Novel Approach of Intrusion Detection Classification Deeplearning Using SVM

Pritesh Nagar, Hemant Kumar Menaria and Manish Tiwari

Abstract The main objective of intrusion detection systems (IDS) is to discover the dynamic and the virulent form of network traffic that simply changes according to the characteristics of the network. The IDS methodology represents a prominent developing area in the field of computer network technology and its security. Different form of IDS has been developed working on distinctive approaches. One such kind of approach where it is used is the machine learning mechanism. In the proposed methodology, an experiment is applied on the data set named as KDD-99, including its subclasses such as denial of service (DOS), other types of attacks and the class without any form of attack. Depending upon the machine learning algorithms various distinct forms of IDS have been developed which further checks the optimization-based potential features in connection with the neural network classifier for the various forms of IDS-based attacks. This approach provides a comparative study between the ANN and the optimizer-based ANN technology. The experimental analysis shows the convolution neural network with SVM show effective analysis providing accurate forms of IDS, thereby improving its detection based on individual class along with maintaining its results fundamentally.

Keywords Intrusion detection system · Denial of service · Artificial neural network

1 Introduction

In the present scenario, the use of Internet is growing at a large pace with highly developed and emerging forms of ever-growing network and its connectivity, but the use of Internet poses a great threat to cyber security. In order to maintain the high level of security, there is an important need to overcome the cyber threats posing problems to various organizations, companies, and firms. One of the major challenges among the cyber security is to maintain the integrity of the intrusion detection system (IDS),

P. Nagar (✉) · H. K. Menaria · M. Tiwari
Geetanjali Institute of Technical Studies, Udaipur, India
e-mail: priteshnagar1983@gmail.com

A. K. Luhach et al. (eds.), *First International Conference on Sustainable Technologies for Computational Intelligence*, Advances in Intelligent Systems and Computing 1045,
https://doi.org/10.1007/978-981-15-0029-9_29

thereby protecting it from major forms of attacks and to conquer the various form of risks of the intruded system [1]. The main function of the IDS is to identify a more precise form of intrusion. The illegal hackers of the security have found a large number of ways to break the security of the system whether it is a cloud network or the wireless-based network. Many researches have been performed by the technologists to curb the security threats from distinct forms of intrusions done to the cloud computing systems and the wireless system. So, the main objective of IDS is to protect the information whether it is governmental, public or private entity [2]. The use of IDS is mainly required in detecting the false and the poor detection rates. Whenever an attack is observed by the system or a harmful activity is done to the system, it automatically generates an alarm resulting in a false-positive alarm [1]. The research mainly focusses upon the enhanced capabilities of the intrusion detecting system and thereby reduces the occurrence of the false type alarms.

1.1 Intrusion Detection System

The term intrusion detection system, i.e. IDS is a developing area having various forms of application in the computer technology and its inter-linked networks. Some of the important forms of IDS which identifies the traffic-data and its changing activities by using an algorithm (single class). But some of the single-class algorithms are not able to fetch a good detection rate and does not provide a low occurrence of the false alarms. So, the working methodology is based on using an intelligent hybrid technology comprising of different technology comprising of different sets of classifiers, which are helpful in enhancing the productivity of the system in an intelligent way. In IDS intelligent based mechanism, various forms of data-mining approaches such as genetic algorithms, classification, decision trees, artificial neural networks, and clustering have been used in the mining of data for the development in the field of IDS also the SVM, i.e. support vector machines technology provides the best technique for classification of the clean as well as the intrusive form of data [3]. The SVM technology deals with high-class accuracy in detecting the data intrusions. To avoid redundancy, inadequacy and the noisy data forms, there is an urgent need to go for selection, i.e. feature-based [4, 5]. The basic operation of an intruder is to search the faulty operative conditions in the network or the systems. So, an intruder helps to find out the best-optimized solutions to identify the intrusions in the data. The main requirement of the IDS is not only to encounter the intruders in the data path, but also to supervise the intruders of the data. The most important security aspects of an intrusion detection system consist of maintaining the following conditions:

- *Confidentiality*: Only an authorized user can detect the system.
- *Availability*: Here, the computer technology provides various forms of resources and the access to the legal users of the system without disturbing the working operation of the system.
- Integrity: The information must be protected from any kind of malicious act.

