International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i04.040 ISSN: 2581-4621

Surveying the Effectiveness of Intrusion Detection using different Deep Learning Models

Bony Mathew Thomas[1], Shalu Shani[2], Christa Rose Mary John[3], Sebin Thomas[4], Binny S.[5]

[1234] *PG – Master of Computer Application, Kristu Jyoti College of Management and Technology, Changanassery, Kerala, India*

[5] *Associate Professor, Department of Computer Application, Kristu Jyoti College of Management and Technology, Changanassery, Kerala, India*

ABSTRACT

The rapid expansion and progression of the internet have raised serious concerns regarding the prevalence of cyber-attacks. In order to safeguard data from malicious activities, intrusion detection systems (IDS) have emerged as effective solutions employing artificial intelligence techniques like machine learning and deep learning. This survey examines relevant literature on intrusion detection systems with a particular emphasis on the learning algorithms employed by deep learning approaches. It addresses recent deep learning research using a variety of algorithms, learning techniques, and datasets to produce an operational intrusion detection system.

Keywords –IDS, DBN, RNN, LSTM, CNN, AE

1. Introduction

The protection of data, programs, servers, and network infrastructure against unauthorized access or modification is known as cyber security. The increase in internet usage has resulted in a significant growth in data volume and complexity. Consequently, the need for a robust intrusion detection system has become apparent in order to keep up with the constantly expanding internet and vast amounts of information available. Network security is part of the cybersecurity subsystem, which protects systems that belong to a network against malicious activities. The goal is to ensure data security, integrity and availability through the provision of networked computers. Intrusion Detection involves the monitoring of network traffic and computer events to identify unexpected occurrences. Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) are names that are frequently used interchangeably to refer to related concepts. Deep Learning is a subset of machine learning, which is a subset of artificial intelligence. Consequently, ML and DL are utilized to develop a robust and proficient intrusion detection system.

Machine learning algorithms are algorithms that can learn and adapt based on data. They are designed to generate output based on what is learned from data and examples. Automatic analyses of attacks and security events, such as spam mail, user identification, social media analytics, and attack detection may be performed efficiently using machine learning [1]. The most common methods for machine learning are supervised, unsupervised, semi-Supervised and Reinforcement Learning. Supervised learning is based on identified data, unsupervised learning is based on unidentified data, and semi-Supervised learning is based on both. In order to categorise or discover patterns by a classifier, traditional machine learning approaches require the processing of natural raw data, which depends on effective feature extraction. This is where deep learning comes in. Deep learning is a technique of artificial intelligence inspired by neural networks, which can analyse unstructured and unlabelled data. By stacking layers of artificial neurons, deep learning models can handle increasingly complex functions. It excels at learning abstract representations at multiple levels. Deep neural networks can extract meaningful features from raw data, enabling them to learn and classify information effectively. By concentrating on the technologies, methodologies and implementation of network security measures, this paper provides an overview of Deep Learning intrusion detection technologies.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i04.040 ISSN: 2581-4621

The remainder of the paper is organized as follows: Section 2 addresses the concept of intrusion detection systems. Section 3 is about the different Deep Learning based intrusion detection systems, while section 4 will be concluding this paper.

2. Intrusion Detection

The Intrusion Detection is a method to monitor network traffic and events on computers for the detection of unexpected events. This type of network security is designed for the detection and recognition of risks before services are lost, unlawful access granted or data lose. Depended on the activity, Intrusion Detection System (IDS) can be of two types: a Network Based Intrusion Detection System (NIDS) and a Host Based Intrusion Detection System (HIDS). Hybrid detection is a system that combines the best of both NIDS and HIDS. The techniques for detecting intrusions have been classified into anomaly detection methods and misuse detection methods.

2.1. Anomaly detection

The model operates under the assumption that uncommon network traffic has a low likelihood of occurrence, and it can be accurately distinguished from normal traffic. By utilizing unsupervised learning and statistical learning-based anomaly detection algorithms, it becomes possible to identify novel and previously unknown attacks effectively.

2.2. Misuse detection

The approach utilizes a signature technique, where detection is performed by comparing network activity against known attack signatures while continuously monitoring the IDS for potential threats. This strategy relies on supervised learning and can detect unauthorized or suspicious behavior, serving as a defense against similar attacks.

