A Mechanism for Detecting the Intruder in the Network through a Stacking Dilated CNN Model

P. Nirmala, T. Manimegalai, J. R. Arunkumar, S. Vimala, G. Vinoth Rajkumar, and Raja Raju

1Department of Electronics and Communication Engineering, Saveetha School of Engineering, SIMATS, Chennai, 602105 Tamil Nadu, India
2School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, 600127 Tamil Nadu, India
3Department of Information Technology, Sree Vidyanikethan Engineering College, Sree Sainath Nagar, Tirupati, 517102 Andhra Pradesh, India
4Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, 602103 Tamil Nadu, India
5Department of Electronics and Communication Engineering, J P College of Engineering, Tenkasi, 627852 Tamil Nadu, India
6Department of Mechanical Engineering, St. Joseph College of Engineering and Technology, St. Joseph University in Tanzania, Dodoma, Tanzania

Correspondence should be addressed to P. Nirmala; nirmalajai@gmail.com and Raja Raju; raja.raju@sjuit.ac.tz

Received 10 March 2022; Revised 19 March 2022; Accepted 23 March 2022; Published 12 April 2022

Rapid advancements in the technology and telecommunication areas have led to a massive expansion of network density and information. As a consequence, numerous intruder assaults are being attempted, making it difficult for cybersecurity to identify intruders effectively. The increasing amount of network traffic data has posed a major problem for conventional intrusion detection systems. Moreover, intruders with the intent of launching various assaults inside the networks could not be overlooked. The classification in the article is based on the DL methodologies used in constructing network-based IDS technologies, and it first describes the idea of intrusion detection system. The effectiveness of extracted features and classifications is closely related to detection accuracy, yet typical extraction of features and classification techniques do not function well in this situation. Basic traffic data is also uneven that has a significant effect on classifications findings. A novel intrusion detection model using stacked dilated convolutional autoencoders is proposed and tested it on two additional intrusion detection databases. Many tests have been conducted to define the effectiveness of the strategy. The use of the concept in extensive and practical network systems has a lot of potentiality and possibility. The CTU-UNB database as well as the CTU-UNB database is made up of traffic data from multiple sources. The suggested efficiency of the algorithm is used to evaluate, three types of classification. The deep learning strategy is compared to other ways that were similar. The implications of a number of key hyperparameters are investigated further. The comparison experimental findings show that the suggested approach can reach significantly high efficiency, fulfilling the needs for network intrusion detection systems (NIDS) with higher accuracy.

1. Introduction

The fast development of computerized communication networks has made it easier for enterprises, organisations, and online networking to be more comfortable. Internet purchases, money transfers, industrial manufacturing, and other commercial and public activities have exploded as a result of the Website’s expansion. Cyberattacks and vulnerabilities, on the other hand, represent major concerns to information security. Despite the fact that current security methods like as identity verification, firewalls, and encryption techniques are continually evolving, some first systems protections are still restricted in their ability to identify emerging assaults [1]. Similarly, resulting in frequent growth of numerous
weaknesses and assault methodologies, many forms of cybersecurity risks continued to evolve. As a result, cybersecurity solutions must be utilised to avoid assaults and also to maintain the privacy, availability of materials, and authenticity for online activity. As soon as there is inadequate security rules, improperly configured computer networks, or inadequate software programmes, computer attack vectors would always remain [2]. Information security, information and communications reliability, and security regarding interruption of access will all be provided by a secured computer system or network system. Intrusion detection is described as the difficulty of recognising people who use a computer network unauthorized permission and those who have authorized access and yet are misusing their rights. In principle, instructions could result in the loss of security, authenticity, capacity restriction, or unauthorised utilization of available resources [3]. The following are some clear instances of directives that network administrator are concerned about:

(i) Manipulation of computer system without authorization to allow unauthorised access to the network or personal data
(ii) Illegal access to or change of user data/files
(iii) Alteration of databases or other infrastructure components in networking devices without authorization
(iv) Computer systems that have been accessed without permission

The development of a comprehensive and efficient NIDS is among the primary difficulties in data safety. Despite substantial advancements in NIDS technologies, the bulk of systems still relies on less-capable signature-based methods rather than identifies suspicious techniques to detect threats. The rates of false positive difficulties in collecting valid training examples, training information lifetime, and the software’s behavioural characteristics are all factors for such unwillingness to transition. The present predicament could eventually lead to inadequate and unreliable identification if certain procedures are relied upon. The goal of such a task is to develop a broadly agreed abnormality detection method able to overcome the limits imposed by on-going network configuration [4]. IDS is perhaps the most essential security tool for detecting and restricting malicious network activity. The IDS monitors real-time network traffic and collects Internet traffic in the architecture. The IDS inspects Internet traffic for fraudulent attacks and protects the harmful networks from attackers or assaults by blocking invaders or assaults [5]. Misuse-based IDS and anomaly-based are two types of IDS. By correlating intrusion behaviour to predetermined patterns, misuse-based IDSs are able to detect attacks. Merely recognized attacks, not unknown attacks, are easily noticeable and detected by it. Anomaly-based IDSs, on the other hand, detect variations in network systems from usual behaviour. A robust attack system is supposed to detect fraudulent activity from links which have not been formed [6]. It is sensitive enough to detect unknown threats by observing their multiple criteria in the network infrastructure context.

