0035	0.0046
Area Under Curve	99.7176	99.7892	99.7120	99.7892
	99.7182	99.7687	99.7821	99.7687
	99.7577	99.7300	99.7966	99.7300
	99.7931	99.7180	99.7031	99.7180
Model making time	77.8147	1.2724	0.7455	1.7257
	77.9575	1.2670	0.7437	1.7158
	77.4218	1.2346	0.7447	1.6838
	77.6787	1.2366	0.7571	1.7302

research, the researchers applied KDD99. In the final run, 21 features stayed in the database, and classification algorithms were also practiced. Then many algorithms were considered for the data, such as decision trees, random forests, and CART algorithms. Due to the capabilities of the methods, neural networks indicating 99.98% precision act with the highest efficiency. Through this study, researchers attempt to test the usage of two feature selection methods in foretelling risks in intrusion detection systems.

Data Balancing systems are considered a supported suggested method that the researchers suggest keeping because many accounts relevant to each type of attack seem diverse. Consequently, many accounts with each type of status look analogous. Furthermore, there can be a kind of interaction between the feature selection method and the INTERACT method to show the significance of a feature according to the association between the related features [50]. The researchers compared such methods to decide the most accurate consequences. If the information synthesis methods including Majority Voting are employed, the findings oriented to the categories can similarly be enhanced.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] N. Dutta, N. Jadav, S. Tanwar, H.K.D. Sarma, E. Pricop, Intrusion detection systems fundamentals, in: Cyber Security: Issues and Current Trends, Springer, 2022, pp. 101–127.
[2] A. Javadpour, S.K. Abharian, G. Wang, Feature selection and intrusion detection in cloud environment based on machine learning algorithms, in: 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC), IEEE, 2017, pp. 1417–1421.
[3] A. Javadpour, A.K. Sangaiah, F. Ja'fari, P. Pinto, H. Memarzadeh-Tehran, S. Rezaei, F. Saghafi, Toward a secure industrial wireless body area network focusing mac layer protocols: an analytical review, IEEE Trans. Ind. Inform. (2022).
[4] J.C.-W. Lin, K.-H. Yeh, Security and Privacy Techniques in IoT Environment, 2020, p. 1.
[5] Y. Yao, Research on computer database intrusion detection technology based on virtualization technology, in: 2021 IEEE 4th International Conference on Information Systems and Computer Aided Education (ICISCAE), IEEE, 2021, pp. 349–352.
[6] A.K. Sangaiah, A. Javadpour, F. Ja'fari, P. Pinto, H. Ahmadi, W. Zhang, Cl-mlsp: the design of a detection mechanism for sinkhole attacks in smart cities, Microprocess. Microsyst. 90 (2022) 104504.
[7] C. Vij, H. Saini, Intrusion detection systems: conceptual study and review, in: 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), IEEE, 2021, pp. 694–700.
[8] L.R. Suzuki, Smart cities iot: enablers and technology road map, in: Smart City Networks, Springer, 2017, pp. 167–190.
[9] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, M. Rajarajan, A survey of intrusion detection techniques in cloud, J. Netw. Comput. Appl. 36 (1) (2013) 42–57.
[10] A.K. Sangaiah, A. Javadpour, F. Ja'fari, P. Pinto, W. Zhang, S. Balasubramanian, A hybrid heuristics artificial intelligence feature selection for intrusion detection classifiers in cloud of things, Clust. Comput. 26 (1) (2023) 599–612.
[11] A. Javadpour, P. Pinto, F. Ja'fari, W. Zhang, Dmaidps: a distributed multi-agent intrusion detection and prevention system for cloud iot environments, Clust. Comput. 26 (1) (2023) 367–384.
[12] M. Ozkan-Okay, R. Samet, Ö. Aslan, D. Gupta, A comprehensive systematic literature review on intrusion detection systems, IEEE Access (2021).
[13] I.A. Khan, N. Moustafa, D. Pi, W. Haider, B. Li, A. Jolfaei, An enhanced multi-stage deep learning framework for detecting malicious activities from autonomous vehicles, IEEE Trans. Intell. Transp. Syst. (2021).
