A Review of Intrusion Detection using Deep Learning

Levina Bisen
M.Tech. Scholar
Department of CSE
Vaishnavi Institute of Technology and Science
Bhopal (M.P), India
levisbisen@gmail.com

Sumit Sharma
Professor
Department of CSE
Vaishnavi Institute of Technology and Science
Bhopal (M.P), India
sumit_sharma782022@yahoo.co.in

***Abstract*—As network applications grow rapidly, network security mechanisms require more attention to improve speed and accuracy. The development of new types of intruders poses a serious threat to network security: although many tools for network security have been developed, the rapid growth of intrusion activity remains a serious problem. Intrusion Detection Systems (IDS) are used to detect intrusive network activity. Preventing and detecting unauthorized access to a computer is an IT security concern. Therefore, network security provides a measure of the level of prevention and detection that can be used to avoid suspicious users. Deep learning has been used extensively in recent years to improve network intruder detection. These techniques allow for automatic detection of network traffic anomalies. This paper presents literature review on intrusion detection techniques.**

Keywords: Anomaly, Intrusion Detection System, Supervised, Unsupervised, Web Security

I. INTRODUCTION

Nowadays, the development of the Internet and the use of computer systems have led to a huge electronic transformation of data, with many issues such as information security, privacy, and confidentiality. Significant progress has been made in improving the security of IT systems. However, the security, confidentiality and confidentiality of electronic systems are potentially important problems in computer systems. In fact, no system currently available in the world is 100% secure. In addition, we always can notice that there are huge Attack scenarios. Basically, if a new signature is found on the database of signatures, then the behavior will be considered as an attack [1, 2].

And, it can be exploited by either non authorized or authorized users. Among these tools is the intrusion detection systems (IDS) which allow us to monitor a range of computer systems: an information system, a network or a cloud computing. These IDS detect intrusions and defined as attempts to break the security objectives such as confidentiality, integrity and availability and non-repudiation. We will include the different approaches currently proposed by others on IDS system, network and cloud computing based vulnerabilities in most computer systems. And, it can be exploited by either non authorized or authorized users.

Table 1: Attack types with description

Attacks Category	Description	TCP/IP Layer
DoS	Denial-of-service (fake address generate)	Application Layer
DoS	Denial-of-service (fake address generate)	Transport Layer
U2R	Unauthorized access to local super user (root) privileges	Application Layer
R2L	Unauthorized access from a remote machine	Application Layer
R2L	Unauthorized access from a remote machine	Transport Layer
Probe	Surveillance and other probing	Application Layer
Probe	Surveillance and other probing	Transport Layer
DoS	Denial-of-service (fake address generate)	Transport Layer

It is based on the comparison between the observed behavior and corresponding reference signatures or known each signature describes a very specific attack and each attack can be detected by one or a sequence of events obtained by one or more sensors, collection of information. This approach is used to classify attacks into: attacks that can come from either a host (e.g., audit records, track of command execution, etc.) or a network. This means that their signatures exist in the database, and the databases are frequently updated in order to increase their effectiveness of detections.

In general, IDS generate an alert if there is a deviation between normal and observed behavior [3]-[8]. The basic

 DOI: https://doi.org/10.24113/ijosthe.v7i4.133

idea of the approach is that to detects if a user has an abnormal behavior when comparing his/her usual uses. Using the profile generated from past events and compared it to the current collector profile [9]-[12]. However, this approach can give many false alarms as it might not be able to detect some attacks.

II. RELATED WORK

Sufyan T. Faraj et al. [2] proposed the intrusion detection model using BPANN for classification of anomalous network traffic from normal traffic and achieved the accuracy of about 93%. Anomaly detection system based on back-propagation Multi-Layer Perceptron (MLP) to identify normal users' profile was proposed by Ryan et al. [3]. Their MLP model evaluates the users' commands for possible intrusions at the end of each log session. The top 100 important commands used by the user throughout the session was used to determine the user's behavior. They used a 3-layer MLP model with two hidden layers and found that their MLP model was able to correctly identify 22 cases out of 24.