Furthermore, the technique is utilised to defend the networks against intruders. It also analyses networking flow of traffic and categorises it as normal and anomalous. The study looked at how machine learning (ML) and deep learning could be used to address the requirements of effective IDS. Both ML and DL operate underneath the AI framework and detect meaningful information from huge amounts of information. Due to the advent of enormously potent devices, such technologies are gaining significant prominence in the world of computer security during the last decades (GPUs). Both ML and DL are effective methods for extracting meaningful information in Internet activity and forecasting normal and abnormal actions based on the patterns established. To acquire necessary details from Internet traffic, the ML-based IDS mainly relies on feature extraction [7]. Several ML- and DL-based techniques have been presented by researchers throughout the last years to progress the effectiveness of IDS in recognizing suspicious attempts. Nevertheless, the tremendous rise in Internet activity, as well as the related security vulnerabilities, has presented numerous obstacles for NIDS systems to automatically identify hostile attacks. The study into applying DL approaches for network-IDS is still in its starting stages, and there is still so much of space to investigate such technique within NIDS to identify invaders more effectively. Because of its basic structure, DL-based IDS do not really require feature extraction and are capable of automatically acquiring complicated features from the data.

Deep learning has recently acquired popularity as a result of the possibilities it holds for learning algorithms. Importantly, technology becomes a vital aspect of information security because it allows for a thorough and definitive testing of the prototype. Figure 1 depicts the framework of deep learning. Deep learning algorithms that are based on the human brain’s structural depths teach from the lower grade feature to a higher tier notion. It is due to several layers of the protocol stack. To begin, deep learning is described as the usage of deep networks that are connected to compute techniques which use multiple stages to generate an output. In general, the levels cascading with the following tier receiving the data from the past stage are inputting information and generating an output. The stages typically include the inputs tier; it contains fundamental data, then multiple hidden layers, and ultimately, the later phases that provide the outputs. DL approaches retrieve unique properties in information from the least level to the top level using multiple-layer structures or deep frameworks, and they can expose massive quantities of pattern in the data [8]. The algorithm is mostly based on unstructured characteristics that create higher representation of the data from lower tiers. In addition, new deep learning approaches are being developed to respond to growing data quantities and the need for greater precise and decisive assessment [9]. Because of their outstanding outcomes in speech perception, language processing, and some other areas, deep learning methods had gained a reputation as advanced algorithms. The major
reason for this is that deep learning methods are linked to two key features: deep hierarchical models and understanding long-term pattern classification correlations in wide scale sequence information [10]. The IDSs use a variety of classification techniques to categorise network traffic flow and intrusion datasets, including artificial neural networks, K-nearest neighbour, Bayesian and decision tree, support vector machines (SVMs), and convolutional neural network (CNN). For IDS, a stacking dilated CNN approach is employed in this paper.

Deep learning techniques are used to accomplish predictions and classification techniques in a variety of domains. In particular, CNN is the utmost extensively used technique for deep learning information analysis. The CNN is capable of analysing characteristics from a variety of databases, including Internet traffic data sources. Furthermore, it accurately detects contributory characteristics in comparison to existing feature extraction techniques. After completing the selection of features, the convolutional neural network implements effectively in the cataloguing phase and delivers high accuracy for a huge data. The CNN provides the same convolutional kernels, which reduce the amount of features and training dataset. The main benefit of such a CNN is to lessen the quantity of extracted features that are utilised to quickly recognize attack types [11]. Layer of convolution, layer of pooling, and fully connected layer are the three main levels of the CNN. Those layers are also configured which customs a comprehensive convolutional structure. These convolutional layers build multiple local features by using a greater amount of kernels (filters) for the supplied attribute values.