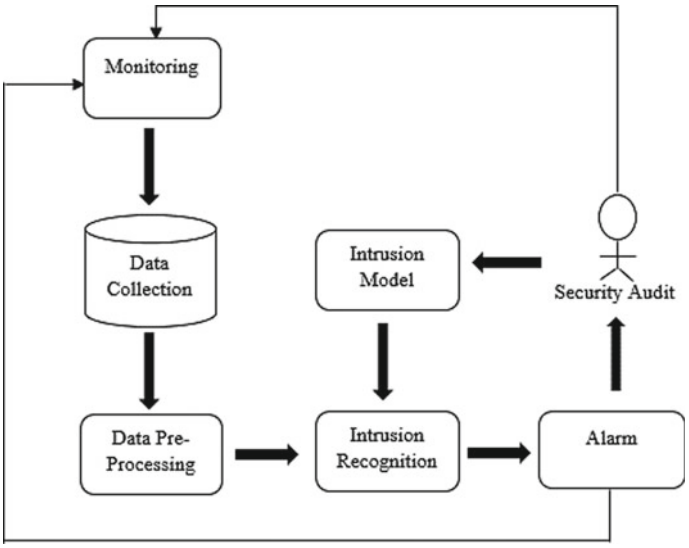

Fig. 1 Basic structure of IDS

The process of intrusion detection system popularly started its operation in 1990. The process of IDS acts as a security alarm where it provides an alarming state in case of any kind of violation in the form of messages, emails or audio-video [6] (Fig. 1).

The IDS is designed as a tool for securing the system from various types of malwares or intrusions interrupting the working if the system [2]. The main function of IDS is to inspect the various types of attacks done on the system, thereby providing a defence mechanism to fight against these attacks in such a way that it also provides information about the intrusions. So, IDS provides a mechanism that deals with the safety of current network security system [7].

1.2 IDS: Architecture

The architecture of IDS comprises of its unique core element, i.e. sensor popularly known as the analyzing engine to pin-point the intrusions occurring in the system. The sensor consists of a mechanism that helps in detecting the intrusions. In Fig. 2, the sensor gets the data (raw) from the given sources as shown which consists of the audit trails, knowledge-based data, and syslog. The 'syslog' includes the authority to the particular system or the system file configuration [7].

The sensor consists of a component known as event generator which performs the data collection shown in Fig. 2. It detects the way of collecting the data. The event generator consists of network, operating system, and the network applications where

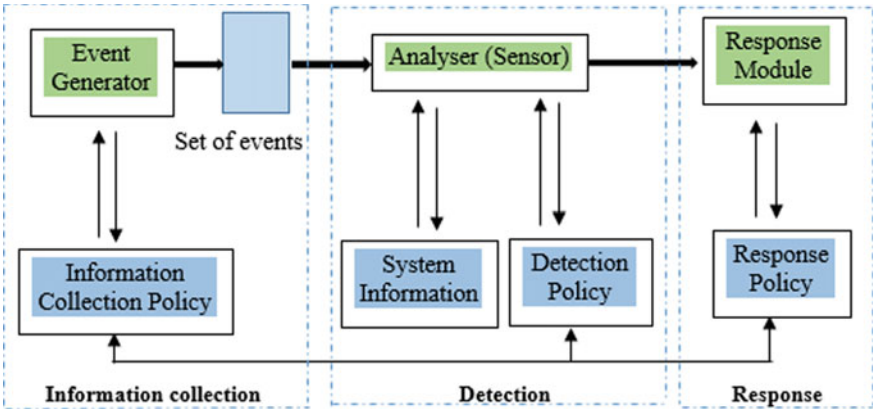

Fig. 2 IDS components

it generates a set of events including audit (log) of the system or the packets of the network. This form of set events also involves the policy of information collection, i.e. in or out of the system. Sometimes, it is not necessary to store the data as it reaches simply to the analyser. So, basically, the key role of the sensor is to extract or filter the data and remove the unwanted form of the data that is achieved from the event data set system [6, 8]. Additionally, the database holds the configurational parameters of IDS that includes its mode of communication methods based on the response module. The sensor itself contains its own data observing all the historical multiplex forms of intrusions. Practically, the IDS may follow a structure based on an 'agent' principle where small modules (autonomous) are designed on 'per-host' basis approach.

The agent mainly monitors and filters the activities scheduled within the area, i.e. fully protected and further starting its initial analysis by undertaking a response action [3]. When a suspicious act or event is detected, an agent issues an alarm. These can be shifted or cloned on another system. The system further may include the transceivers monitoring all the operations effected by agents of another host, i.e. specific. The results fetched by the transceivers are provided to a single unique monitor where the monitor can coordinate the distributed form of information. In addition, some filters are used for aggregation and the selection purpose [9, 10].

1.3 IDS: Classification and Types

There are various categories of IDS based on structure or detection. The IDS are classified based on characteristics as represented in Fig. 3.