Similarly, a method primarily based intrusion detection approach that gives the flexibility to generalize from previously determined behavior to acknowledge future unseen behavior was proposed by Ghosh et al. [4]. Their framework employs artificial neural networks (ANNs) and may be used for each anomaly findon so as to find novel attacks and misuse detection so as to detect best-known attacks and their variations.

Meng et al. [8] compared the ANN, SVM and DT schemes to detect anomalies in a unified environment and concluded that J48 algorithm performed better than the other two schemes. The detection rate of species with frequent weak attacks (U2R, R2L) was also high.

Sumaiya Thaseen Ikram et al. [9] roposed an intrusion detection model using chi-squared feature selection and the Multi Class Support Vector Machine (SVM). To optimize the kernel parameter of the radial basis function, a parameter optimization technique is used, namely gamma, represented by "!" And constant over-regulation "C". These are the two important parameters required by the SVM model. The main idea behind this model is to create a multi-class SVM that has not yet been adopted for IDS in order to reduce training and testing times and increase the accuracy of individual classification of network attacks.

Manjula et al. [10] roposed a classification and prediction model for intrusion detection that was created using classification algorithms for machine learning, namely logistic regression, Gaussian Naive Bayes, Support Vector Machine, and Random Forest. An experimental result shows that Random Forest Classifier performs the other methods to determine if the traffic is normal or if it is an attack.

Feng et al. [13] proposed extreme learning machines with SVMs to detect network intrusion and classified as normal or abnormal behavior.

Kuang et al. [15] proposed intrusion detection system by combining principal component analysis (PCA), Genetic algorithm (GA) with SVM. The result analysis shows the average false alarm rate of 1.03%.

Gogoi, Bhattacharyya et al. [16] proposed real time network intrusion detection system that was designed in multiple layers and achieved false positive rate of 3.4% on KDD Cup dataset.

Wathiq Laftah Al-Yaseen et al. [17] proposes hybridization of machine learning approach such as SVM and ELM to improve efficiency of detection system. The result was implemented on KDD Cup 1999 dataset and achieved accuracy of 95.75%.

III. MEASURABLE CHARACTERISTICS OF IDSS

Characteristics of IDSs can be measured quantitatively. Some of these characteristics are:

A. Coverage

Evaluating the detection of intrusion detection systems is a difficult task with many consequences. The range of any intrusion detection system depends on the attacks that IDS can detect under ideal conditions. The number of dimensions that make up each attack makes assessment difficult. Each attack has a specific goal and works against certain software.

Attacks can also target a specific version of a protocol or a specific operating mode. Several websites may find some attacks more significant than others, which has a significant impact on the evaluation. For example, e-commerce websites may be very interested in finding distributed denial of service attacks, while military websites may pay close attention to surveillance attacks.

B. Probability of False Alarms

A false alarm is a warning caused by normal harmless background traffic. The probability of false alarms determines the percentage of false alarms generated by an IDS in a given environment during a certain period of time. Measuring false alarms can be difficult because an IDS can have different percentages of false alarms in different network environments. In addition, the various aspects associated with host activity and network traffic can make it difficult to determine which aspects cause false alarms.

In addition, configurable IDS that can be set to reduce the rate of false alarms make it difficult to determine the correct configuration of an IDS for a particular false alarm test. A noteworthy point is that there is a school of thought in the field of intrusion detection which believes that there are no false alarms. Each alarm is assumed to contain information in a well-designed system. For example, you can see some packages that look like a test for vulnerable systems. The

administrator may want to know, even if it's not yet a problem and isn't actually the beginning of an attack. In this diagram, the system only reports alarms for important events for administrators, which significantly reduces the number of false alarms.

C. Probability of Detection

This measure, also known as the success rate, determines the frequency of attacks that have been correctly identified by an IDS in a given environment for a period of time. The number of attacks used in the IDS test largely determines the result of this measurement. Since the probability of detection is linked to the percentage of false alarms, we can repeat what has already been said about the configurable IDs and conclude that it is difficult to find the right configuration for a specific success rate test.