The CNN is also beneficial in terms of enhancing detection capability. Convolutional neural networks (CNNs) are a deep learning (DL) technique that was used in a variety of applications. Not only can it choose characteristics, but it could also categorize traffic information. It can also automatically identify good characteristics than typical selection techniques. The more traffic data the CNN has, the more valuable characteristics it can acquire, and the finer classifications it can make. However, in a massive data environment, machine learning algorithms are prone to overfit. As a result, CNN is well-suited to large-scale networks. Furthermore, when comparing to other DL techniques, the most significant benefits of the method is that it uses the similar convolutional kernels and drastically decreases the occurrence of variables and training computation time; it can quickly identify attack types of traffic data [12]. There were also various investigations into the use of CNN domain of detecting intruders. Some studies, instead, solely used CNN to choose characteristics or categorize traffic, ignoring the database imbalances, which is critical to detection algorithms. To overcome problems with unequal Internet traffic categorization, a revolutionary unbalanced information gravitation-based categorization approach was developed, which succeeded well. However, it has a high computational cost. To normalize the database, the sample technique lowers the amount of all traffic categories to the class with the fewest. The huge reduction in database amount, on the other hand, could decrease CNN’s attribute selection performance [13].

The focus of the study is to develop a unique NIDS by combining the capabilities of unsupervised training and CNNs to identify or train essential characteristics in enormous quantities of unprocessed system packets autonomously. The research proposes a network intrusion detection model based on stacking dilated convolutional autoencodes. By stacking dilated convolution layers, the model can get a very large receptive field [14]. The framework is validated using malicious traffic data from a wide variety of malicious apps in a variety of classification techniques. Implementation of various set of parameters on evaluation findings, as well as determination the best hyperparameters for the proposed model, is also investigated and explained. Convolutional networks make use of convolutional layers, which have been shown to improve feature extraction capability [15]. The experimental findings show that the model could achieve exceptional results and match the amount of high accuracy and adaptation in NIDs.

The following explains how the rest of this research study is organised: The second section discusses similar works in the field of feature selection and categorization. In Section 3, the overall system architecture is provided, as well as the system’s working flow. The achievement is demonstrated in Section 4 by the many tests that are carried out in order to evaluate the suggested system. Section 5 highlights the contributions and accomplishments made in this work.

2. Related Works

Network security has long been a major issue. Network security has long been protected by intrusion detection systems. To increase the efficiency of intrusion detection systems, a multiple ML methods are used with supervised methods gaining popularity and being regarded as a viable option. Several cognitive techniques are used to increase IDS detecting capabilities. Supervised methods are one of these strategies that are gaining popularity and have been shown to outperform individual instructional strategies. Furthermore, the integrity of learning algorithm consumes
substantial effect proceeding intrusion detection ACC. Furthermore, the integrity of training information is an essential variable which can significantly improve detection performance. The residual density proportions are by far the strongest unitary classifications because, now, users know that. Researchers can develop a potent intrusion detection technique with good efficiency, low classification difficulty, and robust performance by combining the strong quality-improved conversion with SVM ensembles. The quality-improvement method is a necessary component to recreate the original characteristics in order to give high-quality and compact training examples. Then, to use the properly processed data, an SVM ensemble classification is performed, and ultimately, the intrusion detection system is produced. The logarithmic marginal density proportion is performed, and ultimately, the intrusion detection model was therefore built on the properly processed data, an SVM ensemble classification is performed, and ultimately, the intrusion detection system is produced. The logarithmic marginal density proportion conversion is added to the raw characteristics in order to produce fresh and improved-quality altered training data. The intrusion detection model was therefore built using an SVM ensemble. Experimental findings suggest that the suggested methodology can produce a good and stable performance, with substantial competitive benefits of efficiency, predictive ACC, and FP, with training duration when compared to other conventional techniques. This solution, however, only studied the basic situation of intrusion detection difficulties and cannot account for diverse forms of attacks. The research proposed an efficient IDS established from SVM and information augmenting [16].

Numerous information mining-based IDS approaches are employed to network traffic information and host information in the earlier centuries considering the vast quantities of vulnerability scanning information as well as the complicated and diverse aspects of intrusion activities. Unfortunately, there are a number of difficulties that will need to be investigated in relation to present intrusion detection systems (IDS). Using the KDD99 benchmarking intrusion detection database, researchers compared the performances of the proposed approach to that of established learning techniques. The test results reveal that using minimal computational resources, the suggested approach obtained higher DR and considerably reduce the FP for various forms of network traffic. The suggested technique also resolves various data mining challenges, such as responding with continuous attributes, lacking data points, and noise reduction in training data. The abnormality detection approach detects new assaults by separating abnormal from regular actions, and it yields high detection rates (DR) for various threats, but it also generates a lot of false positives (FP). Anomaly-based IDS develops rules by examining gathered audit data, which are the operating system’s activity logs. Predictive intrusion detection is continuously being built to address the challenges of evaluating large amounts of datasets and optimising detecting rule effectiveness. The study presents a supervised responsive network detections by a NB classification and regression trees that accomplishes manage detection methods and keeps false positives at an appropriate standard for various kinds of network intrusions, as well as removing redundant characteristics and conflicting illustrations from training data which contribute to making the detection method complicated [17].