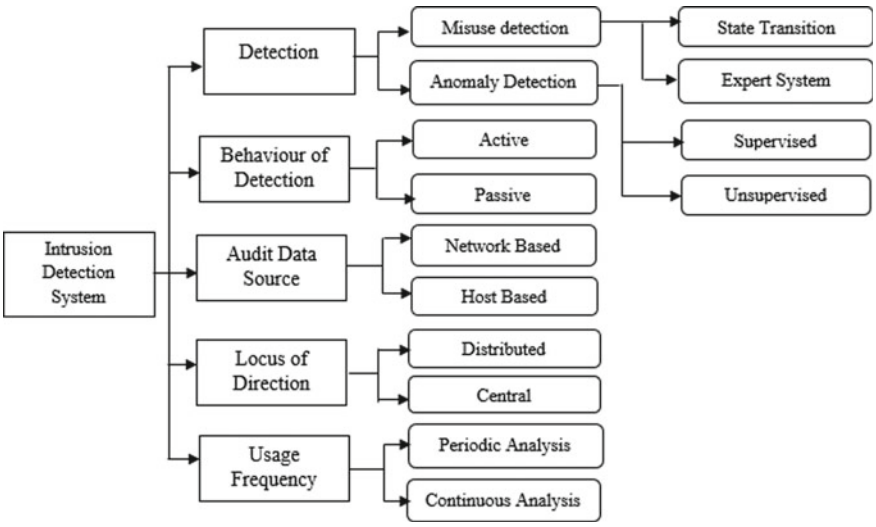

Fig. 3 Classification of IDS based on its characteristics

1.3.1 Based on Structure

The process of IDS is divided into three of its important categories based on its framework. These are host-based IDS, application-based IDS, and network-based IDS.

1. *Host-based intrusion detection system [HIDS]*: The type of detection that is placed in the computer server represents the host of the system usually called as HIDS. As the name suggests a mechanism that helps in analyzing the stored and the system files and further tells about the changes or the deletions done by the attacker in the system files. The HIDS simply detects the part, i.e. not detected by the NIDS mechanism. These are more liable to the attacks that are direct in nature and are inclined to attacks based on DOS, i.e. denial of service.
2. *Application-based IDS*: The application-based IDS is another development of HIDS, which monitors the different types of events such as the inspection of the files, checking the abnormal functions like exceeded permission, void-file execution, etc. It helps in analyzing the communication between the user and the application and monitors the traffic of the network, i.e. encrypted [11].
3. *Network-based intrusion detection system [NIDS]*: The Network-based IDS represents a passive network analyzing the traffic related to the network and for finding out the evidence of various forms of attacks. When a NIDS detects an attack, it provides an instant report to the administrator. It basically checks the types of attack that are incoming and outgoing networks and is usually placed inside the router. But the NIDS is unable to find out the encrypted source of information and is not able to distinguish some forms of attacks. There is no effect of system-failure over the NIDS. The main function after the installation

process is to identify and match the signatures present in the database with the attacking form of signatures.

2 Related Work

This section of literature survey represents the most important section of the thesis. The research study includes the extractions of various articles, books, journals, and research papers from various distinct publications at the national and the international levels. Modi et al. [7] conducted a survey on different intrusions that affected the integrity of cloud-resources, confidentiality, availability, and the services linked. The proposals of subsuming the intrusion prevention systems (IPS) and intrusion detection systems (IDS) in cloud technology are examined. The researcher's recommended the positioning of IDS/IPS in clouded environment to acquire the needed security in the next generation future-based network developments. Kamarudin et al. [9] proposed their study on technology of network security that has become a supreme method for the protection of information or the data. With the excessive growth of Internet technology, various forms of attack cases are observed in a day-to-day life. It includes performance analysis based on machine learning algorithm known as decision tree (J48) where a comparison has been done with two of the other machine learning algorithms named as the neural networks (NN) and the support vector machines (SVM's). These algorithms were tested on the strategy of false alarm rate, detection rate, accuracy, and accuracy of four classes of attacks. From the experimental analysis, it was observed that the decision tree (J48) algorithm performed well as compared to the other two machine learning algorithms. Elshoush et al. [1] focused on proper prevention of attacks that were linked to the computer-based systems. As the motive of complete prevention of attacks is not possible, so the process of using the intrusion detection systems (IDSs) play a crucial role to overcome the harm that is done to the operating systems. Two most important formsof methods based on intrusion detection were used, the first one was misuse-based detection and the second was the anomaly based detection. A CIIDS, i.e. collaborative intelligent intrusion detection system was proposed to examine both the methods, as the individually obtained results from both the methods resulted in less form of accuracy. Specifically, there are two major challenges in CIIDSs research strategy. Both of them were reviewed and highlighted. The two challenges were the architecture of CIIDSs and alert-correlation algorithms. Further, it concluded, the occasion for the integrated-solution to large-scale CIIDS. Mohammed and Sulaiman [3] conducted a study on using smart and intelligent form of data-mining methods in order to observe the intrusion occurring in the local type of networks. This paper suggested an improved strategy IDS that combines the expert systems, the processes of data mining as carried out in WEKA. The classification generally consists of a principle based on detection as well as it includes some of the conditions of WEKA such as data-mining open-source processes. The combined methodology gives an improved