[14] K.P. Jadhav, M. Gangwar, Intrusion detection system and vulnerability identification using various machine learning algorithms, in: Proceedings of International Conference on Recent Trends in Computing, Springer, 2022, pp. 527–536.
[15] R. Panigrahi, S. Borah, A.K. Bhoi, M.F. Ijaz, M. Pramanik, Y. Kumar, R.H. Jhaveri, A consolidated decision tree-based intrusion detection system for binary and multiclass imbalanced datasets, Mathematics 9 (7) (2021) 751.
[16] S. Shao, P. Satam, S. Satam, K. Al-Awady, G. Ditzler, S. Hariri, C. Tunc, Multi-layer mapping of cyberspace for intrusion detection, in: 2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA), IEEE, 2021, pp. 1–8.
[17] M. Husnain, K. Hayat, E. Cambiaso, U.U. Fayyaz, M. Mongelli, H. Akram, S. Ghazanfar Abbas, G.A. Shah, Preventing mqtt vulnerabilities using iot-enabled intrusion detection system, Sensors 22 (2) (2022) 567.
[18] M.A. Pastore, M. Pastore, E. Dulaney, CompTIA Security+ Study Guide: Exam SY0-101, John Wiley & Sons, 2006.
[19] R. Di Pietro, L.V. Mancini, Intrusion Detection Systems, vol. 38, Springer Science & Business Media, 2008.
[20] U. Kumar, B.N. Gohil, A survey on intrusion detection systems for cloud computing environment, Int. J. Comput. Appl. 109 (1) (2015).
[21] A.D. Jasim, et al., A survey of intrusion detection using deep learning in Internet of things, Iraqi J. Comput. Sci. Math. 3 (1) (2022) 83–93.
[22] G.S. Lalotra, V. Kumar, A. Bhatt, T. Chen, M. Mahmud, iretads: an intelligent real-time anomaly detection system for cloud communications using temporal data summarization and neural network, Secur. Commun. Netw. 2022 (2022).
[23] A. Shaikh, P. Gupta, Real-time intrusion detection based on residual learning through resnet algorithm, Int. J. Syst. Assur. Eng. Manag. (2022) 1–15.
[24] P.R. Maidamwar, M.M. Bartere, P.P. Lokulwar, Implementation of network intrusion detection system using artificial intelligence: survey, in: Proceedings of the 2nd International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications, Springer, 2022, pp. 185–198.
[25] P.V. Astillo, D.G. Duguma, H. Park, J. Kim, B. Kim, I. You, Federated intelligence of anomaly detection agent in iotmd-enabled diabetes management control system, Future Gener. Comput. Syst. 128 (2022) 395–405.
[26] P. Dixit, P. Bhattacharya, S. Tanwar, R. Gupta, Anomaly detection in autonomous electric vehicles using ai techniques: a comprehensive survey, Expert Syst. (2022).
[27] M.B. Pranto, M.H.A. Ratul, M.M. Rahman, I.J. Diya, Z.-B. Zahir, Performance of machine learning techniques in anomaly detection with basic feature selection strategy-a network intrusion detection system, J. Adv. Inf. Technol. 13 (1) (2022).
[28] S. Naaz, K. Mir, I.R. Ansari, Enhancement of network security through intrusion detection, in: Soft Computing for Security Applications, Springer, 2022, pp. 517–527.
[29] R.A. Disha, S. Waheed, Performance analysis of machine learning models for intrusion detection system using Gini impurity-based weighted random forest (giwrf) feature selection technique, Cybersecurity 5 (1) (2022) 1–22.
[30] P. Himthani, G.P. Dubey, Application of machine learning techniques in intrusion detection systems: a systematic review, in: Proceedings of Third International Conference on Sustainable Computing, Springer, 2022, pp. 97–105.

[31] Z. Li, W. Sun, L. Wang, A neural network based distributed intrusion detection system on cloud platform, in: 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, vol. 1, IEEE, 2012, pp. 75–79.
