IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

STRENGTHENING CYBER DEFENSE: EVENT DRIVEN ARTIFICIAL NEURAL NETWORK

VISHNUPRAKASH VS

Department of Computer Science and Engineering

Paavai College of Engineering

(Affiliated to Anna University, Chennai

Namakkal, Tamil Nadu, India

SUNDARRAJ R

Department of Computer Science and Engineering

Paavai College of Engineering

(Affiliated to Anna University, Chennai

Namakkal, Tamil Nadu, India

NANDHAKUMAR S

Department of Computer Science and Engineering

Paavai College of Engineering

(Affiliated to Anna University, Chennai)

Namakkal, Tamil Nadu, India

MR.P. PRAKASH

Assistant professor Department of CSE

Paavai College of Engineering

Affiliated to Anna University, Chennai

Namakkal, Tamil Nadu ,India

Abstract— An intrusion detection system, or IDS, is designed to be a software program that keeps an eye on system or network activity and alerts users when anything suspicious is happening. Concerns regarding how to safely transmit and preserve digital information are raised by the internet's explosive expansion and use. In order to obtain important information, hackers today employ a variety of attack techniques. New things like viruses and worms being imported as the internet becomes more prevalent in society. In order to create system vulnerabilities, malicious individuals employ a variety of methods, such as password cracking and the detection of unencrypted information. As a result, users require security to protect their system from hackers. One of the most often used security methods is the firewall mechanism, which is intended to keep private networks isolated from public networks. IDS are utilized in credit card fraud, medical applications, insurance agencies, and network-related operations. These assaults are detectable with the aid of numerous intrusion detection techniques, methods, and algorithms. This paper's primary goal is to present a comparative analysis of intrusion detection methods utilizing different deep learning and machine learning approaches. In this paper we can implement the hybrid algorithm which includes Convolutional neural network (CNN) with Long short-term memory (LSTM) to improve the accuracy in intrusion detection.

Index Terms— Intrusion detection, Machine learning, Deep learning, Convolutional neural network, Network datasets.

Introduction

Networking is the informal social exchange of ideas and information between people who share a profession or a shared interest. Often, networking starts with a single area of agreement. Professionals utilize networking to widen their social networks, learn about job openings in their industries, and stay up to date on news and trends within their sectors and the broader community. (The phrase "computer networking" describes the process of connecting several machines to enable easy information and software resource sharing.) An association of computers that share resources hosted on or offered by the network nodes via digital links using a set of standard communication protocols is known as a computer network. Numerous telecommunication network technologies, including physically wired, optical, and wireless radio-frequency techniques that can be set up in a range of network topologies, are used to provide the connections between nodes. In a computer network, networking devices, personal computers, servers, and other general-purpose or specialty hosts can all be referred to as nodes. They are identified by their hostnames and network addresses. Hosts serve as enduring labels for the nodes and are rarely changed once they are initially assigned. Communication technologies such as the Internet Protocol use network addresses to locate and identify nodes. Numerous factors, including as the bandwidth, communications protocols used to manage network traffic, size, topology, traffic control mechanism, and organizational goal, can be used to categorize computer networks. Numerous services and applications are supported via computer networks, including the usage of email and instant messaging programs, digital video and audio, shared use of application and storage servers, printers, and fax machines, as well as access to the World Wide Web. The majority of contemporary computer networks employ packet-mode transmission-based protocols. A packet-switched network uses packets, which are organized data units. A packet's size is usually limited by the packet network's physical link technologies to a specific maximum transmission unit (MTU). Before being transferred, a lengthy message is broken up into smaller pieces, which are then put back together to form the original message. Two types of data are contained in packets: control data and user data (payload). Error detection codes, source and destination network addresses, sequencing information, and other data required by the network to convey user data are provided by the control information. Payload data is often located between packet headers and trailers, which contain control information. Compared to a network that uses circuit switching, users can more evenly divide the transmission medium's bandwidth when packets are used. As long as the link isn't overused, other users' packets can fill up the gap left by one's absence, allowing the cost to be shared with minimal interruption. A packet's necessary path via a network is frequently not instantly available. The packet is then queued and awaits a link that becomes available.