performance of IDS-based systems and helps to maintain the detection in its more effective form. The result was based on evaluating a new design produced a better form of detection based on efficiency. So, the study presented a good approach to analyse the experiments on behalf of intrusion detection. Vinchurkar et al. [8] conducted a research on intrusion detection systems that consisted of high-level security of networks, and thus provides the system dealing with security of network and the intrusion-based attacks. The ideal features of IDS include a monitoring activity of network and the threats. The intrusion detection system is generally classified on the basis of the model and the data-source. But some of IDS techniques are more challenging in nature. The anomaly based IDS can be detected easily using various anomaly detection techniques. The process of dimension reduction is based on the analysis of principle component. The problem of construction classifier can be identified using a support vector machine methodology. Nadiammai et al. [6] focused upon the security issue of the networks and various developments in applications running on distinct platforms capturing an attention towards security of the network. This type of paradigm exploited the vulnerabilities of security that are technically difficult and expensive to solve. Hence, intrusion is used as a key to compromise the integrity, availability, and confidentiality of a computer resource. Four issues such as classification of data, high-level of human interaction, lack of labelled data, and effectiveness of distributed denial of service attack are being solved using the proposed algorithms like EDADT algorithm, hybrid IDS model, semi-supervised approach and varying HOPERAA algorithm, respectively. Our proposed algorithm has been tested using KDD cup data set. All the proposed algorithm shows better accuracy and reduced false alarm rate when compared with existing algorithms. Agrawal et al. [4] worked on the need of the present world dealing with huge amounts of data, i.e. transferred and stored from location or another. When the data gets transferred or is stored somewhere then it gets exposed to many forms of attack. However, many types of techniques and the detection mechanism have been developed to overcome the problem of data risk. Thus, to examine the data and to identify the kind of attack done on the data various mining techniques of data have emerged to make it free from any kind of loss related activity. The process of anomaly detection uses mining techniques of data to recognize the hidden behaviour inside the whole set of data, which might increase the chance of being attacked in an easy way. The use of hybrid-based approaches has also been made to judge the form of attacks whether known or unknown in nature. This research has reviewed data-mining techniques for anomaly detection to provide better understanding among the existing techniques that may help the interested researchers to work in future. Jabez et al. [12] proposed a study based on intrusion detection system (IDS) that presents an application of a software monitoring the activities of the system network generating reports to the management system. The main objective of this study was based on IDS detection and the prevention systems (IDPS). So, this work proposed a new strategy known as outlier-detection which used a data set measured by the neighbourhood outlier factor (NOF). Here, a model, i.e. trained consists of large data sets with storage environment of distributed type to improve the IDS-based performance of the system. The experimental analysis proved that the proposed strategy detects the malicious

content in a very effective way. Jabbar et al. [5] proposed the research based on the intrusion detection system to notify and identify the type of activities or normal users or the hackers performing malicious operations. In this paper, a model has been designed for intrusion detection system (IDS) using a classifier based on random forest, where the random forest (RF) denoted an ensemble classifier and that performed very well as compared to the other classifiers that worked traditionally for an effective classification of different forms of attacks. Gupta et al. [2] proposed work on IDS to pin-point the harmful malicious attacking activities done to the system. But this kind of framework carried a disadvantage of the number of false-positive and alert rates, which resulted in decreased proficiency of the IDS systems. This research has complied in many other researches and provides a single-metric technique to the false-positive alarms in the process of IDS which would further help the future researchers to extract and gain the knowledge to propose the further studies. He et al. [11] proposed the method of fuzziness based on the technique of instance selection for a huge amount of data sets in order to increase the supervised learning algorithm-based efficiency. It did so by improving the design shortcomings of intrusion detection system (IDS). The methodology proposed was dependent over a new type of single-layer feed-forward neural network (SLFN) known as random weight neural network (RWNN). Siddiqui and Farooqui [10] proposed a work using the IDS tool for anomaly detection that provides network security to the system. The IDS represents a method to detect the processes of cyber-attacks and this process of detection is based on the amount of distinct forms of intrusive activities occurring in the operation of the system as the detection of an intrusion denotes a very complicated process. So, this paper conducted a study based on classifier named cascaded support vector or it might be called as an improved version of ensemble classifier using a function, i.e. kernel function. This kernel function represents a Gaussian function. A neural network technique has been used for collecting its features based on different and distinct forms of attacks and this algorithm is more effective than the earlier method used. Wang et al. [13] proposed a methodology that focused on the fact that the security of the network has been increased at a very large pace for all the organizations, firms, and the most important is the security of an individual. The main aim was to obtain high-quality improvement in detection for the trained data set. As the ratio of marginal density denotes a powerful classifier, i.e. univariate in its nature, the study adopted for the obtaining the results is based on framing an IDS based on SVM method entailing its augmented features. Uniquely, a method has been implemented based on logarithmic values of the ratios of the marginal density in order to obtain a good quality of its transformed features, which improved the rate of detection based on SVM model. The set of data named NSL-KDD is basically used for the proposed method and the experimental results showed that the results are far much better than the existing forms or methods specifically targeting the rate of accuracy, its training speed, and the false alarm rate.

3 The Proposed Method

In this section, we discussed the proposed approach and the methodology used to achieve the results.

3.1 Proposed Technique

The proposed technique involves the following steps:

The author has proposed a hybrid model which consists of SVM, i.e. support vector machine combined different classification-algorithm to mitigate the rates of the false-positive alarms. To obtain the pre-thesis objective, a methodology has been proposed which is further divided into three types of phases.