The Internet technology has a wide range of uses in the battlefield, business, pollution monitoring, and a variety of other areas. The Internet of Things is becoming increasingly popular as technological advances. There have been a slew of application domains released. The intrusion detection system has becomes increasingly prevalent as one of the technologies. Wireless sensor networks, as among the most technology aspects of the twenty-first century, serve a critical role in integrating the logical aspect of organizational with the current external reality. Dos attacks, active attacks, authenticity assault, fake routing protocol attack, and flooding attack known to as KNN following classification method in wireless sensor nodes are the most common security risks to the Internet of Things, which is made up of wireless sensor networks. The technology can distinguish aberrant networks from regular nodes by analyzing the anomalous actions, and they examine the intrusion detection system’s configuration determination and error rate. The detecting program’s formulation and simulation are discussed in detail in this paper. By upgrading the wirelessly intermediate node routing protocol, this system has accomplished efficient and speedy intrusion detection. The experiment outcomes demonstrate that the technology seems to have an improved detection quality and precision, which is in line with the intrusion detection specification. Nevertheless, the dynamic nature of the communication channels, combined with a poor software infrastructure, has posed significant security problems to wireless sensor networks, severely limiting their application. In a wireless sensor network, the technology may identify flooding attacks. Researchers also perform tests to see how flooding affects the environment. The simulated results suggest that overflow can have a significant impact on system flow, particularly in bigger networks. The simulations reveal that the device is capable of effectively preventing flooding attacks. The study suggested an IDS established on K-near-neighbour [18].

An aggregation classifier, which is a collection of classifications, outperformed separate classifiers in machine learning. Despite various ensemble algorithms exist, finding a good composite structure for a given dataset remains a challenging problem. To discover improved behavioural variables for PSO, the local uni-modal sampling strategy is employed as an optimizer. Researchers used some random selections from the well-known KDD99 dataset for the empirical analysis. The novel techniques and also the weighted majority algorithm (WMA) are used to generate maximum classification. The findings of the experiments show that its novel method can produce ensembles that outperform WMA in classification performance. When binary classifications disagree, the final determination is obtained by combining their performance. Implementing multiclass categorization algorithms to act as the base expertise is an alternative solution. By doing LUS metaoptimization, PSO variables are improved; nonetheless, the projected advantage of AC is small, particularly, while one considers the extremely long duration required LUS to execute. Although researchers improved by 0.0529 percent on average as
comparing to PSO, it required 500 times longer than average. LUS’ precision improvements come at the expense of substantially longer runtimes. Finally, researchers can say that weight derived using metaheuristic techniques can increase intrusion detection and prevention effectiveness. As a result, LUS has not shown to be a successful strategy for combining classification model into an ensemble for intrusion detection. A unique ensemble development method has been proposed which employs PSO determined weights to generate a more accurate classification model for intrusion detection [19].

The preprocessing of communication networks, the identification of important components, and the construction of fast classification algorithm that categorize normal and anomalous sequences are all critical parts in developing compact IDS. As a result, the architecture of IDS is examined from such three different perspectives in this paper. The objectives of this study are to eliminate unnecessary occurrences from the learning algorithm that allows it impartial, find an appropriate subset of attributes using a KNN-based feature selection technique, and implement the proposed IDS with a neuro-tree to improve detection performance. The compact IDS was created by combining a KNN-based feature selection approach that maximises the IDS’s sensitivity and selectivity with an adaptive neural ensemble decision tree method to generate optimal results. To accomplish the identification of abnormal system patterns, an exhaustive experimental assessment of the suggested approach with a family of six decision tree classifications, particularly, NB Tree, RF, and RT model, has indeed been presented. The categorization algorithm is a neuro-tree model, which has a detection rate of 98.4 percent that is higher than NN and extended C4.5. The properties of the suggested technique are summarised using several performance measures such as true positive, false positive, recall, $f$-measure, and precision. The database is supplied with a varied amount of classes; the suggested technique performs better. These support the assertion that perhaps the selected approaches and training methodology neuro-tree is an effective intrusion detection approach. A lightweight intrusion detection system (IDS) for accurately detecting deviations is built [20].