A hardware or software program known as an intrusion detection system (IDS) keeps an eye out for hostile activities or policy infractions on a network or systems. Usually, a security information and event management (SIEM) system is used to collect data centrally or to report any malicious behavior or violations to an administrator. A SIEM system employs alarm filtering algorithms to separate harmful activity from false alerts by combining outputs from different sources. The breadth of IDS types varies from individual PCs to extensive networks. Network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS) are the most widely used classifications. An example of a HIDS is a system that keeps an eye on critical operating system files; an example of a NIDS is a system that examines incoming network traffic. IDS can also be categorized based on detecting methodology. The two most popular varieties are anomaly-based detection, which looks for deviations from a model of "good" traffic and frequently uses machine learning, and signature-based detection, which identifies malicious patterns like malware. Another common variant is reputation-based detection (recognizing the potential threat according to the reputation scores). Some IDS products have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system. Intrusion detection systems can also serve specific purposes by augmenting them with custom tools, such as using a honeypot to attract and characterize malicious traffic. Although they both relate to network security, an IDS differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS describes a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. This is traditionally achieved by examining network communications, identifying heuristics and patterns (often known as signatures) of common computer attacks, and taking

action to alert operators. A system that terminates connections is called an intrusion prevention system, and performs access control like an application layer firewall

Related work

Aljawarneh, Shadi, Monther Aldwairi, et.al…[1] proposed the Efficiently detecting network intrusions requires the gathering of sensitive information. This means that one has to collect large amounts of network transactions including high details of recent network transactions. Assessments based on meta-heuristic anomaly are important in the intrusion related network transaction data's exploratory analysis. These assessments are needed to make and deliver predictions related to the intrusion possibility based on the available attribute details that are involved in the network transaction. We were able to utilize the NSL-KDD data set, the binary and multiclass problem with a 20% testing dataset. This paper develops a new hybrid model that can be used to estimate the intrusion scope threshold degree based on the network transaction data's optimal features that were made available for training. The experimental results revealed that the hybrid approach had a significant effect on the minimization of the computational and time complexity involved when determining the feature association impact scale. The accuracy of the proposed model was measured as 99.81% and 98.56% for the binary class and multiclass NSL-KDD data sets, respectively. Intrusion detection systems (IDS) are generally divided into two types (see Fig. 1): misuse and anomaly intrusion detection systems. For a misuse IDS, instructions are identified based on parameters of system weaknesses and known attack signatures. However, it does not recognize attacks that are new or unfamiliar. On the other hand, anomaly IDS is based on normal behavior parameters and utilizes them to pinpoint any action that deviates significantly from normal behavior. The misuse intrusion detection mechanism identifies intrusions by matching existing intrusion patterns in consideration for examination with previously identified patterns.

Sultana, Nasrin, et.al…[2] Network Intrusion Detection systems (NIDS) have been developed rapidly in academia and industry in response to the increasing cyber-attacks against governments and commercial enterprises globally. The annual cost of cybercrime is continuously raising. Organizations can lose their intellectual property with such malicious software crept into the system which may lead to disruptions to a country's critical national infrastructure. Organizations deploy a firewall, antivirus software, and an intrusion detection system (NIDS) to secure computer systems from unauthorized access. Software Defined Networking Technology (SDN) provides a prospect to effectively detect and monitor network security problems ascribing to the emergence of the programmable features. Recently, Machine Learning (ML) approaches have been implemented in the SDN-based Network Intrusion Detection Systems (NIDS) to protect computer networks and to overcome network security issues. A stream of advanced machine learning approaches – the deep learning technology (DL) commences to emerge in the SDN context. In this survey, we reviewed various recent works on machine learning (ML) methods that leverage SDN to implement NIDS. More specifically, we evaluated the techniques of deep learning in developing SDN-based NIDS. In the meantime, in this survey, we covered tools that can be used to develop NIDS models in SDN environment. This survey is concluded with a discussion of ongoing challenges in implementing NIDS using ML/DL and future works. Software-defined network is an emerging architecture that decouples network control and forwarding functions so that the network control can be directly programmable. The segregation of the control plane from the data plane enables easy network management.

