Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 09, September-2023

A Survey on Methods and Datasets of Intrusion Detection System (IDS) In Deep Learning

[1*] J.Archana [2] Dr.A.S. Aneetha
1Research Scholar,
Department of Computer science,
Vels Institute of Science Technologies and Advanced Studies (VISTAS),
Pallavaram, Chennai.

[1*]Assistant Professor,
Department of Computer science,
D.B.Jain College of arts & science,
Chennai.

[2]Associate Professor,
Department of Computer science,
Vels Institute of Science Technologies and Advanced Studies (VISTAS),
Pallavaram, Chennai.

Abstract - Due to the advent of a limitless communication paradigm and an increase in the number of networked digital devices in recent years, there has been a rising concern about cybersecurity, which attempts to protect either the system's information or communication technology. Intruders develop new attack types on a daily basis; consequently, in order to prevent these attacks, they must initially be precisely detected by the intrusion detection systems (IDSs) in use, and then appropriate responses must be provided. IDSs, which serve as vital for network security, are made up of three basic components: data collecting, feature selection/conversion, and a decision engine. The final component has a direct impact on system efficiency, and the employment of machine learning techniques is one of the most intriguing research fields. Deep learning has recently evolved as a novel approach that, through its own unique learning process, permits the utilization of Big Data with a low training time and high accuracy rate. As a result, it has begun to be used in intrusion detection systems. In this paper, it research aims to explore deep learning-based intrusion detection system approaches by doing a study of the literature and providing prior knowledge in either deep learning algorithms or intrusion detection systems.

Key Words: intrusion detection systems, network security, Deep learning, real-time attackers.

Introduction

Many organisations today keep their data in a variety of methods. The only obligation for these organisations is to safeguard their official and private information from external and internal intruders. Additionally, it's feasible that an approved user will expose company data for any reason. Because duplicate IP addresses and attacks on packets might be generated, it can be difficult to identify the attacker in real-time. Prior methods, such as firewalls and IDS, were unable to identify real-time attackers who entered the system without the admin's awareness. A collection of hardware and software make up a computer network. Each component carries its own set of dangers, weaknesses, and security problems. The data is exposed because of the software assault. The numerous activities carried out on the systems can be quickly discovered utilising log files by those who are familiar with programming and systems. They could contribute to security. The issue arises when users of a system are assaulted by intruders and are unable to identify the problem because they lack basic programming expertise. Different attack types exist. The task of identifying an internal or insider attack, however, is the most difficult.

Every user wants their systems to be protected from any harmful attacks (internal or external) in the field of network security. IDS and Internal IDS both have the ability to recognise internal intruders and identify the exterior attacks made by the intruders. With exchange, these methods assist us with system security.

With over 26 billion connected devices in 2019, network attacks are continually evolving and cyber threats are

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 09, September-2023

becoming severe problems as a result of how heavily dependent government, military, and commercial organisations are on the internet. ID

Due to this huge size of the network and uncontrolled/anonymous structure of the Internet, preserving both information and communication of the company has emerged as a challenging issue.

I. Concept of taxonomy in Intrusion Detection system

With the increased usage of the internet, there is an increase in cyber attack events. Bullying has a virtual existence in cyberspace. During this attack, the victim is subjected to intimidation, threats, and extortion. The attack could take the form of capturing the individuals' passwords or psychological pressure.

(a) Intrusion Detection System:

Intrusion Detection Systems are critical software or hardware security solutions to mitigate dangers that would otherwise arise when transporting information, prohibiting illicit access or assault, and reporting attacks to those in charge of security.[1].

Identification of attacks was first brought up in the 1980 survey "Computer security threat monitoring and surveillance." The following are the causes for the requirement for intrusion detection systems:

1) It determines attacks that other security measures cannot avert.

2) It adapts to the analytical phase prior to the attack.

3) It enables attack analysis, system restoration, and the correction of attacking variables.

Early detection, extensive information collecting, and evidence quality are all advantages of intrusion detection systems. The following are the weaknesses of intrusion detection systems: packet disintegration and timing assaults scan sequence mixing, and package hijacking.