With the evolution of the Internet throughout time, the amount of Internet-based cyberattacks has risen as well. To guarantee information security, a strong IDS is essential. IDS’ aim is to keep track of the activities in a system and evaluate those for indicators of potential abnormalities. Although little work has been conducted in this area, more comprehensive research is still to be completed. Utilizing attribute selection approaches, a subset of major characteristics is chosen from the entire collection of characteristics, and the set of major characteristics is being used to training various types of classifications to create the IDS. To find findings, the NSL-KDD dataset is subjected to fivefold cross-validation. Furthermore, it is discovered that the $k$-NN classification outperforms the others and that the informational benefit ratio-based attribute selection approach outperforms some others. Using feature selection methods, a subset of relevant features is picked, and the collection of major characteristics is then utilised to train various types of classifications. This study employs PCA, IGR, CFS, and maximum, minimum relevance feature extraction approaches, as well as $k$-nearest neighbor, neural network, support vector machine, and Naïve Bayes classifiers. As each of the classifications and feature extraction methods has advantages and disadvantages, the study employs a variety of feature selection techniques and classifications. It is tough to select one over the other when it comes to installing an intrusion detection system. Furthermore, since all of the configurations provide considerable accuracy, the experimental results indicate that machine learning may be employed in intrusion detection. The $k$-NN classification outperforms the others, while among the feature extraction approaches, the IGR information classification algorithm outperforms the others while CFS falls short. IGR feature selection with $k$-NN has the accurate results of all the configurations. As a result of this research, it can be determined that using a combination of IGR feature selection and $k$-NN to design an efficient intrusion detection system is possible. The research proposes an IDS for networks based on machine learning that has a strong union of feature selection algorithm and classification by analyzing the configurations of most prominent attribute selection strategies and classifications [21].

Intrusion detection is a critical component of information assurance, and the fundamental technique is the ability to reliably recognize diverse network attacks. Furthermore, researchers investigate the quality of the model in dual and multiple categorizations, as well as how the neurons of hidden layer and number of iterations affect the quality of the model. On the standard given dataset, researchers compared it to J48, ANN, RF, and SVM with ML-based models suggested by past researchers. The investigational results indicate that RNN-IDS is well adapted to constructing a categorization model with good precision and that its effectiveness in binary and multiclass categorization is greater to those of classic machine learning classification techniques. The RNN-IDS model enhances intrusion detection performance and introduces a novel intrusion detection research methodology. The RNN-IDS model provides high reliability in binary and multiclass categorization, as well as great forecasting capacity for intrusion prevention. When compared to conventional different classifiers like J48, Naive Bayesian, and random forest, the outcome achieves good accuracy rates and detecting rates with such a least false-positive rate, particularly when performing multiclass classification on the NSL-KDD database. Both of the precision of intrusion detection and the capacity to recognize the type of attack can be improved with the models. However, with GPU acceleration, the learning curve cannot be shortened, and the gradients are expanding and dissolving. A DL-based intrusion detection scheme is presented and also a DL approach for attack detection using RNN-IDS [22].

As the number of nodes grows, so do the security vulnerabilities. Network attacks have expanded dramatically, necessitating the use of effective IDS. Information gathering has grown in prominence as a tool for detecting intrusions. The core impression is to use alternating decision trees (ADT) to categorize different sorts of assaults using
intrusion data. The alternating decision tree algorithm is a very well binary classifier decision tree approach. Decision trees and boosted are combined in alternating decision trees (ADTree). ADTree is a unique categorization structure that is simple to use, easily understandable, and durable. ADT is a supervised training approach that builds an inductive tree in binary cataloguing difficulties. The ADT generates a DT that includes predictions and splitting nodes. It is a supervised boosting approach called the ADT technique. It focuses on using ADT to categorize assaults. The empirical analysis relies on the NSL-KDD dataset. For DOS, Probe, DOS, R2L, and U2R, the technique achieved AC of 97.61 percent, 97.15 percent, and FAR of 3.3, 5.5, 2.38, that is, significantly higher than other previous techniques. For the modeling findings, researchers employed the NSLKDD dataset. Three sorts of attacks are grouped together. The suggested technique efficiently classifies various sorts of attacks. For the modeling and Naive Bayes algorithm, DR and FAR are calculated. An order to enhance performance should raise the DR while lowering the FAR. In the categorization of IDS assaults, the suggested technique creates greater DR and lowers the FAR. It does not, however, incorporate iterative and incremental model into ADT tree to categorise different sorts of attacks. The author presents an innovative way of classifying intrusion attempts [23].