Peng, Kai, et.al,…[3] Intrusion detection system (IDS) provides an important basis for the network defense. Due to the development of the cloud computing and social network, massive amounts of data are generated, which inevitably brings much pressure to IDS. And therefore, it becomes crucial to efficiently divide the data into different classes over big data according to data features. Moreover, we can further determine whether one is normal behaviour or not based on the classes' information. Although the clustering approach based on K-means for IDS has been well studied, unfortunately directly using it in big data environment may suffer from inappropriateness. On the one hand, the efficiency of data clustering needs to be improved. On the other hand, differ from the classification, there is no unified evaluation indicator for clustering issue, and thus, it is necessary to study which indicator is more suitable for evaluating the clustering results of IDS. In this paper, we propose a clustering method for IDS based on Mini Batch K-means combined with principal component analysis. First, a pre-processing method is proposed to digitize the strings and then

the data set is normalized so as to improve the clustering efficiency. Second, the principal component analysis method is used to reduce the dimension of the processed data set aiming to further improve the clustering efficiency, and then mini batch K-means method is used for data clustering. More specifically, we use K-means++ to initialize the centres of cluster in order to avoid the algorithm getting into the local optimum, in addition, we choose the Calsski Harabasz indicator so that the clustering result is more easily determined. Compared with the other methods, the experimental results and the time complexity analysis show that our proposed method is effective and efficient. Above all, our proposed clustering method can be used for IDS over big data environment.

Farahnakian, Fahimeh, et.al,…[4] In recent years, significant research has been focused on developing Intrusion Detection Systems (IDSs) to improve software and system security. Generally, IDSs can be divided into two main categories: misuse-based IDSs and anomaly based IDSs. Misuse-based IDSs detect known attacks based on the predetermined signature. Therefore, dynamic signature updating is so important and new attack definitions are frequently released by IDS vendors. However, the misuse-based IDS cannot incorporate the rapidly growing number of vulnerabilities and exploits. Anomaly-based IDSs are designed to capture any deviation from profiles of normal behaviour. Therefore, they are more suitable than misuse-based detection systems for detecting unknown or novel attacks without any prior knowledge. One of the most challenging problems facing network operators today is network attacks identification due to extensive number of vulnerabilities in computer systems and creativity of attackers. To address this problem, we present a deep learning approach for intrusion detection systems. Our approach uses Deep Auto-Encoder (DAE) as one of the most well-known deep learning models. The proposed DAE model is trained in a greedy layer-wise fashion in order to avoid over fitting and local optima. The experimental results on the KDD-CUP'99 dataset show that our approach provides substantial improvement over other deep learning-based approaches in terms of accuracy, detection rate and false alarm rate.

Idhammad, Mohamed, et.al,…[5] Intrusion and attack tools have become more sophisticated challenging existing Cloud IDSs by large volumes of network traffic data, dynamic and complex behaviours and new types of attacks. It is clear that IDS for Cloud should analyse large volumes of network traffic data, detect efficiently the new attack behaviour's and reach high accuracy with low false. However pre-processing, analysing and detecting intrusions in Cloud environments using traditional techniques have become very costly in terms of computation, time and budget. However, many security issues arise with the transition to this computing paradigm including intrusions detection. Regardless the important evolution of the information security technologies in recent years, intrusions and attacks continue to defeat existing intrusion detection systems in Cloud environment. Attackers developed new sophisticated techniques able to bring down an entire Cloud platform or even many within minutes. New records are breached each year by attacker. Recently a destructive DDoS attack has brought down more than 70 vital services of Internet including Github, Twitter, Amazon, Paypal, etc. Attackers have taken advantages of Cloud Computing and Internet of Things technologies to generate a huge amount of attack traffic; more than 665 Gb/s. tem is designed to be inserted in the Cloud side by side with the edge network components of the Cloud provider. This allows intercepting incoming network traffic to the edge network routers of the physical layer. A time-based sliding window algorithm is used to pre-process the captured network traffic on each Cloud router and pass it to an anomaly detection module using Naive Bayes classifier. A set of commodity server nodes based on Hadoop and MapReduce are available for each anomaly detection module to use when the network congestion increases.

Rustam, Zuherman, et.al,…[6] In this globalization era, cybercrime has been entering every aspect through internet network. The development of Intrusion Detection System (IDS) is being studied deeply to solve the problem. There are several classifier algorithms for Intrusion Detection System such as Support Vector Machine (SVM) and Fuzzy C-Means (FCM). In this study, we will compare proposed model using both Support Vector Machine and Fuzzy C-Means to find a better result that increase accuracy of the network attacks. KDD Cup 1999 will be used to evaluate which algorithms work best. The results are very encouraging and show that SVM and FCM can be a useful tool for intrusion detection system. Through the Internet, we can have immediate access to know everything that is happening in every corner around the world. With that convenience, it also attracts some parties to misuse the facility by putting some attack to our network. Intrusion Detection System is a method that can help us detect what kind of attack is trying to

harm our data. It can monitor computer systems and network traffic. The increasing awareness of attack to the system triggered us to develop IDS with a better classifier.