2.3. Attack classification

Denial of Service (DoS) attacks are a prevalent form of network resource attack that disrupts network services for all users. Attackers employ diverse methods to exhaust network resources and render services inaccessible. Probe, involves scanning all devices within a network to identify open ports that can be exploited to gain unauthorized network access. In Remote to User (R2U) attacks, the attacker sends packets to different devices on the network with the aim of gaining access as a local user. Worms are malicious applications that can self-replicate from one device to another, causing widespread damage. User to Root (U2R) attacks involve intruders attempting to gain access to network resources by employing various methods and techniques to escalate their privileges as a local user.

3. Intrusion Detection Systems using Deep Learning

This section explains how researchers utilized deep learning techniques to develop an Intrusion Detection System (IDS).

3.1. Deep Belief Networks-Based Attack Detection Methods

The Deep Belief Network (DBN) is a stacked Restricted Boltzmann Machine (RBM). RBM is a neural network structure that comprises visible and hidden neurons, forming an undirected graph model. RBM's random structure lends itself well to training DBN layer by layer. In the context of intrusion detection, many attempts have been made to utilize Deep Belief Networks (DBN). However, several challenges still persist, including the presence of redundant information and the potential for getting trapped in local maxima.

To address these issues, Zhao et al. [2] propose a novel approach that combines the strengths of DBN and PNN (Probabilistic Neural Network) for intrusion detection. Their methodology involves rescaling the original input data using the nonlinear descriptive capabilities of DBN, which effectively reduces the dimensionality while preserving the essential characteristics of the original data. Additionally, they utilize the particle swarm optimization algorithm to decrease the quantity of hidden nodes in each layer of the network. Furthermore, they introduce PNN to classify the low-dimensional information. Through experiments conducted on the dataset KDDCup99, the authors demonstrate that their proposed approach has partially resolved the aforementioned challenges. By integrating DBN and PNN, they have achieved improved intrusion detection performance, addressing the issues of redundant information and local maxima to some extent.

DOI:10.46647/ijetms.2023.v07i04.040 ISSN: 2581-4621

Alrawashdeh and Purdy [3] address the challenge of real-time attack detection in intrusion detection systems by proposing a DBN-based anomaly detection method. Their approach consists of a single-hidden layer restricted Boltzmann machine (RBM) and a fine-tuning layer built using a logistic regression classifier. Despite its simplicity, their DBN design achieves both fast processing times (8s CPU time per instance) and high performance (reported accuracy of 97.7%) when tested on the KDDCup99 dataset. The method proposed by the authors allows the use of deep learning methods for detecting attacks on resource-constrained platforms, such as drones, personal computers, and cell phones. This expands the potential usage scenarios for such methods and enables real-time intrusion detection even in resource-constrained environments.

In their study, Alom et al. [4] introduce a platform that leverages Deep Belief Networks (DBN) to detect intrusion attempts in network traffic. Their system begins by employing standardised methods and digital encoding to choose relevant characteristics. Subsequently, DBN is used to categories network intrusion by labelling each feature vector with a class label. Through experiments and analysis, the authors demonstrate that their system is not only capable of detecting attacks, but also rightly identifying and classifying network activities. Importantly, this classification is achieved even when the available data sources are limited, nonlinear and incomplete. The proposed platform showcases the effectiveness of using DBN in understanding intrusion attacks in network traffic and highlights its potential for improving network security.

3.2. Convolutional Neural Network-Based Attack Detection Methods

CNN, or Convolutional Neural Network, is a widely used technique in the field of deep learning. It is characterized by its depth structure and convolution computation. The CNN architecture is commonly employed due to its effectiveness and efficiency. It uses a multilayer perception variation architecture and requires little preprocessing.

A CNN's basic structure consists of layers of input and output as well as several hidden layers, including convolution, pooling, and complete connection layers. CNN has the benefit of requiring less preprocessing and being independent of feature design based on past information. These qualities make CNN a powerful tool for classification tasks compared to other algorithms.