Phase 1: Collection and preprocessing

- Data set collection.
- Extraction of features through a data, i.e.'tcpdump'.
- Converting the obtained features into binary representation.
- Preparation of the input for its classification.

Phase 2: Classification

- To find the best classifier from the available classifier.
- To test and train the tool of classification by the data set-partitioning process.

Phase 3: Result analysis

- To compare the obtained results with their existing work.

The proposed working methodology is designed as in Fig. 4.

3.2 Proposed Flowchart

The proposed steps of flow chart are given as below:

1. *KDD-99 Data set*: This is a type of data set used for the (Third International Knowledge Discovery and Data Mining Tools) competition, held in conjunction with KDD-99 (The Fifth International Conference on Knowledge Discovery and Data Mining). The main task was to build a network based on intrusion detection and to predict a model, i.e. capable of discriminating a good or a bad form of data set. This form of data set maintains a standard including a wide variety of network-based intrusions.
2. *Label features*: A label helps in providing a complete information regarding the set of data.

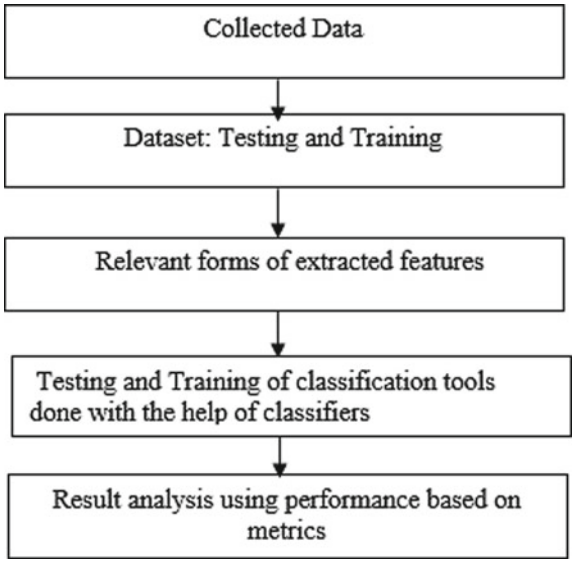

Fig. 4 Proposed methodology

3. *Input in PSO*: Each of the particles has its velocity and position to search for better solution. So, the velocity and position are the inputs used in PSO.
4. *Initialize particles*: The PSO-based technique is initialized with a population of random solution.
5. *Update fitness function*: It helps in judging the individual solutions based on how well they can handle the problem.
6. *Optimize objective form*: Here, the objective is optimized.
7. *Initialize chromosomes*: The process is initialized by building a population of chromosomes which is a set of possible solutions to the optimization problem.
8. *Check the convergence*: These type of methods helps in testing the conditional-convergence, absolute-convergence, interval of convergence or divergence of an infinite series.
9. *Cross over*: A point or place of crossing from one side to the other.
10. *Roulette selection*: It is a method used in genetic algorithms for selection of potentially useful solutions for the purpose of recombination.
11. *Optimize features*: This type of method achieves the best designing technique.
12. *Neural networks:* It represents biologically inspired information processing system.
13. *Test model*: It performs a system or software system.
14. *Precision and recall accuracy:* The precision is a good measure that determines the cost of false-positive is high (Fig. 5).

C. *Algorithm*

Following are the algorithms that are used in the proposed work.

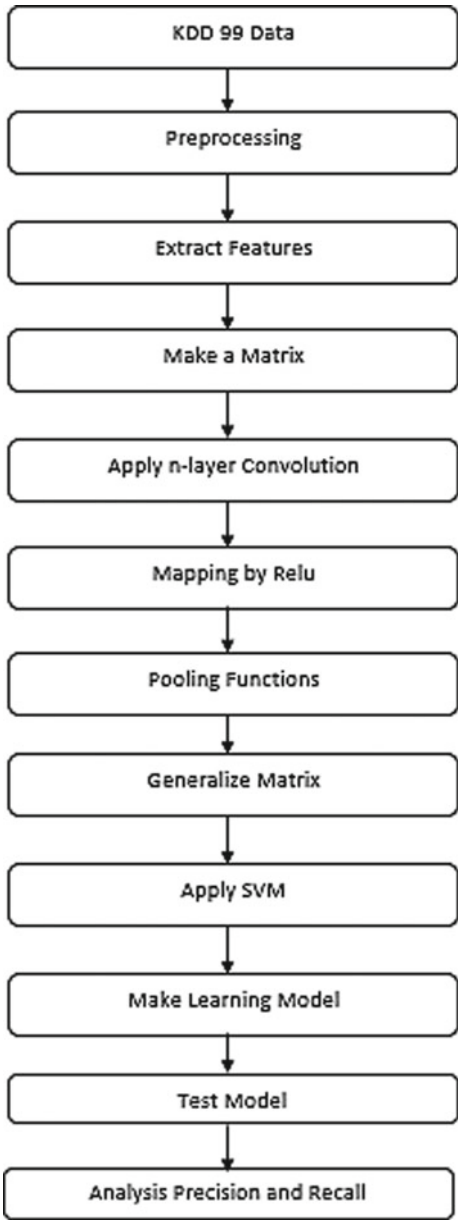

Fig. 5 Proposed flowchart

Algorithm

Step 1: Input bugs in the form of KDD-99l data.