Peng, Kai, et.al,…[7] Tradition network attacks are widely present in fog computing environment. Although the IDS in tradition network have been well investigated, unfortunately directly use of them in fog computing environment may not inappropriate. In this study, we propose a system based on the decision tree, multimethod are compared with this one, not only the 10% dataset but also the full dataset is tested, and the experiment results show that our system is effective. In addition, we also compared the detection time for each method. In the case of guaranteed accuracy, although the decision tree time is not the best one, the calculation time is also acceptable. Above all, our IDS system can be used in fog computing environment over big data. Fog nodes produce massive amounts of data at all times, and, thus, enabling an IDS system over big data in the fog environment is of paramount importance. In this study, we propose an IDS system based on decision tree. Firstly, we propose a preprocessing algorithm to digitize the strings in the given dataset and then normalize the whole data, to ensure the quality of the input data so as to improve the efficiency of detection. Secondly, we use decision tree method for our IDS system, and then we compare this method with Naïve Bayesian method as well as KNN method. Both the 10% dataset and the full dataset are tested. Our proposed method not only completely detects four kinds of attacks but also enables the detection of twenty-two kinds of attacks. The experimental results show that our IDS system is effective and precise. Above all, our IDS system can be used in fog computing environment over big data.

Pham, Ngoc Tu, et.al,…[8] proposed an improved IDS which used feature selection and ensemble models. The proposed models were evaluated using the NSL-KDD training and testing datasets with binary classification. Two feature-selection techniques were applied to reduce the number of irrelevant features and improve classification accuracy. The ensemble models were built based on Bagging and Boosting techniques using tree-based algorithms as the base classifier. The experimental results showed that all the proposed models had high accuracy and low FAR, and the best performance was produced by the bagging model that used J48 as the base classifier and worked on 35-feature subset (84.25% accuracy and 2.79% FAR). Although this model showed the outperformance in comparison with other existing models, there is a limitation that only one dataset was used to evaluate the built classifiers in the paper. Future work will include building classifiers for IDS working with different datasets, and improving the performance of IDS in multi-class classification using ensemble methods and feature selection.

Ahmad, Iftikhar, et al,…[9] Intrusion detection and prevention are essential to current and future networks and information systems, because our daily activities are heavily dependent on them. Furthermore, future challenges will become more daunting because of the Internet of Things. In this respect, intrusion detection systems have been important in the last few decades. Several techniques have been used in intrusion detection systems, but machine learning techniques are common in recent literature. Additionally, different machine learning techniques have been used, but some techniques are more suitable for analysing huge data for intrusion detection of network and information systems.

Sahani, Roma, et.al,…[10] Intrusion detection includes a lot of tools and techniques such as machine learning, statistics, data mining, and so on for the identification of an attack. In recent years, data mining method for network intrusion detection system has been giving high accuracy and good detection on different types of attacks. Decision tree technique is one of the intuitionist and frank classification methods in data mining which can be used for this purpose. It has a great advantage in extracting features and rules. So, the decision tree gives a greater significance to intrusion detection. The tree is constructed by identifying attributes and their connected values which will be used to examine the input data at each intermediary node of the tree. After the tree is formed, it can advise newly coming data by traversing, initial from a root node to the leaf node by visiting all the internal nodes in the path depending upon the test environment of the attributes at each node. The main issue in constructing decision tree is which value is chosen for splitting the node of the tree. In this paper, an improved version of C4.5 algorithm is proposed from the basic concept of C4.5. The detection of intrusion components undergoes two stages. In the first stage, the algorithm evaluates the KDD-99 dataset and constructs the decision tree for detecting the class type as ‘Normal’ or ‘Attack’ type of data in the leaf node in the tree. In the second stage, the classification of attack type is done which will show the attack type. We have considered four types of attacks such as DOS, R2L, U2R, and PROBE. In

this approach, every time the input which is coming from the client system is stored in a database. If incoming data is similar to older one, then no need to go through the apriori algorithm, simply test the type of data which is already defined. If not, then apriori algorithm is applied which consists of associate rules in which all the data are collected. After that, all the frequent item set should be found by applying minimum support mechanism. Then, find the subsets which are common to at least a minimum number constant of the item sets. This would continue until there is no further extension or comparison is found. Then test the leaf data to the defined data type like attack types or normal data. It uses apriori algorithm for making decision tree, and minimum support mechanism gives the way for splitting of attributes or data. This proposed work overcomes the limitations of ID3 algorithm and also increases the system performance and better result in case of large database.