It is difficult to comprehend that packets arriving on the computer are sent for a purpose of assault. A packet entering the system could be for ordinary communication or an attack. Detecting an attack necessitates a complicated and time-consuming calculation.

Intrusion detection systems are classified using a variety of criteria. IDSs are classed depending on their architectural structure, the type of system they safeguard, and the data processing time. There are two categories of intrusion detection systems based on their location: host-based and network-based [2]. IDSs can also be categorised based on their methodologies, which are Signature-Based and Anomaly-Based.

• Host-based intrusion detection system; the server attempts to detect intrusions by tracking traffic, registration files, and transactions.

• Network-based intrusion detection systems (IDS) listen to all network traffic, capture the content of every packet of data going across the network, stop attacks when necessary, and deliver reports.

• Signature-Based IDS detects known attack types.

• Anomaly-Based IDS; detects unknown assaults.

b) Deep learning Architectures for IDS.

A. Convolutional Neural Network (CNN)

Convolutional Neural Networks (CNNs) can learn intricate objects and patterns because they have an input layer, an output layer, multiple hidden layers, and millions of parameters. It subsamples the given input using convolution and pooling processes before applying an activation function, where all of them are hidden layers that are partially connected, with the fully connected layer at the end resulting in the output layer.[6][7][8]. The size of the output image is equivalent to the size of the original image.Convolution is the process of merging two functions in order to generate the output of the other function. The input image is convoluted using CNN filters, resulting in a Feature map. Filters are weights and biases in the network that are generated at random. CNN use the same weights and biases for all neurons rather than having distinct weights and biases for each neuron. Many filters can be built, each capturing a particular feature of the input. Filters are referred to as kernels.

B. RBM (Restricted Boltzmann Machine)

The RBM model has both hidden and visible layers. Units on the identical layer are not coupled and obey the Boltzmann Distribution principles. Each neuron saves the weight computations that take place in each layer. Input weights can be sent via random process nodes using randomly produced stochastic coefficients [15]. RBM does not distinguish between forward and reverse directions because it assigns the same weight to each. RBM is an unsupervised learning model that is typically used for feature extraction and denoising and is trained via a contrastive divergence approach [18].

C. Deep Neural Network (DNN)

DNN is End-to-end machine learning is an algorithm made up of many interconnected layers. Patterns are retrieved from simple feature representations with minimum prior knowledge in DNN. This deep learning approach is commonly utilised in circumstances where typical machine learning algorithms cannot address the problem effectively [14]. This neural network can be used to train a model to do regression and classification.

D.Deep Belief Network (DBN)

The DBN model is made up of numerous RBM layers and a Softmax classification layer [16]Some RBM is stored in a hidden layer on DBN and is utilised for training before being reused at the next training stage [17]. DBN training consists of two stages: unsupervised pretraining and

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 09, September-2023

supervised fine-tuning [19]. DBN detects assaults by using feature extraction and classification [20][21].

E.Autoencoder (AE):

Auto encoders are made up of two parts: encoders and decoders. Encoder is used to extract features from raw data. The decoder then reconstructs the retrieved characteristics. The difference between the encoder input and the decoder output gradually reduces during the training phase. Because Autoencoder is an unsupervised learning algorithm, the dataset does not need to be tagged. If the decoder successfully reconstructs the data using the extracted features, it can be concluded that the encoder's features describe the data substance. There are numerous variations on well-known autoencoders, such as denoising autoencoder [22] and autoencoder sparse [23]. Back-propagation neural networks are used in autoencoders.[25]

F. RNN (Recurrent Neural Network)

RNN is a sequential data artificial neural network. Natural Language Processing (NLP) is widely performed using it [27][26]. Because sequential data is contextual, we should not analyse it independently. Each RNN unit receives both its current and prior statuses in order to collect contextual information. In the RRN model, data flow is one-way, from one hidden unit to the next. Several researchers have developed RNN versions to handle the problem of non-sequential data, such as long-term memory (LSTM).[29], gated recurrent unit (GRU) [28], and bi-RNN [30].