IDS ability is to detect attacks is tied to its ability to identify attacks by marking them or assigning them to known categories. The probability of detection and the probability of false alarms play the most important role in the evaluation of intrusion detection algorithms. Different methods are then used to visually show how a given IDS behaves in relation to these two measures.

One of the most used methods is the operating characteristic curve of the receiver or ROC curve. The ROC curve is a graph of the probability of detection relating to the probability of false alarms. This can be achieved by varying the detection thresholds and maintaining a range of values. The x axis of the ROC graph shows the percentage of false alarms generated during a test, while the y axis shows the percentage of attacks detected for a certain percentage of false alarms.

D. Ability to Handle Stressful Network Conditions

This property shows how an IDS works when there is a lot of traffic. Attackers can send large amounts of data beyond the processing capacity of the host's network or intrusion detection system. Most IDSs should eliminate packets as traffic increases, which can lead to some attacks on deleted packets disappearing. It is up to the evaluation team to determine the threshold at which the performance of IDS and the monitored system significantly decreases [15].

E. Ability to Detect Novel Attacks

This feature shows how much an IDS is able to detect attacks that have not yet taken place. It goes without saying that this measure applies to intrusion detection systems designed to detect unknown attacks such as anomaly and specification-based systems. Signature-based systems are not subject to this measure because signature databases contain known attack patterns [16].

IV. DEEP LEARNING AND INTRUSION DETECTION

Deep learning models consist of diverse deep networks. Among them, deep brief networks (DBNs), deep neural networks (DNNs), convolutional neural networks (CNNs), and recurrent neural networks (RNNs) are supervised learning models, while autoencoders, restricted Boltzmann machines (RBMs), and generative adversarial networks (GANs) are unsupervised learning models. The number of studies of deep learning-based IDSs has increased rapidly from 2015 to the present. For large datasets, deep learning methods have a significant advantage over shallow models. In the study of deep learning, the main emphases are network architecture, hyperparameter selection, and optimization strategy.

A. Autoencoder

An autoencoder contains two symmetrical components, an encoder and a decoder, as shown in Figure 1. The encoder extracts features from raw data, and the decoder reconstructs the data from the extracted features. During training, the divergence between the input of the encoder and the output of the decoder is gradually reduced. When the decoder succeeds in reconstructing the data via the extracted features, it means that the features extracted by the encoder represent the essence of the data. It is important to note that this entire process requires no supervised information. Many famous autoencoder variants exist, such as denoising autoencoders and sparse autoencoders.

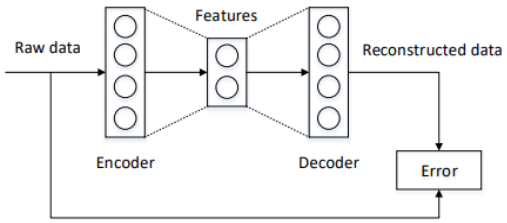

Figure 1: The structure of an autoencoder

B. Restricted Boltzmann Machine (RBM)

An RBM is a randomized neural network in which units obey the Boltzmann distribution. An RBM is composed of a visible layer and a hidden layer. The units in the same layer are not connected; however, the units in different layers are fully connected, as shown in Figure 2. where vi is a visible layer, and hi is a hidden layer. RBMs do not distinguish between the forward and backward directions; thus, the weights in both directions are the same. RBMs are unsupervised learning models trained by the contrastive divergence algorithm, and they are usually applied for feature extraction or denoising.