existing methodologies

The combination of security methods is known as intrusion prevention. Anticipating and thwarting the attacks is its aim. Some newer intrusion detection systems apply intrusion prevention. The goal of intrusion prevention is to warn against such assaults rather than studying the traffic logs, which focuses on finding the attacks after they have already occurred. Intrusion prevention systems restrict communications deemed harmful while intrusion detection systems attempt to provide a warning. For many years, the goal of the network's intrusion detection system was to identify as many potential assaults and incursions as possible and report them so that other people might take the appropriate action. Conversely, the new idea behind the development of network intrusion prevention systems is "taking the necessary measures to counter attacks or detectable intrusions with precision." Generally speaking, the IPS are always monitoring the network's traffic in order to actively intervene, restricting or eliminating any traffic deemed hostile, stopping suspicious sessions, or taking other corrective action in response to an attack or intrusion. In addition to operating in a symmetric manner with the IDS, the IPS analyzes connection contexts, automates log analysis, and suspends questionable connections. Contrary to the classic IDS, the signature is not used to detect the attacks. Before taking action, The IDS must make a decision about an action in an appropriate time. If the action is in conformity with the rules, the permission to execute it will be granted and the action will be executed. But if the action is illegal an alarm is issued. In most cases, the other detectors of the network will be informed with the goal to stop the other computers from opening or executing specific files. Unlike the other prevention techniques, the IPS is a relatively new technique. It is based on the principle of integrating the heterogeneous technologies: firebreak, VPN, IDS, anti-virus, anti-Spam, etc. Although the detection portion of IDS is the most complicated, the IDS goal is to make the network more secure, and the prevention portion of the IDS must accomplish that effort. After malicious or unwanted traffic is identified, using prevention techniques can stop it. When an IDS is placed in an inline configuration, all traffic must travel through an IDS sensor. When traffic is determined to be unwanted, the IDS do not forward the traffic to the remainder of the network. To be effective, however, this effort requires that all traffic pass through the sensor. When an IDS is not configured in an inline configuration, it must end the malicious session by sending a reset packet to the network. Sometimes the attack can happen before the IDS can reset the connection. In addition, the action of ending connections works only on TCP, not on UDP or internet control message protocol (ICMP) connections. A more sophisticated approach to IPS is to reconfigure network devices (e.g., firewalls, switches, and routers) to react to the traffic. Virtual local area networks (VLAN) can be configured to quarantine traffic and limit its connections to other resources. The IPS allows the following functionalities:

- Supervising the behaviour of the application
- Creating rules for the application
- Issuing alerts in case of violations
- Correlating different sensors to guarantee a better

Protection against the attacks.

- Understanding of the IP networks
- Having mastery over the network probes and the logs analysis
- Defending the vital functions of the network carrying out an analysis with high velocity.

The IDS can be distinguished on the basis of where the detection is taking place and how or by which technique it is being detected. The IDS is classified into two niche segment one being Network Intrusion Detection System (NIDS) and the other being Host Intrusion Detection System (HIDS). The first system mentioned helps in the analysis the incoming networking traffic whereas the HIDS functioning is based on the activity of the operating system. The main aspects of data mining on IDS that were dealt with originally were termed as clustering and classification. Since there exist no label for the initial data set for clustering issue, the object created for the clustering algorithm was allocated the same class with similar data records. The behavior of the packet was termed as a normal class or abnormal class according to the features and characteristics of already existing data. In Classification, this works on mining from the already clustered data. This implies that the data is labeled. Classification is a data mining technique which is used for examining a data set. In this world of continuous streaming data, classification plays an important role in classifying the data. Many algorithms such as decision tree, rule-based induction, Bayesian network, genetic algorithm etc are used to classify the data. In existing framework implement, machine learning techniques such as Random Forest, Naives Bayes, Support Vector machine algorithms are implemented to detect the intrusion from network datasets. In existing framework can be provide high false alarm and low accuracy.