Yang and Wang [5] proposed the model for wireless network intrusion detection based on ICNN (Improved Convolutional Neural Network) to address the diversity attack in wireless network traffic and improve the ability to detect malicious intrusions. Their method uses an enhanced Convolutional Neural Network (CNN) to process the data from network traffic and to obtain model convergence. CNN automatically pulls high-level characteristics from low-level incursion traffic data while optimising network parameters using the algorithm of random gradient descent.

Experimental results on the KDDCup99 dataset demonstrated that their proposed method achieved a lower false positive, providing a significant advantage over previous methods for wireless network intrusion detection.

3.3. Recurrent Neural Network -Based Attack Detection Methods

RNN, or Recurrent Neural Network, is a neural network architecture that includes a memory feature to retain previous information. This characteristic enables RNNs to effectively handle time-series data. However, RNNs face challenges like explosion or gradient disappearance, which can hinder their ability to capture long-term dependencies. To address these issues, researchers have introduced LSTM (Long Short-Term Memory) and GRU (Gated Recurrent Unit) models. These models incorporate gate mechanisms and memory cells to effectively maintain long-term relationships and retain crucial information throughout the information flow.

Le et al. [6] use the LSTM method to detect intrusions. They concentrate on choosing the best optimizer for LSTM-based gradient descent optimisation. Six popular optimisation techniques are compared, including Adagrad, RMSprop, Adadelta, Adam, Nadam and Adamax. The LSTM model with the Nadam optimizer turns out to be the most efficient for intrusion detection, according to their tests.

To improve the accuracy of intrusion detection systems, Staudemeyer [7] advises taking into account the time-series features of known malicious behavior and network traffic. They use Long Short-Term Memory (LSTM) for intrusion detection to support the theory by making use of LSTM's capacity to simulate long-term dependency. In order to balance computational expense and detection efficiency, they create a four-memory block network with each block comprising two cells.

Kim et al. [8] utilize the Long Short-Term Memory (LSTM) architecture for intrusion detection, benefiting from its ability to handle long-term dependencies and mitigate the vanishing gradient issue during training. Through

DOI:10.46647/ijetms.2023.v07i04.040 ISSN: 2581-4621

experiments, they determine the size of the hidden layer and learning rate to be 80 and 0.01, respectively. The LSTM model they created, however, displays a greater false detection rate after training using the KDDCup99 dataset as compared to Staudemeyer's method [7]. The outcomes of the experiments show that the LSTM model proposed, outperforms previously published methods. LSTM's capability to learn and correlate continuous connection records in a time-varying manner contributes to its superior performance in detecting attacks.

3.4. Autoencoder -Based Attack Detection Methods

An autoencoder is a neural network-based data compression algorithm that compresses input data into a lower-dimensional feature space and then reconstructs it into the output. It is commonly used for outlier detection and dimension reduction, as it can effectively learn representations of the input data. In the context of anomaly detection in cybersecurity, autoencoders are employed to capture abnormal behaviors by representing them in the compressed feature space. This approach provides the advantage of dynamically representing unknown categories of attacks, enabling the detection of novel and previously unseen threats.

In [9], a deep learning classification model was proposed for Intrusion Detection Systems (IDS) using the NSL-KDD and KDDCup99 datasets. The authors introduced a deep learning method utilizing the Non-symmetric Deep Autoencoder (NDAE), an unsupervised learning technique. Their model demonstrated faster training times compared to Deep Belief Networks (DBN) and achieved a 5% improvement in accuracy compared to pure Autoencoders. The proposed model consisted of two NDAEs, each with three concealed layers, and they were connected using a Random Forest (RF) method. To evaluate their approach, the authors used the NSL-KDD and KDDCup99 datasets. Their findings revealed that their proposed model outperformed other machine learning algorithms like RF and Support Vector Machines (SVM) in terms of accuracy and false positive rate.

In [10], Farahnakian et al. employs deep stacked autoencoders to overcome the issue of imbalanced distribution in gathered network raw data. They concentrate on building classification models for identifying aberrant behaviors by extracting informative and relevant feature representations. Four autoencoders that were trained greedy layer wise make up the proposed network design. Experimental results on the KDDCup99 dataset demonstrate the effectiveness of their approach, achieving a high accuracy of 94.71% in abnormal detection, even in the presence of unbalanced data. By leveraging deep stacked autoencoders, the authors successfully tackle the issue of unbalanced data distribution and showcase the potential of their approach in detecting abnormal network behaviors.