[32] M. Zekri, S. El Kafhali, N. Aboutabit, Y. Saadi, Ddos attack detection using machine learning techniques in cloud computing environments, in: 2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), IEEE, 2017, pp. 1–7.
[33] S. Sahil Ahmed, M. Kankar, B. Rudra, Intrusion detection techniques for detection of cyber attacks, in: Computer Communication, Networking and IoT, Springer, 2021, pp. 127–134.
[34] M. Thangavel, B. Jeyapriya, K. Suriya, Detection of worms over cloud environment: a literature survey, in: Research Anthology on Architectures, Frameworks, and Integration Strategies for Distributed and Cloud Computing, 2021, pp. 2472–2495.
[35] P. Singh, A. Kaur, R.S. Batth, S. Kaur, G. Gianini, Multi-disease big data analysis using beetle swarm optimization and an adaptive neuro-fuzzy inference system, Neural Comput. Appl. 33 (16) (2021) 10403–10414.
[36] D. Parfenov, I. Bolodurina, L. Zabrodina, A. Zhigalov, Development of a solution for identifying network attacks based on adaptive neuro-fuzzy networks anfis, in: 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), IEEE, 2021, pp. 0491–0495.
[37] N. Koryshev, I. Hodashinsky, A. Shelupanov, Building a fuzzy classifier based on whale optimization algorithm to detect network intrusions, Symmetry 13 (7) (2021) 1211.
[38] M.T. Ashraf, K. Dey, S. Mishra, M.T. Rahman, Extracting rules from autonomous-vehicle-involved crashes by applying decision tree and association rule methods, Transp. Res. Rec. 2675 (11) (2021) 522–533.
[39] J.D. Cabelin, P.V. Alpano, J.R. Pedrasa, Svm-based detection of false data injection in intelligent transportation system, in: 2021 International Conference on Information Networking (ICOIN), IEEE, 2021, pp. 279–284.
[40] D. Xuan, H. Hu, B. Wang, B. Liu, Intrusion detection system based on rf-svm model optimized with feature selection, in: 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), IEEE, 2021, pp. 1–5.
[41] M. Mohammadi, T.A. Rashid, S.H.T. Karim, A.H.M. Aldalwie, Q.T. Tho, M. Bidaki, A.M. Rahmani, M. Hosseinzadeh, A comprehensive survey and taxonomy of the svm-based intrusion detection systems, J. Netw. Comput. Appl. 178 (2021) 102983.
[42] J. Gu, S. Lu, An effective intrusion detection approach using svm with naïve Bayes feature embedding, Comput. Secur. 103 (2021) 102158.
[43] P. Parkar, A. Bilimoria, A survey on cyber security ids using ml methods, in: 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE, 2021, pp. 352–360.
[44] A. Saber, M. Abbas, B. Fergani, Two-dimensional intrusion detection system: a new feature selection technique, in: 2020 2nd International Workshop on Human-Centric Smart Environments for Health and Well-Being (IHSH), IEEE, 2021, pp. 69–74.
[45] H.F. Eid, A.E. Hassanien, T.-h. Kim, S. Banerjee, Linear correlation-based feature selection for network intrusion detection model, in: International Conference on Security of Information and Communication Networks, Springer, 2013, pp. 240–248.
[46] J. Song, Z. Zhu, P. Scully, C.J. Price, Modified mutual information-based feature selection for intrusion detection systems in decision tree learning, J. Comput. 9 (7) (2014) 1542–1546.
[47] L. Breiman, J.H. Friedman, R.A. Olshen, C.J. Stone, Classification and Regression Trees, Routledge, 2017.
[48] J.R. Quinlan, Induction of decision trees, Mach. Learn. 1 (1) (1986) 81–106.
[49] A. Liaw, M. Wiener, et al., Classification and regression by randomforest, R News 2 (3) (2002) 18–22.
[50] Z. Zhao, H. Liu, Searching for interacting features in subset selection, Intell. Data Anal. 13 (2) (2009) 207–228.