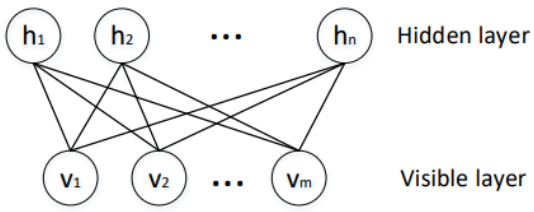

Figure 2: The structure of the RBM

C. Deep Brief Network (DBN)

A DBN consists of several RBM layers and a SoftMax classification layer, as shown in Figure 3. Training a DBN involves two stages: unsupervised pretraining and supervised fine-tuning. First, each RBM is trained using greedy layer-wise pretraining. Then, the weight of the softmax layer are learned by labeled data. In attack detection, DBNs are used for both feature extraction and classification [20–22].

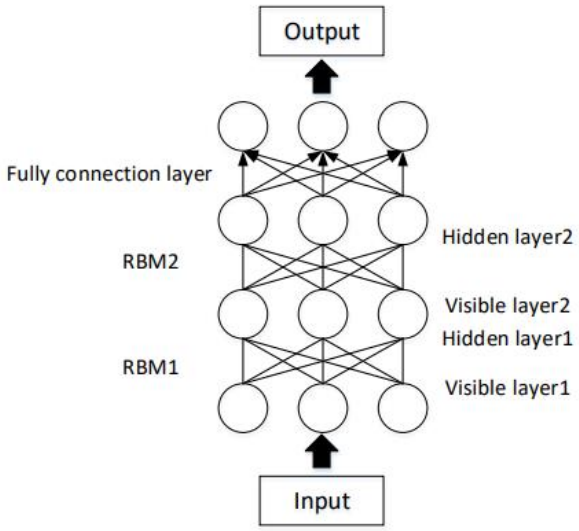

Figure 3: The structure of the DBN

D. Convolutional Neural Network (CNN)

CNNs are designed to mimic the human visual system (HVS); consequently, CNNs have made great achievements in the computer vision field. A CNN is stacked with alternate convolutional and pooling layers, as shown in Figure 4. The convolutional layers are used to extract features, and the pooling layers are used to enhance the feature generalizability. CNNs work on 2-dimensional (2D) data, so the input data must be translated into matrices for attack detection.

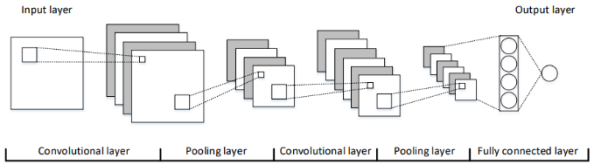

Figure 4: The structure of a CNN

E. Recurrent Neural Network (RNN)

RNNs are networks designed for sequential data and are widely used in natural language processing (NLP). The characteristics of sequential data are contextual; analyzing isolated data from the sequence makes no sense. To obtain contextual information, each unit in an RNN receives not only the current state but also previous states. The structure of an RNN is shown in Figure 5. Where all the W items in Figure 8 are the same. This characteristic causes RNNs to often suffer from vanishing or exploding gradients. In reality, standard RNNs deal with only limited-length sequences. To solve the long-term dependence problem, many RNN variants have been proposed, such as long short-term memory (LSTM), gated recurrent unit (GRU), etc.

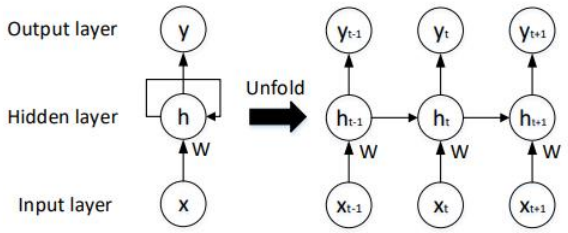

Figure 5: The structure of an RNN

F. Generative Adversarial Network (GAN)

A GAN model includes two subnetworks, i.e., a generator and a discriminator. The generator aims to generate synthetic data similar to the real data, and the discriminator intends to distinguish synthetic data from real data. Thus, the generator and the discriminator improve each other. GANs are currently a hot research topic used to augment data in attack detection, which partly ease the problem of IDS dataset shortages. Meanwhile, GANs belong to adversarial learning approaches which can raise the detection accuracy of models by adding adversarial samples to the training set.