Paper [11] proposes a network intrusion detection approach based on Self-taught Learning (STL) which uses a stacked autoencoder (SAE) to learn the features from the input data. The learned features are then used to train a Softmax Regression (SMR) classifier for classification. The proposed approach is evaluated on the NSL-KDD dataset and compared with previous works based on various metrics. The results show that the proposed approach achieves a classification accuracy rate of more than 98% for all types of classification. The proposed approach is effective for network intrusion detection and its performance is comparable to the best results obtained in various previous works

4. Performance Evaluation and Comparisons

The findings of attack detection employing the various techniques outlined in Section 3 are shown in Table 1 and Table 2 in detail. The assessments in the majority of the stated approaches concentrate on accuracy, precision, and F1-score from the many metrics available. These measurements are commonly used to assess the performance of intrusion detection methods. Accuracy provides an overall assessment of correct classifications, precision evaluates the accuracy of attack classifications, and F1-score balances precision and recall. By considering these evaluations, the methods can be compared and analyzed based on their effectiveness in detecting and classifying attacks. Fig. 1 and Fig. 2 shows the statistical analysis of discussed methods on KDDCup99 dataset and NSL-KDD dataset respectively.

According to the performed literature comparison, the rank of detection performance of deep learning methods follows the order DBN, LSTM, CNN, and AE, in descending. DBN achieves the highest performance because of its ability to handle large amounts of unlabeled data through multiple layers. LSTM may outperform CNN due to its utilization of temporal information for more accurate modeling. On the other hand, AE's performance may suffer when dealing with extensive unlabeled data, as it might lack sufficient prior knowledge or the necessary layers to capture the inherent complexity effectively.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i04.040 ISSN: 2581-4621

Because of their completeness, the accuracy (ACC) values obtained by the given techniques serve as the initial assessment index. Interestingly, the greatest performance obtained on the KDDCup99 dataset (99.14% by Zhao et al. [2]) is greater than that obtained on the NSL-KDD dataset (98.3% by Javaid et al. [11]), showing that NSL-KDD is more difficult due to the existence of unknown instances in the testing dataset.

The effectiveness of AE-based approaches varies. The enhanced AE-based approaches generally outperform traditional AE-based methods. This discrepancy can be attributed to the potential loss of important information during the compression process in the AE structure. The improved AE methods are better able to capture essential and informative aspects of the input data through additional design enhancements. Similarly, LSTM-based methods demonstrate better performance than RNN-based methods. This is because the structural design of memory cells and gates in LSTM models allows them to effectively maintain long-term information and model long-term relationships. In short, the enhanced AE-based methods and LSTM -based methods exhibit superior performance compared to their traditional counterparts, showcasing the importance of intelligent design choices in capturing and modeling essential information.

Researchers have proposed numerous RNN- and DBN-based methods for attack detection, and we can consider DBN-based methods as standard unsupervised algorithms, while RNN-based methods (LSTM) can be viewed as supervised algorithms. By comparing these two groups, we can assess their respective advantages and disadvantages. RNN-based methods, with their ability to retain information from previous time steps and incorporate temporal information into the classification process, can achieve more accurate classification. However, RNN models require a substantial number of training instances to demonstrate their power, which can be challenging to obtain, particularly for unknown or rare attacks. On the other hand, DBN-based methods have the capability to automatically discover patterns and features in input data without relying on labeled data. The unsupervised nature of DBN networks also reduces the risk of overfitting, as they undergo a pretraining procedure that learns from unlabeled data. This characteristic aligns well with the real-world network security environment, where anomalies and attacks may be unknown or not well-defined. Additionally, DBN models are relatively easier to train, converge faster, and have lower computational requirements compared to deep structures like CNNs. Consequently, unsupervised learning methods, such as DBN, are likely to produce better classification results, particularly in scenarios involving small, imbalanced, or redundant datasets. In summary, RNN-based methods excel at incorporating temporal information for accurate classification but require sufficient training instances, while DBN-based methods exhibit the advantages of unsupervised learning, such as automatic feature discovery and resilience to overfitting, making them well-suited for network security applications.