Step 2: Preprocessing of data test to remove the noisy data.

Step 3: Extract the bigrams and make the matrix.

Step 4: Apply n-layer convolution and mapping by Relu.

Step 5: Pooling of function and generalize the matrix.

Step 6: Apply the SVM

With optimization model $min_{\omega,\xi,Q} P(\omega, \xi)$ we describe the model of SVM classification.

$$min_{\omega,\xi,Q} P(\omega, \xi_r) = \frac{1}{2}\omega^g \omega + \frac{1}{2}\gamma \sum_{r=1}^{n} \xi_r^2$$

$$s_r[\omega^t \phi(u_r) + Q = 1 - \xi_r, r = 1, 2, \ldots, n$$

$$\xi = (\xi_1, \xi_2, \ldots, \xi_n)$$

Where

$\xi_r \leftarrow$ Slack variable

Q $\leftarrow$ Offset

$\omega \leftarrow$ Support vector

$\gamma \leftarrow$ Classification parameter for balancing the model complexity and fitness error.

Then, describing the classification decision function:

$$F(z_r) = sgn\left(\sum_{r=1}^{n} \alpha_r s_r L(q, q_r) + Q\right)$$

Step 7: Make learning and testing model.

Step 8: Analyze the precision and recall.

4 Result Analysis

4.1 Experimental Setup

(a) *Data set description*: The experiments as discussed above are mainly executed with the help of KDD-99 data set having around 41 sets of feature sets. Such type of features is mainly used for the process of optimization and further it involves the mechanism of learning and currently, these are basically used for analyzing in terms of various kinds of attacks. This work is comprised of evaluating the rate of accuracy in IDS methodology. In the part of analysis, the data is taken

based on the number of intrusions in the process. The attacks are divided into four of its classes: (1) Probe, (2) Dos, (3) U2R, and (4) R2L. In our methodology, we use three of the following categories: (1) other attack which mainly consists of probe, U2R and R2L (2) Normal attacks, and (3) DoS-attack. Further, the evaluation of precision, accuracy, *F*-measure, and recall is done in several cases.

Figure 6 shows the analysis in respect of precision, accuracy, *f*-measure, recall, etc. This figure involves the demonstration of efficiency analysis from all four types of algorithm. Analysis demonstrates that ANN with both SPO and GA give better result in terms of all the four parameters, i.e. precision, accuracy, recall, and *f*-measure. In Fig. 7, represents the parameters investigation of various kind of classifiers and the proposed approach. In investigation parameters like exactness, review, precision, and f-measure fluctuate as indicated by classifier yet one examination clear about proposed methodology (ANN with GA in neural system) demonstrate huge enhance all parameters. In the event that examination just proposed methodology, review demonstrate huge enhancement then different parameters so it will clear sign of decreasing false negative rate so assaults distinguishing proof is successful in proposed approach in view of enhance weight given by ANN_GA approach.

Figures 7 and 8 parameters investigation of various classifier and proposed approach. In investigation parameters like exactness, review, precision, and f-measure fluctuate as indicated by classifier yet one examination clear about proposed approach (PSO with GA in neural system) demonstrate huge enhance all parameters. In the proposed methodology review demonstrate huge enhancement then different parameters so it will clear sign of decreasing false negative rate so assaults distinguishing proof