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 amount of items in order to be trained. Process is placed on millions of data points. Deep learning is learns 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. Some research works related to deep learning in field of intrusion detection are summarized below in table I.

Table I: Contribution of Deep Learning in field of IDS

Technique	Attack Types	Metrices	Ref
Recurrent Neural Network	DoS, R2L, U2R and probe	Detection rate and false alarm rate	[22]
	DoS, R2L, U2R and probe	Detection rate and false alarm rate	[23]
	HTTPWeb, unknown TCP, secure web, misc application, SMTP, IMAP, Flowgen, ICMP, DNS, IRC	Error rate, accuracy, precision, recall, F1- score and AUC	[24]
Deep Belief Network	Android malware	Precision, recall and F1-score	[25]
Stacked autoencoder	DoS, R2L, U2R and probe	Detection rate and false alarm rate	[26]
Stacked denoising autoencoders	PC malware	Accuracy, precision, recall and F1-score	[27]
Convolutional Neural-Learning Classifier System (CN-LCS)	Abnormal queries	Accuracy	[28]
Deep Neural Network with Support Vector Machine and Clustering Technique	Dos, Prob, U2R, R2L	Error rate, accuracy, recall	[29]

V. CONCLUSION

In this paper, a detailed survey of intrusion detection system methodologies, types, and technologies with their advantages and limitations. Several machine learning techniques that have been proposed to detect attacks are reviewed. However, such approaches may have the problem of generating and updating the information about new attacks and yield high false alarms or poor accuracy. In addition, the most popular datasets used for IDS research have been explored and their data collection techniques, evaluation results and limitations have been discussed. As normal activities are frequently changing and may not remain effective over time, there exists a need for newer and more comprehensive datasets that contain wide-spectrum of malware activities.

REFERENCES

[1] A. Kartit, A. Saidi, F. Bezzazi, M. El Marraki & A. Radi, "A new approach to intrusion detection system," Journal of Theoretical and Applied Information Technology, Vol. 36, No. 2, 2012, pp. 284-289.

[2] Sufyan T Faraj Al-Janabi, Hadeel Amjed Saeed, "A neural network based anomaly intrusion detection system", IEEE, 2011.

[3] J. Ryan, M. Lin, and R. Miikkulainen, "Intrusion Detection with Neural Networks," Conference in Neural Information Processing Systems, 943–949.

[4] A. K. Ghosh and A. Schwartzbard, "A Study in Using Neural Networks for Anomaly and Misuse Detection," Conference on USENIX Security Symposium, Volume 8, pp. 12–12, 1999.

[5] P. L. Nur, A. N. Zincir-heywood, and M. I. Heywood, "Host-Based Intrusion Detection Using Self-Organizing Maps," in Proceedings of the IEEE International Joint Conference on Neural Networks, pp. 1714–1719, 2002.

[6] K. Labib and R. Vemuri, "NSOM: A Real-Time Network-Based Intrusion Detection System Using Self-Organizing Maps," 2000.

[7] Sharma, R.K., Kalita, H.K., Issac, B., "Different firewall techniques: a survey", International Conference on Computing, Communication and Networking Technologies (ICCCNT), IEEE, 2014.

[8] Meng, Y.-X., "The practice on using machine learning for network anomaly intrusion detection", International Conference on Machine Learning and Cybernetics (ICMLC), Vol. 2, IEEE, 2011.

[9] Sumaiya Thaseen Ikram, Aswani Kumar Cherukuri, "Intrusion detection model using fusion of chi-square feature selection and multi class SVM", Journal of King Saud University –Computer and Information Sciences, 2016.

[10] Manjula C. Belavagi and Balachandra Muniyal, "Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection, Procedia Computer Science", Elsevier, 2016.

[11] Saad Mohamed Ali Mohamed Gadal and Rania A. Mokhtar, "Anomaly Detection Approach using Hybrid Algorithm of Data Mining Technique", International Conference on Communication, Control, Computing and Electronics Engineering, IEEE, 2017.