G. General Adversarial Network (GAN)

GAN is a framework for investigating generative models [31]. GAN model has two sub networks, generator and discriminator. The generator can generate synthetic data that is similar to real data. Meanwhile, a discriminator tries to distinguish between simulated and genuine data. As a result, generator and discriminator complement each other. GAN can train a generative neural network to simulate a training data distribution without labels. The generative network transforms random input vectors into outputs that are comparable to the training data. In GAN, there is a second generative network that attempts to discriminate between actual training data and sample data generated by the generative network .

II. TYPES OF ATTACKS

Attacks can be passive or active [5]. The attacker's attempt to acquire access to the system distinguishes an active attack. During an active attack, the intruder will enter data into the system and perhaps change data within the system. Active assaults include distributed denial of service (DDoS), session replay, and masquerade. Viruses, worms, and Trojans are instances of active attacks. The passive assault attempts to learn or use system information but has no effect on system resources. Wiretapping, encryption, and scanning are examples of passive assaults.

An attack can be carried out by either an outsider or a member of the organization's staff. An insider attack is a hostile attack on a network or computer system conducted by someone who has been granted system access. UBS PaineWebber is one example of an insider attack. An unlawful use of the system started an external attack. Spoofing, spamming, and spinning are examples of outsider attacks.

Pharming:

Pharming is the practise of a hacker gaining access to a computer system and installing malicious code that redirects network website traffic to the hacker's fake sites. Many websites request personal information from their visitors.

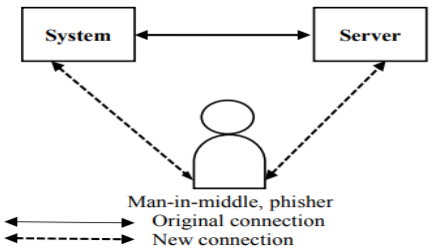
The pirate obtains sensitive and personal information from fraudulent websites. DNS cache poisoning and host file change are used in phishing attacks.

DOS (Denial of Service):

DOS is an attack in which the perpetrator attempts to render a machine or network resource unavailable to its intended users by disrupting service on a host connected to the internet for a short or long period of time. DOS assaults include flooding the network, halting connections, and blocking individuals from gaining access. DOS assaults deprive legitimate customers of the service they have come to expect.

Eavesdropping Attack:

Eavesdropping is a sort of electronic attack in which digital communication is disrupted by someone who was not supposed to receive it. The guy in the middle attack is the best illustration of an eavesdropping attack. Direct listening to digital or analogue voice communication and data shifting relative to any kind of communication are the two main types of eavesdropping assaults.



Phishing:

Phishing is the fraudulent attempt to obtain sensitive information. These details include usernames, passwords, credit card information, and other personal information. Spear phishing, clone phishing, and whaling are examples of phishing attacks.

Spear phishing:

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 09, September-2023

Spear phishing is a type of e-mail spoofing in which an individual or organisation is specifically targeted in order to obtain sensitive information.

Clone phishing:

Clone phishing is a sort of phishing in which the recipient's address is duplicated in order to create an identical e-mail with different content.

Whaling phishing

Whaling phishing is a type of phishing that targets high-profile people including top executives, celebrities, businessmen, politicians, and others. Technical support scams, malware attachments, social network exploits, and fraud scams are all examples of phishing.

DDOS (Distributed Denial of Service) Attack:

In DDOS, the inbound traffic flooding the victim comes from a variety of sources. A DDOS attack perpetrator use a large number of IP addresses. The fundamental distinction between DOS and DDOS is the use of systems in both assaults. DOS uses a single internet connection in a network, whereas DDOS uses several lines connecting to various devices.

A brute force attack is a way of collecting Information such as passwords or PIN (Personal Identification Number) by trial and error. A dictionary assault, also known as a search attack

Brute Force Attack:

A brute force attack is a way of collecting information such as passwords or PIN (Personal Identification Number) by trial and error. Dictionary attacks, searches, and rule-based search attacks are examples of brute force attacks. Using strong passwords will help you avoid this attack.