Proposed methodologies

Deep learning is an emerging trend in the area of machine learning. It is sub-field of machine learning in artificial neural networks. Using deep learning approach in the application area, we can process on large number of items in order to be trained. Process is placed on millions of data points. Deep learning is learning features from the data. If large amount of data is available, it can reduce the performance of system. For achieving better accuracy in terms of performance deep learning is well suited learning mechanism. Learning is varying in three major categories i.e. supervised, semi-supervised and unsupervised. Here, the intrusion detection is carried out with respect to the deep learning approach. Intrusion is the term that can violate security of computer system or network. And another is intrusion detection is the process to identify intrusion. Intrusion detection technique is classified in two methods i.e. anomaly detection or misuse detection. With the rapid expansion of computer networks during the past decade, security has become a crucial issue for computer systems. Different machine learning based methods have been proposed in recent years for the development of intrusion detection systems. This project presents a neural network approach to intrusion detection. A Convolutional neural network with Long short-term memory is used for intrusion detection based on an off-line analysis approach. While most of the previous studies have focused on classification of records in one of the two general classes - normal and multiple attack, this research aims to solve a multi class problem in which the type of attack is also detected by the neural network. Hybrid algorithm is a layered feed forward network typically trained with static back propagation (BP). Such networks have found their way into countless applications requiring static pattern classification. The hybrid model is a flexible type of CNN composed of one input layer, one or more hidden layers, and one output layer.

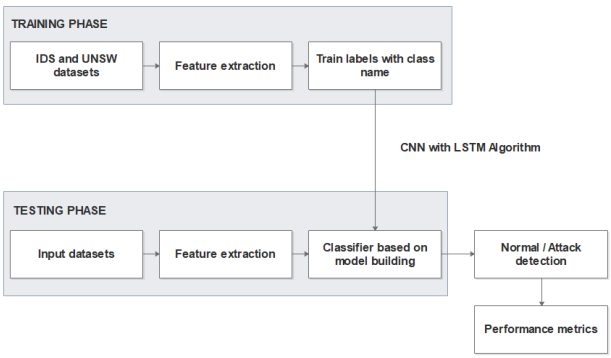

FIG 1 PROPOSED FRAMEWORK

Fig 1 defines proposed work of the system. In this architecture contains two phases such as training and testing phase. Training phase, we can input the KDD cup datasets for predict the classification accuracy in intrusion detection. Using pre-processing steps to eliminate the irrelevant data. Then extract features to predict the attack with improved accuracy. In testing phase, KDD cup dataset can be input to system and

perform hybrid algorithm with Convolutional neural network with LSTM. Finally implemented hybrid deep learning algorithm to identify the attacks based on label attributes. Then evaluate the performance of the system in terms of accuracy, error rate values.

EXPERIMENTAL RESULTS

In this system implemented for intrusion detection using deep learning algorithm in Python framework as front end and MySQL as Back end. The multiple attacks are shown in fig

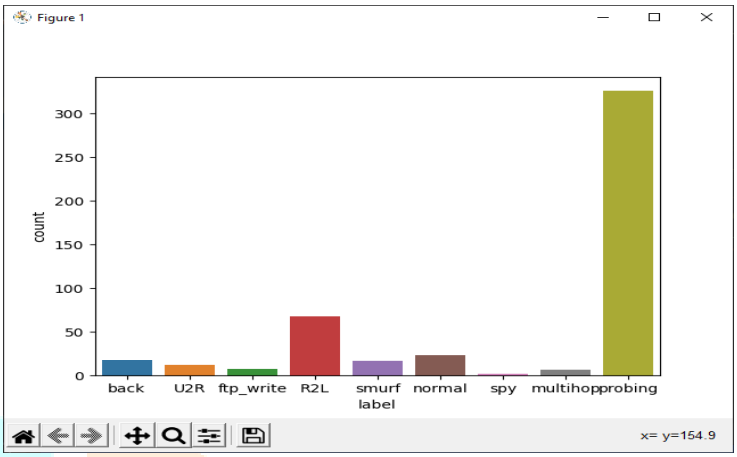

FIG 2: ATTACK TYPES

The performance of the system can be evaluated in terms of accuracy.

We can evaluate the performance of each algorithm and compare the performance based on accuracy parameter. The performance of the system can be analyzed in terms of F-measure parameter. The performance of the system is evaluated using Precision, Recall and F-measure.