[12] Ibrahim, H. E., Badr, S. M., & Shaheen, M. A., "Adaptive layered approach using machine learning techniques with gain ratio for intrusion detection systems", International Journal of Computer Applications, Vol. 56, issue 7, pp. 10–16, 2012.

[13] Wen Feng, Qinglei Zhang, Gongzhu Hu, Jimmy Xiang Huang, "Mining network data for intrusion detection through combining SVMs with ant colony networks", Elsevier, Vol 37, pp 127-140, 2014.

[14] Deshpande, A., & Sharma, R., "Anomaly Detection using Optimized Features using Genetic Algorithm and MultiEnsemble Classifier", International Journal Online of Sports Technology & Human Engineering(IJOSTHE), 5(6), 2018. Retrieved from https://ijosthe.com/index.php/ojssports/article/view/79.

[15] Kuang, F., Xu, W., & Zhang, S., "A novel hybrid KPCA and SVM with GA model for intrusion detection", Applied Soft Computing Journal, Vol. 18, pp. 178–184, 2014.

[16] Prasanta Gogoi, D.K. Bhattacharyya, B. Borah1 and Juga, K. Kalita, "MLH-IDS: A Multi-Level Hybrid Intrusion Detection Method", The Computer Journal, Vol. 57 issue 4, pp. 602-623, 2014.

[17] Wathiq Laftah Al-Yaseen , Zulaiha Ali Othman ,Mohd Zakree Ahmad Nazri, "Multi-Level Hybrid Support Vector Machine and Extreme Learning Machine Based on Modified K-means for Intrusion

Detection System", International Journal in Expert Systems With Applications, Elsevier, 2017.
[18] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in 2009 IEEE symposium on computational intelligence for security and defense applications, 2009, pp. 1–6.
[19] Nour Moustafa & Jill Slay, "The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set", Information Security Journal: A Global Perspective, 2015.
[20] Zhao, G.; Zhang, C.; Zheng, L. "Intrusion detection using deep belief network and probabilistic neuralnetwork", In Proceedings of the 2017 IEEE International Conference on Computational Science andEngineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC),Guangzhou, China, 21–24 July 2017; Volume 1, pp. 639–642.
[21] Alrawashdeh, K.; Purdy, C. "Toward an online anomaly intrusion detection system based on deep learning",In Proceedings of the 2016 15th IEEE International Conference on Machine Learning and Applications(ICMLA), Anaheim, CA, USA, 18–20 December 2016; pp. 195–200.
[22] Zhao, G.; Zhang, C.; Zheng, L. "Intrusion detection using deep belief network and probabilistic neuralnetwork", In Proceedings of the 2017 IEEE International Conference on Computational Science andEngineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC),Guangzhou, China, 21–24 July 2017; Volume 1, pp. 639–642.
[23] Yin C et al , "A deep learning approach for intrusion detection using recurrent neural networks", IEEE Access 5:21954–2196, 2017.
[24] Kim J, Kim H, "Applying recurrent neural network to intrusion detection with hessian free optimization", International workshop on information security applications. Springer, 2015.
[25] Yuan X, Li C, Li X, "DeepDefense: identifying DDoS attack via deep learning", IEEE international conference on smart computing (SMARTCOMP), 2017.
[26] Wang Z et al, "Droiddeeplearner: identifying android malware using deep learning", Sarnoff symposium. IEEE, 2016.
[27] Jing L, Bin W, "Network intrusion detection method based on relevance deep learning", international conference on intelligent transportation, big data & smart city (ICITBS). IEEE, 2016.
[28] Bu S-J, Cho S-B, "A hybrid system of deep learning and learning classifier system for database intrusion detection", International conference on hybrid artificial intelligence systems, SpringeR, 2017.
[29] Kim J et al, "Long short-term memory recurrent neural network classifier for intrusion detection", International conference on platform technology and service (PlatCon), IEEE, 2016.