III.Network Datasets

Finding the suitable data set is the most onerous step in determining the efficacy of Intrusion Detection Systems. Analysing the network will provide the information needed for the data. Because gathering information from the network is expensive, developers want to govern their networks or systems using publicly available datasets. This section discusses the most often used data sets for attack detection systems.

A.NSL-KDD

To improve the performance of machine learning algorithms on KDD Cup99, the data size was decreased by eliminating duplicated entries, and the NSL-KDD dataset was developed. It comprises the essential records from the whole KDD Cup99 dataset. It contains the same data features as the data content KDD Cup99 [10]. The NSL-KDD differs from the original KDD Cup99 in the following ways: 1) The classifier is not biased because there is no redundant data in the training set.

2) The reduction ratio is smaller since there is no repetitious data in the test set.

3) The number of records from each difficult level group is proportionate to the percentage of records in the KDD dataset.

Each data set contains 41 attributes that describe various aspects of the flow, with one label indicating whether the attribute is an attack type or normal. The four assault types are further classified as DOS, Probe, R2L, and U2R.

B.CICIDS2017

The Canadian Institute for Cybersecurity (CIC) developed this dataset. The CIC IDS 2017 dataset includes common assaults that are comparable to real-world data. It also contains the results of the network traffic analysis performed using CIC Flow Meter, as well as the source and destination IP addresses, ports, protocols, and attacks. Furthermore, the dataset is likely to be accessible to everybody. CIC has identified eleven criteria required for the development of a trustworthy benchmark dataset [11]. Complete Network Configuration, Complete Traffic, Labelled Dataset, Complete Interaction, Complete Capture, Available Protocols, Attack Diversity, Heterogeneity, Feature Set, and Metadata are among the criteria.

The CICIDS2017 dataset includes labelled network flows (including entire packet payloads in.pcap format), matching profiles, and labelled flows and CSV files for machine and deep learning.

C.CSE-CIC-IDS2018

The dataset was generated by The Canadian Institute for Cybersecurity (CIC) and Communications Security Establishment (CSE). It contains thorough information about attacks as well as abstract distribution models for computer systems. The dataset embraces seven different attack scenarios, spanning brute force, DoS, web, infiltration, botnet, DDoS, and heartleech [12].

- Brute force attack; they collected these types of attacks using the FTP Patator and SSH Patator tools.
- DoS attack; they collected various types of attacks using the Hulk, Golden Eye, Slow loris, and Slow http test tools.
- Web attack; they collected these types of assaults using Damn Vulnerable Web App (DVWA) and in-house selenium framework (XSS and Brute-force) tools.
- Infiltration attack; they collected these types of attacks using the Nmap and port scan tools.
- Botnet assault; screenshots and keylogging were used.
- DDoS assault; for UDP, TCP, or HTTP requests, they employed Low Orbit Ion Canon (LOIC).
- Heart leech is a denial-of-service attack.

Every day, the CIC team recorded raw data, including network traffic and event logs. They used the CICFlowMeter-V3 to extract more than 80 network traffic features from raw data. Finally, they saved them into a CSV file per machine.

D.MCFPB to Traffic Merged with Benign

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 09, September-2023

The Malware Capture Facility Project (MCFP) provides complete bot malware traffic traces. It evolved in a laboratory setting. This data collection contains data about true bot infection to recreate an incident. Because discrete bot malware samples are run and traffic traces are provided without benign traffic, labels can be efficiently added to each event before combining. The absence of benign activity, and thus the absence of misleading alerts, poses a challenge to the power of data representation.[13] contains more information about this dataset.