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

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

$$\text{F measure} = 2* \frac{\text{Precision} * \text{Recall}}{\text{Precision}+\text{Recall}}$$

The performance evaluation result is shown in following table 3 and shows in fig 4.

Algorithm/ Performance measures	Precision	Recall	F-measure
KNN	42	80	55
MLP	44	82	57
Hybrid	46	88	60

Table 3: Performance Table

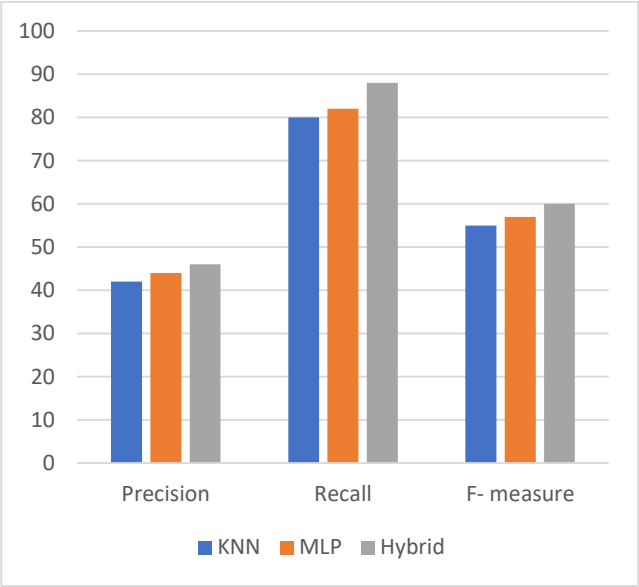

FIG 3: PERFORMANCE CHART

The proposed neural network approach, as shown in Figure 3, provides higher level F-measure values than the existing MLP and KNN algorithm.

Conclusion

Intrusion detection plays an important role in the network security as the applications and their behavior are changing day to day. Network intrusion detection has extensively researched in recent years and many techniques have been proposed including machine learning and deep learning techniques. As a result, there increased the need for accurate classification of the network flows. Here we have proposed deep learning model using CNN with LSTM based feature selection for the accurate classification of intrusion detection. In this paper we have demonstrated the construction of a lightweight neural network capable of real-time network intrusion detection. In the process, we have also provided greater insight into methodologies used by different classification schemes. We discussed potential procedures for both data processing and optimization which are generalizable to other supervised machine learning methods. We also outlined a fast method of identifying key attributes in the neural network based on the connection weights.

References

[1] Aljawarneh, Shadi, Monther Aldwairi, and Muneer Bani Yassein. "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model." Journal of Computational Science 25 (2018): 152-160.

[2] Sultana, Nasrin, et al. "Survey on SDN based network intrusion detection system using machine learning approaches." Peer-to-Peer Networking and Applications 12.2 (2019): 493-501.

[3] Peng, Kai, Victor CM Leung, and Qingjia Huang. "Clustering approach based on mini batch kmeans for intrusion detection system over big data." IEEE Access 6 (2018): 11897-11906.

[4] Farahnakian, Fahimeh, and Jukka Heikkonen. "A deep auto-encoder based approach for intrusion detection system." 2018 20th International Conference on Advanced Communication Technology (ICACT). IEEE, 2018.

[5] Idhammad, Mohamed, Karim Afdel, and Mustapha Belouch. "Distributed intrusion detection system for cloud environments based on data mining techniques." Procedia Computer Science 127 (2018): 35-41.

[6] Rustam, Zuherman, and Durrabida Zahras. "Comparison between support vector machine and fuzzy c-means as classifier for intrusion detection system." Journal of Physics: Conference Series. Vol. 1028. No. 1. IOP Publishing, 2018.

[7] Peng, Kai, et al. "Intrusion detection system based on decision tree over big data in fog environment." Wireless Communications and Mobile Computing 2018 (2018).

[8] Pham, Ngoc Tu, et al. "Improving performance of intrusion detection system using ensemble methods and feature selection." Proceedings of the Australasian Computer Science Week Multiconference. 2018.

[9] Ahmad, Iftikhar, et al. "Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection." IEEE access 6 (2018): 33789-33795.

[10] Sahani, Roma, et al. "Classification of intrusion detection using data mining techniques." Progress in computing, analytics and networking. Springer, Singapore, 2018. 753-764.