DL	Method	ACC (%)	PR (%)	FS
DBN	Zhao et al. [2]	99.14	93.25	-
DBN	Alrawashdeh and Purdy [3]	97.70	97.81	0.975
LSTM	Le et al. [6]	97.54	98.95	-
LSTM	Kim et al. [8]	96.93	98.80	-
LSTM	Staudemeyer [7]	93.85	-	-
CNN	Yang and Wang [5]	95.36	95.55	0.930
Sparse AE	Shone et al. [9]	97.85	99.99	0.980
Sparse AE	Farahnakian and Heikkonen [10]	94.71	94.53	-

Table 1: Quantitative evaluation of the stated attack detection approaches employing different deep learning structures on the KDDCup99 dataset.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 3 Volume No.7 May - June – 2023
DOI:10.46647/ijetms.2023.v07i04.040 ISSN: 2581-4621

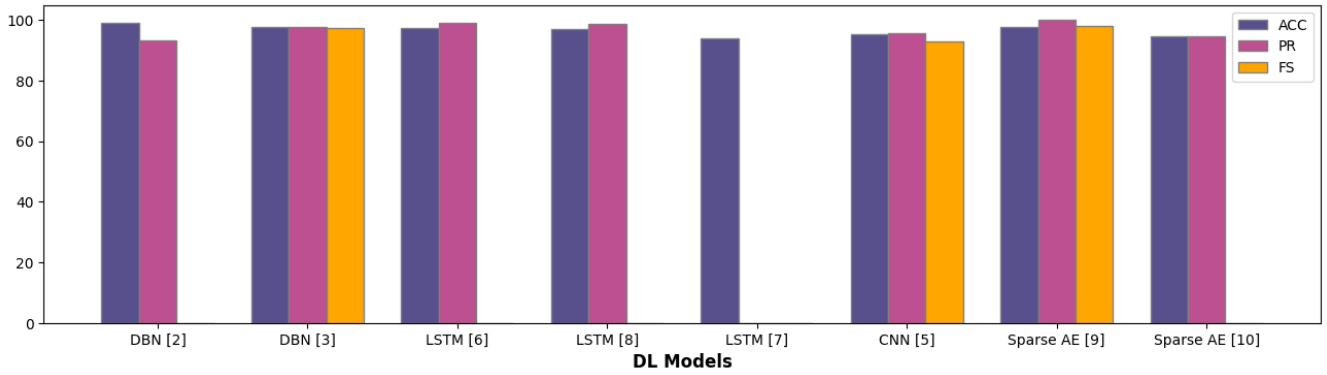

Fig. 1: Statistical analysis of the stated deep learning structures on the KDDCup99 dataset

DL	Method	ACC (%)	PR (%)	FS
Sparse AE	Javaid et al. [11]	98.30	-	0.990
DBN	Alom et al. [4]	97.50	-	-
Sparse AE	Shone et al. [9]	89.22	92.97	0.910

Table 2: Quantitative evaluation of the stated attack detection approaches employing different deep learning structures on the NSL-KDD dataset.