IV. CONCLUSION

An intrusion detection system is essential in the cybersecurity area for preventing network intrusions. Its effectiveness is directly proportional to the decision engine used. Instead of signature-based detection, the system must be implemented as anomaly detection with a learning system to maximise its adaptability. Deep learning has evolved as one of the most recent training and classification techniques used in this engine. As a result, the purpose of this work is to provide a brief review of deep learning-based intrusion detection systems, as well as an overview of many aspects of intrusion detection and deep learning algorithms. Furthermore, this work lists and describes several publicly available datasets, including their characteristics and drawbacks. We hope that this comprehensive survey of deep learning-based intrusion detection systems will be useful to researchers in this field. Although the majority of the researchers suggested their method using older datasets, future work will benefit from using the newest datasets with other deep learning approaches.

V.REFERENCES

[1] G. Karatas¸, "Genetic algorithm for intrusion detection system," in Signal Processing and Communication Application Conference (SIU), 2016 24th. IEEE, 2016, pp. 1341–1344.

[2] G. Karatas and O. K. Sahingoz, "Neural network based intrusion detection systems with different training functions," in Digital Forensic and Security (ISDFS), 2018 6th International Symposium on. IEEE, 2018, pp. 1–6.

[3] O. Can and O. K. Sahingoz, "An intrusion detection system based on neural network," in 2015 23nd Signal Processing and Communications Applications Conference (SIU), May 2015, pp. 2302–2305.

[4] U. Cekmez, Z. Erdem, A. G. Yavuz, O. K. Sahingoz, and A. Buldu, "Network anomaly detection with deep learning," in 2018 26th Signal Processing and Communications Applications Conference (SIU), May 2018, pp. 1–4.

[5] Lazarevic, Aleksander, Yipin Kumar and Jaideep Srivastava, "Intrusion Detection: A Survey", managing cyber Threats, Springer US, 2005, pp 19-78, 2005.

[6] Razavian,A.S., Azizpour,H., Sullivan, J.,& Carlsson, S. (2014). CNN features off-the-shelf:Anastounding baseline for recognition. *IEEE Computer Society Conference on Computer Vision andPatternRecognitionWorkshops*.https://doi.org/10.1109/CVPRW.2014.131

[7] Krizhevsky,A.,Sutskever,I.,&Hinton,G.E.(2012).Image Net classification with deep convolutionalneuralnetworks.*AdvancesinNeuralInformationProcessingSystems*.https://doi.org/10.1061/(ASCE)GT.1943-5606.0001284

[8] G. Karatas and O. K. Sahingoz, "Neural network based intrusion detection systems with different training functions," in Digital Forensic and Security (ISDFS), 2018 6th International Symposium on. IEEE, 2018, pp. 1–6.

[9] Lawrence, S., Giles, C. L., Tsoi, A. C., & Back, A. D. (1997). Face recognition: A convolutional neural- network approach. IEEE Transactions on Neural Networks. https://doi.org/10.1109/72.554195

[10] G. Meena and R. R. Choudhary, "A review paper on ids classification using kdd 99 and nslkdd dataset in weka," in Computer, Communica- tions and Electronics (Comptelix), 2017 International Conference on. IEEE, 2017, pp. 553–558.

[11] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization." in ICISSP, 2018, pp. 108–116.

[12] T. Shibahara, T. Yagi, M. Akiyama, D. Chiba, and T. Yada, "Efficient dynamic malware analysis based on network behavior using deep learning," in Global Communications Conference (GLOBECOM), 2016 IEEE. IEEE, 2016, pp. 1–7.

[13] S. Garcia, M. Grill, J. Stiborek, and A. Zunino, "An empirical compar- ison of botnet detection methods," computers & security, vol. 45, pp. 100–123, 2014.

[14] Zhang, H., Wu, C. Q., Gao, S., Wang, Z., Xu, Y., & Liu, Y. (2018). An Effective Deep Learning BasedScheme forNetwork Intrusion Detection.*Proceedings - International Conference on PatternRecognition*.https://doi.org/10.1109/ICPR.2018.8546162

[15] Alrawashdeh, K., & Purdy, C. (2017). Toward an online anomaly intrusion detection system based on deeplearning.*Proceedings - 2016 15th IEEEInternational Conference on Machine LearningandApplications,ICMLA2016*.https://doi.org/10.1109/ICMLA.2016.167

[16] Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H., & Wang, C. (2018). Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access. https://doi.org/10.1109/ACCESS.2018.2836950

[17] Nadeem, M., Marshall, O., Singh, S., Fang, X., & Yuan, X. (2016). Semi-Supervised Deep Neural Network for Network Intrusion Detection. Research and Practice.