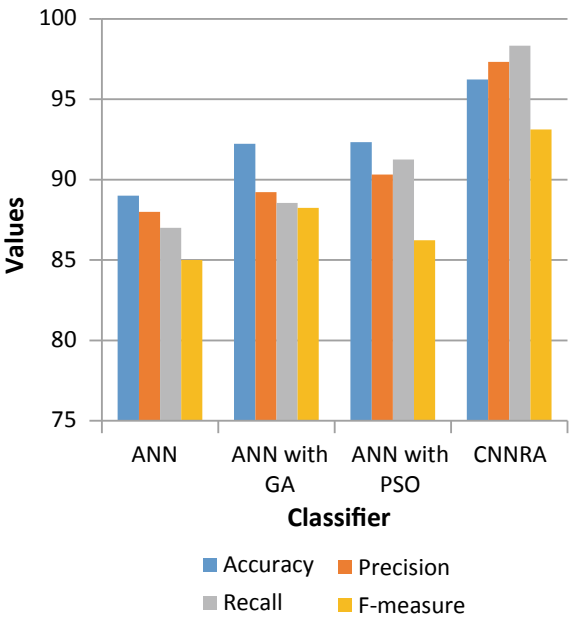

Fig. 6 Simulated graph of comparison parameters

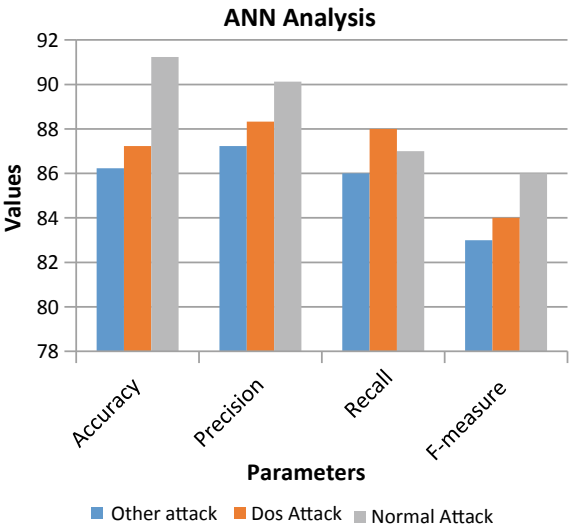

Fig. 7 Analysis of ANN

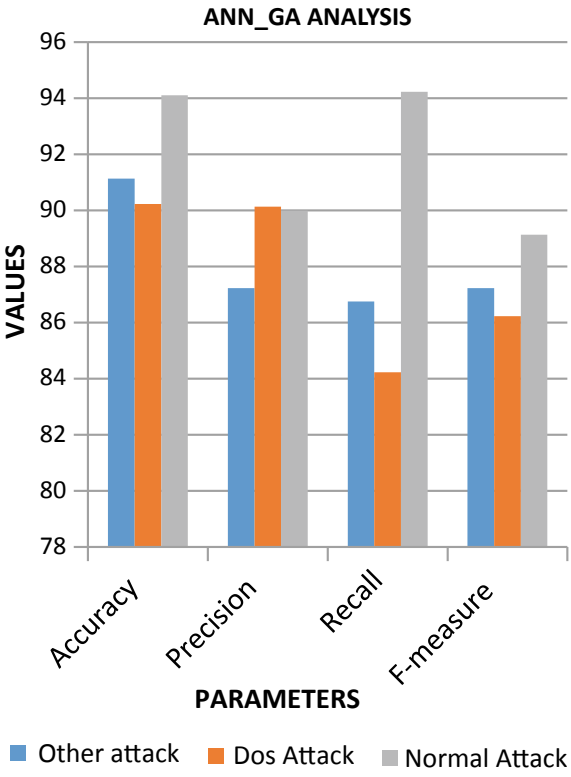

Fig. 8 Analysis with ANN and ANN_GA

is successful in proposed approach in view of enhance weight given by PSO_GA approach CNNRA.

In Fig. 8, profundity investigation of every one of the three classes in ANN and ANN_GA. In this examination, we endeavour to indicate what the criticalness of our methodology is. This exchange we precede in perception (3) moreover. So first point which examination by typical class n which no assault working and in the two cases ANN and ANN with GA perform well contrast with other parameter like exactness, review, and f-measure yet ANN_GA still preferable precision over ANN, so include weighted by enhancement by one way or another perform in view of decreasing covering data learning. On the off-chance that examination through DOS assaults it additionally indicate higher exactness in ANN with GA. So we can close feature advance weight is better methodology so by what means can enhance improvement these perception talk about in next standard (Fig. 9).

At last from the whole analysis it can be concluded that algorithm CNNRA gives better result for all the attacks we examined in our work. In Fig. 10, examination proceed from perception (2) and attempt to discovering centrality of streamlining enhancement impact on various classes' recognition by characterization. On the off-chance that investigation the both chart demonstrate the compelling review; however, for ordinary class so decrease the false-positive rate this enhancement occurring with all classes like DOS assault and different assaults yet the viable outcome appear in other assault which increment fundamentally in proposed approach. So PSO streamlining is great, however, PSO with GA more enhance in other assault and ordinary class.