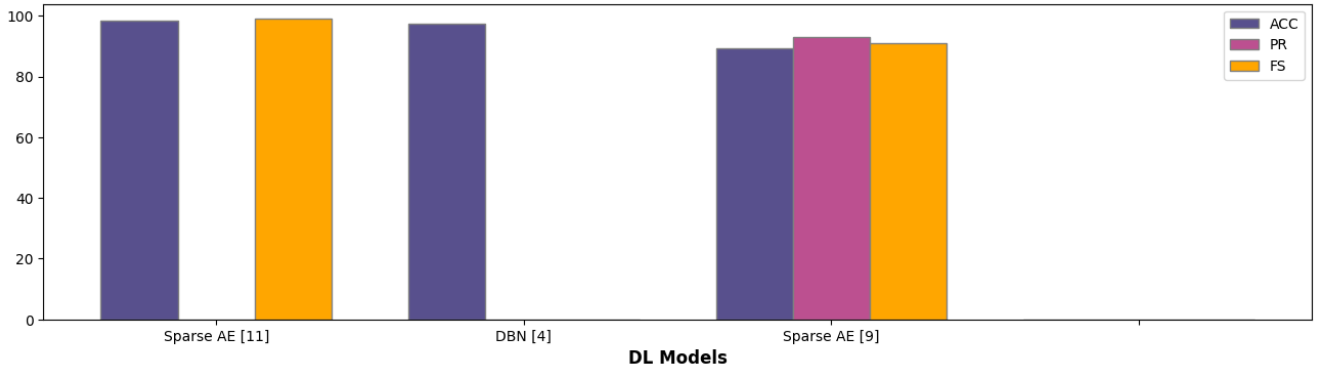

Fig. 2: Statistical analysis of the stated deep learning structures on the NSL-KDD dataset

CONCLUSION

The need of implementing advanced cybersecurity solutions cannot be emphasised in a rapidly developing digital world where malicious intelligence and cyber threats are on the rise. The intrusion detection systems are becoming an essential part of our daily life because they protect against any threats. However, it is difficult to develop an intrusion detection system that can effectively recognise and react to the wide range of threats and attacks. The advancement of intrusion detection systems is greatly aided by these diligent academics' research efforts. They offer priceless insights for boosting these systems' detection and reaction capacities, enhancing their capacity to defend against a variety of dangers in our networked society.

References

[1] D. I. Edeh, "Network intrusion detection system using deep learning technique," M.S. thesis, Dept. Comput., Univ. Turku, Turku, Finland, 2021.

[2] G. Zhao, C. Zhang, and L. Zheng, “Intrusion Detection Using Deep Belief Network and Probabilistic Neural Network,” 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC), Guangzhou, China, 2017, pp. 639-642.

DOI:10.46647/ijetms.2023.v07i04.040 ISSN: 2581-4621

[3] K. Alrawashdeh and C. Purdy, "Toward an Online Anomaly Intrusion Detection System Based on Deep Learning," 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, 2016, pp. 195-200.
[4] M. Z. Alom, V. Bontupalli and T. M. Taha, "Intrusion detection using deep belief networks," 2015 National Aerospace and Electronics Conference (NAECON), Dayton, OH, USA, 2015, pp. 339-344.
[5] H. Yang and F. Wang, "Wireless Network Intrusion Detection Based on Improved Convolutional Neural Network," in IEEE Access, vol. 7, pp. 64366-64374, 2019.
[6] T. -T. -H. Le, J. Kim and H. Kim, "An Effective Intrusion Detection Classifier Using Long Short-Term Memory with Gradient Descent Optimization," 2017 International Conference on Platform Technology and Service (PlatCon), Busan, Korea (South), 2017, pp. 1-6.
[7] R. C. Staudemeyer, "Applying long short-term memory recurrent neural networks to intrusion detection," South African Computer Journal, vol. 56, no. 1, pp. 136-154, 2015.
[8] J. Kim, J. Kim, H. L. Thi Thu and H. Kim, "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection," 2016 International Conference on Platform Technology and Service (PlatCon), Jeju, Korea (South), 2016, pp. 1-5.
[9] N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, Feb. 2018.
[10] F. Farahnakian and J. Heikkonen, "A deep auto-encoder based approach for intrusion detection system," in Proceedings of 2018 20th International Conference on Advanced Communication Technology (ICACT), IEEE, Chuncheon, South Korea, pp. 178-183, Jul. 2018.
[11] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies (formerly BIONETICS), pp. 21-26, New York, NY, USA, Dec. 2016.
[12] Y. Li, R. Ma, and R. Jiao, “A hybrid malicious code detection method based on deep learning,” International Journal of Security and Its Applications, vol. 9, no. 5, pp. 205–216, 2015.
[13] J. A. Abraham and V. R. Bindu, "Intrusion Detection and Prevention in Networks Using Machine Learning and Deep Learning Approaches: A Review," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2021, pp. 1-4 .
[14] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, “Deep learning approach for intelligent intrusion detection system,” IEEE Access, vol. 7, pp. 41525-41550,2019.
[15] Y. Wu, D. Wei, and J. Feng, "Network attacks detection methods based on deep learning techniques: a survey," Security and Communication Networks, vol. 2020, Article ID 8872923, pp. 1-17, August 2020.