[18] Deng, J., Zhang, Z., Marchi, E., & Schuller, B. (2013). Sparse autoencoder-based feature transfer learningfor speech emotion recognition. *Proceedings - 2013 Humaine Association Conference on AffectiveComputingandIntelligentInteraction, ACII2013*. https://doi.org/10.1109/ACII.2013.90

[19] Ranzato,M.,Boureau,Y.L.,&LeCun,Y.(2009).Sparsefeaturelearningfordeepbeliefnetworks. *Advancesin NeuralInformationProcessingSystems20-Proceedingsofthe2007 Conference*.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 09, September-2023

[20] Alrawashdeh, K., & Purdy, C. (2017). Toward an online anomaly intrusion detection system based on deeplearning.*Proceedings - 2016 15th IEEEInternational Conference on Machine Learning andApplications,ICMLA2016*.https://doi.org/10.1109/ICMLA.2016.167

[21] Zhao, G., Zhang, C., & Zheng, L. (2017). Intrusion detection using deep belief network and probabilisticneural network. *Proceedings - 2017 IEEE International Conference on Computational Science andEngineering and IEEE/IFIP International Conference on Embedded and Ubiquitous Computing,CSEandEUC2017*.https://doi.org/10.1109/CSE-EUC.2017.119

[22] Vincent, P., Larochelle, H., Bengio, Y., &Manzagol, P. A. (2008). Extracting and composing robustfeatureswithdenoisingautoencoders. *Proceedingsofthe25thInternationalConferenceonMachineLearning*.https://doi.org/10.1145/1390156.1390294

[23] Deng, J., Zhang, Z., Marchi, E., & Schuller, B. (2013). Sparse autoencoder-based feature transfer learningfor speech emotion recognition. *Proceedings - 2013 Humaine Association Conference on AffectiveComputingandIntelligentInteraction, ACII2013*. https://doi.org/10.1109/ACII.2013.90

[24] Haider, W., Hu, J., Slay, J., Turnbull, B. P., & Xie, Y. (2017). Generating realistic intrusion detectionsystemdatasetbasedonfuzzyqualitativemodeling.*JournalofNetworkandComputerApplications*.https://doi.org/10.1016/j.jnca.2017.03.018

[25] Graves,A.,&Jaitly,N.(2014).Towardsend-to-endspeechrecognitionwithrecurrentneuralnetworks. *31stInternationalConferenceonMachineLearning,ICML2014*.

[26] Graves,A.,Mohamed,A.R.,&Hinton,G.(2013).Speechrecognitionwithdeeprecurrentneuralnetworks.*ICASSP,IEEEInternationalConferenceonAcoustics,SpeechandSignalProcessing - Proceedings*.https://doi.org/10.1109/ICASSP.2013.6638947

[27] Chung, J., Gülçehre, Ç., Cho, K., &Bengio, Y. (2014). Empirical Evaluation of Gated Recurrent NeuralNetworks onSequenceModeling.*CoRR,abs/1412.3*. http://arxiv.org/abs/1412.3555

[28] Hochreiter,S.,&UrgenSchmidhuber,J.J.(1997).Longshortterm memory.Neuralcomputation. *MEMORYNeuralComputation*.

[29] Schuster, M., & Paliwal, K. K. (1997). Bidirectional recurrent neural networks. *IEEE Transactions onSignalProcessing*. https://doi.org/10.1109/78.650093

[30] Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A.,&Bengio,Y.(2014).Generativeadversarialnets.*AdvancesinNeuralInformationProcessingSystems*.https://doi.org/10.3156/jsoft.29.5_177_2

(This work is licensed under a Creative Commons Attribution 4.0 International License.)