Intrusion detection is among the maximum pressing security issues. A considerable variety of approaches through ML methodologies have already been established. These are, unfortunately, not very good at detecting all forms of invasions. Every assault has been consigned a categorization and the mappings of attack features. Problems with identifying limited assaults to use an attack pattern database are also examined, with potential strategies for enhancement given. ML algorithms have been evaluated and analysed in regard of its sensing properties for different types of attacks. There are also drawbacks associated for each of the categories. The article also includes a number of data mining methods for machine learning. Finally, innovative methods for detecting attacks utilizing machine learning techniques are discussed. The growing number of specific network computer attacks has had a negative impact on user confidentiality and protection. Researchers have consumed so much period evolving various ways for identifying attacks. An evolutionary approach was used to evaluate the essential performances of machine learning techniques. A single classifier strategy and a multiple classifier technique were used in the comparative. The limitations of employing machine learning algorithms to identify low-frequency assaults on a training set have indeed been addressed. Unfortunately, not all of the strategies for evaluating performance are used to ensure that the findings are repeatable. In this study, a thorough research and analysis of several ML algorithms is conducted in order to conclude the difficulties with these approaches in recognizing intruding behaviours [24].

The complexity of the database is decreased in the created system by first performing data preparation on the NSL-KDD dataset and then utilising multiple techniques and algorithms. For feature extraction, two additional solutions have been suggested. The multilayered architecture is composed by selecting relevant machine learning techniques depending on the nature of assault. The KDD dataset is used to conduct presentation evaluation on the developed framework, including such AC, true positive, false positive, $F$-measure, MCC, and duration. To illustrate the suggested system’s performance, it is examined to review the literature, and its results are evaluated. The suggested method has been proved to have good accuracy false-positive frequencies in all sorts of attacks. Depending on the type of attack, a composite multilayered intrusion detection method is designed that employs several machine learning approaches. When compared to earlier studies, the most significant outcome of this study is the presentation of a system performs detection mechanism with really excellent performance levels in practically all performance measures and low error rates. The database is initially transformed and normalised before being used in the creation of an intrusion detection system. Then, utilising two new methods that use separate techniques and algorithms, training and test samples are constructed. The component quantities of database quantities are decreased by about half using the suggested feature selection technique, and extremely effective values are achieved with all these information in the testing. The testing and training activities were carried out using the NSL-KDD percent 20 classification model. Following the feature representation, testing was done to establish the most relevant machine learning technique for the attack patterns, as well as the techniques to be deployed. The suggested system’s performance was assessed using several measures including such AC, true positive, false positive, $F$-measure, MCC, and duration. Throughout the study, a hybrid and layered IDS is developed that employs a mix of ML and various classification algorithms to deliver high-performance detecting mechanism in a various attack patterns [25].

3. Proposed Methodology for Dilated CNN

The section introduces a methodology for intrusion detection systems from a broad perspective. Following that, a quick overview of how the datasets were created is given. Finally, the technique’s deep learning process is discussed in depth.

3.1. Model Description. A data module is being used to utilise raw traffic on a network from the Contagio-CTU-UNB dataset. Dilated convolutional autoencoders (DCAEs) learn layers in feature extraction in massive amounts of unlabelled dataset in the unsupervised pretraining phase. After that, supervised fine-tuning using the back propagation approach and a small number of labelled samples improves the descriptions learnt from unlabeled data.

High-level view of the DCAE-based model’s training process is depicted in Figure 2. The development method consists of unsupervised pretraining and supervised fine-tuning.

As demonstrated in Figure 3, the network is trained as a typical CNN without pooling layer and without employing
Dilated Convolutions

3. Dataset. Three different categorization experiments are carried out on two different datasets. The CTU-UNB database is made up of botnet traffic from the CTU-13 database as well as standard traffic in UNB ISCX IDS 2012 dataset. The Contagio-CTU-UNB database is made up of six different categories of network traffic data. Sections of the CTU-UNB database are responsible for the normal and botnet traffic. The threat glass portal is the source of the web-based malware traffic. Exploits, APT’s, and scans are all traffic generated by parts of contagio or deep end research.

3.3. Data Preprocessing. It serves as a link in the systems and the users by transferring data. That is where every user requests and data are performed. It examines the information and requires that an intrusion detection process be performed. It is in charge of gathering the appropriate dataset from the database and supplying it to the servers in accordance with the queries in such situation. It can also be used.
3.4. Feature Extraction with IDS Module. The two key processes of the IDS modules are feature selection and categorization. The intrusion detection module is responsible for feature extraction and categorization.

3.5. Feature Selection Phase. The module’s main purpose is to choose the most contributing characteristics for the categorization process. It accomplishes it by employing the CRF and LCFC technique. Sort the characteristics into groups based on how far apart the traits are. Then, using CRF, choose two features that help you make decisions about intrusion records. The coefficient of correlation value is determined using conventional formulae after the features to receive the output that is delivered from the server via user requests.
3.6. Classification Phase. To avoid overfitting, the early stopping method is employed. In addition, the abstraction characteristics are used to complete a classification process using the softmax classifiers. The approach is more adaptive and flexible because of the usage of a variety of raw network traffics and unsupervised pretraining.