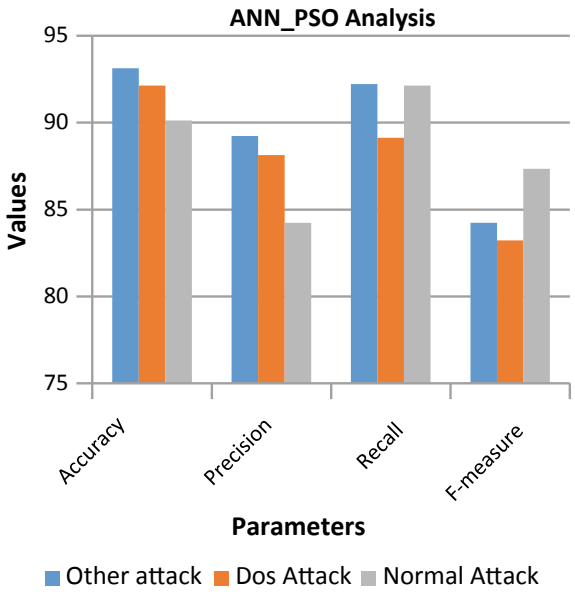

Fig. 9 Analysis of ANN_PSO

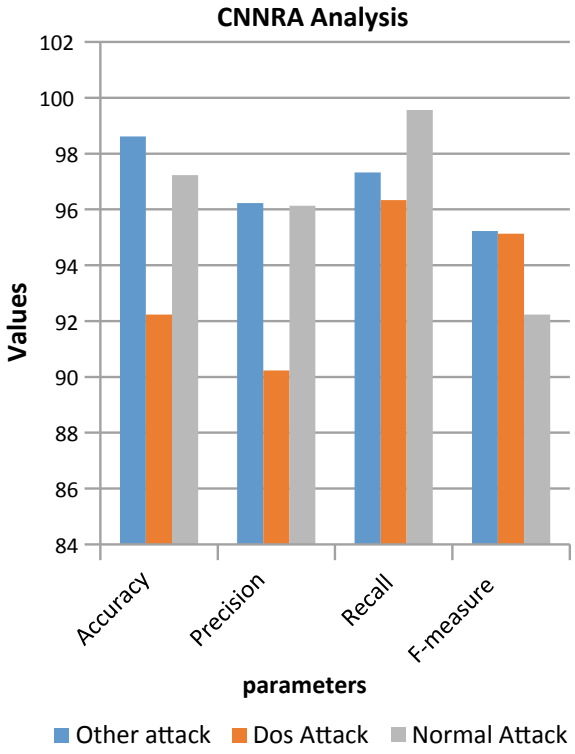

Fig. 10 Analysis with ANN_PSO and CNNRA

5 Conclusion

The present scenario experiences various forms of developments and a huge growth in advanced processing technologies consisting of connectivity among different networks, but methodology is vulnerable by the activities of the intruders or the attackers of the system. These specifically smart attackers interrupt the operation with new and fascinating methods of data-breaching among large networks. Though there are various forms of available intrusion of intrusion detection systems that can detect the intrusions occurring in the network, i.e. based on the false-positive detection rate and the alert rates, but with the detection rate of intrusions, they also have a high false-positive rate resulting in an adequate system comprising of low accuracy level of the system and are generally more prone to different kinds of attack. This usually helps the intruder to enter into the system and perform a pre-planned attack. So, this pre-thesis will propose a hybrid approach to reduce the false-positive alarms. The experimental analysis consists of a specified particular form of data set and the process of feature-based selection will be done to improve the analysis. These features obtained will be used for the classification-tool training and testing the performance of the system. Finally, the result obtained will be compared with the results that already exist.

References

1. Elshoush, H.T., Osman, I.M.: Alert correlation in collaborative intelligent intrusion detection systems—A survey. Appl. Soft Comput. **11**(7), 4349–4365 (2011)
2. Gupta, N., Srivastava, K., Sharma, A.: Reducing false positive in intrusion detection system: A survey. Int. J. Comput. Sci. Inf. Technol. **7**(3), 1600–1603 (2016)
3. Mohammed, M.N., Sulaiman, N.: Intrusion detection system based on SVM for WLAN. Proc. Technol. **1**, 313–317 (2012)
4. Agrawal, S., Agrawal, J.: Survey on anomaly detection using data mining techniques. Proc. Comput. Sci. **60**, 708–713 (2015)
5. Farnaaz, N., Jabbar, M.A.: Random forest modeling for network intrusion detection system. Proc. Comput. Sci. **89**, 213–217 (2016)
6. Nadiammai, G.V., Hemalatha, M.: Effective approach toward intrusion detection system using data mining techniques. Egypt. Inform. J. **15**(1), 37–50 (2014)
7. Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., Rajarajan, M.: A survey of intrusion detection techniques in cloud. J. Network Comput. Appl. **36**(1), 42–57 (2013)
8. Vinchurkar, D.P., Reshamwala, A.: A review of intrusion detection system using neural network and machine learning (2012)
9. Jalil, K.A., Kamarudin, M.H., Masrek, M.N.: Comparison of machine learning algorithms performance in detecting network intrusion. In: 2010 International Conference on Networking and Information Technology (ICNIT), pp. 221–226. IEEE, New York (2010)
10. Siddiqui, A.K., Farooqui, T.: Improved ensemble technique based on support vector machine and neural network for intrusion detection system. Int. J. Online Sci. **3**(11) (2017)
11. Ashfaq, R.A.R., He, Y., Chen, D.: Toward an efficient fuzziness based instance selection methodology for intrusion detection system. Int. J. Mach. Learn. Cybernet. **8**(6), 1767–1776 (2017)
12. Jabez, J., Muthukumar, B.: Intrusion Detection System (IDS): Anomaly detection using outlier detection approach. Proc. Comput. Sci. **48**, 338–346 (2015). ISSN 1877-0509. http://dx.doi.org/10.1016/j.procs.2015.04.191
13. Wang, H., Jie, G., Wang, S.: An effective intrusion detection framework based on SVM with feature augmentation. Knowl.-Based Syst. **136**, 130–139 (2017)