4. Stacked Dilated Convolutional Model

Dilated convolutional autoencoders (DCAEs) have a similar design to traditional autoencoders. The architecture of a dilated convolutional autoencoder is shown in Figure 4. An activating method transforms the inputs into convolution layers (Equation (1)):

\[ \bar{f} = s(A \ast \bar{E}' + y'). \]

where \( \bar{f} \) is the two-dimensional output map, \( A \) is the two-dimensional inputs transformed from a numerical vectors.

In proposed model, the activation function \((\ast)\) is a rectified linear unit, AF input vector. The DCAE operation is represented by the symbol. Following that, the hidden layer’s feature mappings are transferred into the reconstructions using an inverted convolution (Equation (2)):

\[ A = s \left( \sum_c \bar{f} \ast \bar{E}' + \bar{y}' \right), \]

where \( A \) is a collections of feature maps with the same structure as the input \( A \); also, \( i \) is a set of feature maps with the same shape as the input \( A \). Weight matrices \( \bar{E} \) and \( E \) both have the same initial values.

The dilated convolutional autoencoder’s training purpose was minimizing the variance among the input vectors \( A \) as well as the reconstructed \( B \). The mean squared error is the cost function in proposed model (MSE) (Equation (3)):

\[ M(A, B) = \frac{1}{2} \sum_j (A_j - B_j)^2. \]

By layering many DCAEs, the DCAEs could be used to create a DNN. The hidden layer results the preceding DCAE has been used as the input of the following DCAE. Stacking DCAEs is a demanding layer-wise unsupervised training procedure. Dilated convolutions get the benefit of being able to have a broader variety of visual field without information loss. As a result of these advantages, it is better suited to information extraction. First, using dilated convolutions expands the activation functions of the layers, allowing them to learn more global characteristics. Dilated convolutions, as opposed to max-pooling, can safeguard the data input from data lost. Second, the DCAEs’ model training method does not require labelled data, which is more feasible in practise. Finally, compared to fully link neural networks, DCAEs have fewer parameters. As a result, DCAEs outperform other unsupervised DL methods for effectiveness and efficiency.

5. Result and Discussion

Initially, some classification metrics for performance analysis is briefly introduced in this section. Following that, the experimental procedure and environment are detailed. Finally, some key experimental findings are presented.

For the performance analysis experiments, six assessment measures are used. AUC, precision, recall, f-measure, receiver-operating characteristic (ROC) curves, and matrix of confusion are the six measures, correspondingly. True negatives (TN), true positives (TP), false negatives (FN), and false positives (FP) are the selected classification functions that these metrics are related to (FN). To put it another way, true negative and true positive accurately count the amount of intrusions and classify them as normal. The percentage of assaults and normal data that is wrongly recognized is represented by FP and FN, accordingly. The confusion matrix \( Z \), whose starting diagonal entries reflect the amount of properly projected data, can be used to compute those basic components. The ROC graph represents the classifications model’s overall performance of TP and FP. The greater the true positive and the smaller the false
positive, the greater will be the AUC. AUC illustrates the proportion of clearly recognized data across all samples. The fraction of successfully detected attacks against all anticipated attackers and all actual existing attacks is described by precision and recall correspondingly. The weighted mean of recall with precision is the $F$-measure.

To assess the effectiveness of the proposed scheme, the Contagio-CTU-UNB dataset is used and the CTU-UNB database to complete three types of classification techniques. The Contagio-CTU-UNB database is used for 6-class classifications, and the CTU-UNB dataset is used for class-2 as well as class-8 classifications. The class-6 classification includes normal data as well as five other types of malicious traffics data. Standard and botnets data in CTU-UNB database are included in the class-2 classification. The performance of three types of categorization tasks is shown in Table 1.

The DCAE had the same amount of hidden layers as the SAE and the DBN. In comparing to other deep learning networks, the DCAE achieved the greatest accuracy in the 6-classification challenge. However, in the binary classification, the technique performed best, with a 99.59 percent accuracy rate. The results of 8-class classification were significantly lower than those of 6-class classification. Table 2 shows the precision (P%), recall (%R), and $f$-measure (%F) of class-6 classification.

After approximations, the DCAE approach surpassed the comparison of DL approaches and obtained the similar approximate variable with three measurements. The accuracy, recall, and $f$-measure of the 8-class classification problem are given in Table 3. Figure 5 shows the line chart for the accuracy, $F$-measure, and recall of class 8 classification.

The 6-class classification of confusion matrix uses the technique that is shown in Table 4. The amount of accurately categorised samples in the testing dataset is shown by the leading vertical. There are fewer examples wrongly recognised in botnets and scans. Similarly, Table 5 demonstrates the 8-class classifying task’s confusion matrix utilizing proposed method. Despite the fact that the menti and sogou had the lowest datasets, they nevertheless performed admirably. The binary classifier AUC score was 1.00, indicating that the technique did exceptionally well in binary classification. In the meantime, the AUC for 6-class and 8-class categorization was 0.99. The approach almost certainly delivers huge amount of true positives as well as a least amount of false alarms.

In particular, the class with the fewest data has the worst effectiveness, which has an effect on the overall values. However, the strategy worked effectively even when there was a limited amount of training data. Tables 4 and 5 support this conclusion.

Furthermore, after completing the 2-class classifications task that discovered botnets data, the network was maintained to assess the proposed model’s generalisation.
capabilities. The generalisation of characteristics learnt in CTU-UNB dataset was therefore evaluated using a different testing set incorporating kinds of attacks from the Contagio-CTU-UNB dataset. The current test set contains a total of 16000 samples that contains 2 types of traffic data, standard, and attack, as shown in Table 6. A normal and botnet data from the CTU-UNB dataset’s test set are chosen since the Contagio-CTU-UNB dataset’s normal and botnet data might be included in the CTU-UNB dataset’s training set. In addition, the Contagio-CTU-UNB dataset’s test set contains four types of complicated assaults (network-based malware, exploit, APT, and scan). Particularly, the CTU-UNB dataset is used to save a system that has been trained well in the class-2 classification problem. The saved framework was then used to analyse the fresh test set data. In other words, in the generalisation assessment task, the developed framework was implemented to determine some unknown traffic data or several unknown threats.

The current test set has a detection accuracy of 89.9%. Table 7 illustrates the accuracy, recall, and F-measure of the generalisation experimental evaluation. According to the findings of the evaluation, Suggested model might acquire certain useful and generic properties from botnet data in order to identify anonymous attacks.

In the DCAE approach, the best parameters from experiments conducted were chosen, as shown in Table 8. Table 8 compares studies on convolutional autoencoders with varied amounts in the layers of convolution and two basic types of AF. The completely linked layer’s unit number were modified to the same as its input values since the model might perform better. The sigmoid function and the ReLU function were chosen as activation functions for convolutional autoencoders. Saturating nonlinearities and nonsaturating nonlinearities are represented by these types of AF. The functional form that matched to the sigmoid function has been the cross-entropy loss.

The experimental findings reveal that the quantity of layers as well as the activation functions (AF) that is used has no impact on the results of the network. It may, however, have a significant impact on the program execution. When compared to the sigmoid function, the ReLU function saves time. Once the activation function is the ReLU, the amount of layers has negligible consequence towards the program execution. As a result, when it comes to overall efficiency, the ReLU function outperforms the sigmoid function.

The goal of the research would be to use DL approaches to automatically and efficiently absorb important features in the unlabeled original traffic data. In conclusion, the research indicates that the suggested method can learn classification model from enormous quantities of unlabeled training set and attain great performance. Sections of the prefix and header data of packet headers are used to create training examples through the session. The proposed DL strategy performed admirably on a variety of categorization tasks. These findings concentrated on the feature representations are derived from raw traffic data. Such feature representations are certain to be successful in identifying different abnormal network traffics while generating a low number of false alarms. The findings of the experiments also demonstrate that adding further layers of convolutional autoencoders does not improve efficiency as much as predicted. It is possible that this is because the first convolutional layer’s number of hidden modules is sufficient to learn usable classification model. Furthermore, various activation functions have one significant impact on training time.

6. Conclusion

An intrusion detection approach through stacking dilated CNN is introduced and applied for recognizing as well as detects the attackers efficiently in wireless networks. Massive
amounts of unlabeled original traffic data can be autonomously learned important feature representations using the suggested DL approach. The Contagio-CTU-UNB dataset and the CTU-UNB dataset were constructed using computer traffic data from different sources. To assess the proposed effectiveness of the algorithm, three different categorization activities are used. Deep learning method is compared to other techniques of a similar nature. The impacts of a number of vital hyperparameters are investigated further. Experiments show that the model outperforms others in detecting intruders from large amounts of data. By combining significant computational approaches, this method was able to accomplish exceptional performance that fulfills the demands of large-scale and real-world network systems.

**Data Availability**

The data used to support the findings of this study are included within the article.

**Conflicts of Interest**

The authors declare that there is no conflict of interest regarding the publication of this article.

**Acknowledgments**

The authors would like to express their gratitude towards Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences (Formerly known as Saveetha University) for providing the necessary infrastructure to carry out this work successfully.

**References**


