Journal of Scientific and Technical Research
13 (2) 2023, 15-23
http://www.publishingindia.com/jstr

Secure Cyber Threats using Network Intrusion Detection System with Deep Learning

Anisha Chaudhary[1], Babita Kumari[2] and Kuldeep Chouhan[3*]
[1,2]Under Graduate Student, Department of Computer Science and Applications, Sharda School of Engineering and Technology, Sharda University, Greater Noida, Uttar Pradesh, India
[3]Professor, Department of Computer Science and Applications, Sharda School of Engineering and Technology, Sharda University, Greater Noida, Uttar Pradesh, India
[*]Corresponding Author: kuldeep0009@gmail.com

Abstract: NIDS plays a crucial role in safeguarding computer networks against cyber threats. This work explores the application of deep learning techniques in enhancing NIDS capabilities. A subset of machine learning called deep learning has demonstrated remarkable potential in identifying complex patterns within network traffic data. By leveraging CNN and RNN the proposed NIDS achieves superior accuracy in detecting various types of intrusions, including anomalies and known attack patterns. The model is more flexible and effective at spotting new threats because it can gather relevant features on its own from raw network data. An overview of deep learning's application to NIDS is given in this paper. In this work, we will discuss various DL architectures such as CNN and RNN and their use in feature extraction, anomaly detection, and classification of network traffic. We also emphasize the benefits and difficulties of employing deep learning for intrusion detection, such as data pre-treatment and model complexity training on large-scale datasets that help the NIDS perform well in terms of generalization and real-time prediction accuracy. Moreover, the integration of deep learning allows for the system to continuously learn and improve its detection accuracy over time. We demonstrate how Deep Learning-based NIDS can enhance intrusion detection's accuracy and robustness in the dynamic and complex cyber threat environment through a review of previous studies.

Keywords: CNN, Cyber threats, Deep learning, Neural networks, RNN.

I. Introduction

The integration of deep learning into Network Intrusion Detection Systems (NIDS) represents a significant advancement in identifying and addressing network security threats. The adoption of deep learning methods, with a focus on deep neural networks in particular, enhances the accuracy and robustness of intrusion detection in network intrusion detection systems. NIDS is a state-of-the-art method for improving cyber security. These systems harness the power of deep learning, a subset of artificial intelligence (AI) to safeguard networks from unauthorized access and cyber threats by analyzing network traffic patterns and continuously learning from data. NIDS can quickly detect anomalies and potential security breaches, providing a proactive defense against evolving cyber threats.

A. Cyber Threats using NIDS

In the contemporary era of digitalization, the utilization of technology has yielded manifold advantages for individuals, organizations and society at large. Nevertheless, the augmented reliance on interconnected systems and the internet has also rendered us vulnerable to cybersecurity hazards. Cyber threats encompass a diverse range of malicious activities that are intended to exploit vulnerabilities in computer networks, systems, and data. These threats have the potential to result in data breaches, service disruption, financial losses, and compromised privacy. To counter these potential threats, implementing a NIDS is an essential component of a comprehensive cybersecurity plan. Whether as specialized software or hardware, a NIDS is specifically designed to monitor network traffic and identify any unauthorized or malicious activity. NIDS serves a critical function in identifying potential security breaches and promptly notifying network administrators, thereby enabling them to take immediate action to mitigate any associated risks.

B. Cyber Threats with Deep Learning

The realm of cyber security is in a constant state of flux, owing to the increasingly intricate and sophisticated nature of cyber threats. Deep learning, a subcategory of AI has demonstrated considerable promise in augmenting cyber security by enhancing the precision and efficacy of threat detection and response. Deep learning models, particularly neural networks, are adept at assimilating intricate patterns and features from voluminous datasets, rendering them highly suitable for tackling diverse cyber threats. The following are some of the ways in which deep learning is being employed to counter cyber threats.

- *Malware Detection*: Deep learning models possess the capability to scrutinize the code and behaviour of files

with the aim of identifying hitherto undetected malware. These models can acquire the ability to discern patterns and characteristics that are suggestive of malicious software, even when presented in polymorphic forms.

- *Intrusion Detection*: To identify malware that hasn't been identified before, deep learning models show that they can analyze the behaviour and code of files. Even in polymorphic variants, these models have the potential to learn to identify patterns and characteristics typical of malicious software.
- *Phishing Detection*: Deep learning models can analyze email content, headers, and sender conduct of email in order to detect phishing attempts. These models acquire the ability to differentiate between authentic and malevolent emails by discerning the subtle indicators.

C. Advantages

- *Data Availability:* Because deep learning models require large amounts of carefully selected training data, these volumes could pose a cybersecurity risk due to the sensitive nature of the data.
- *Adversarial Attacks:* Malicious actors can attempt to deceive deep learning models by making subtitle modifications to data inputs, leading to incorrect predictions or classifications.
- *Interpretability:* It can be challenging to comprehend how deep learning models make decisions because of the inherent challenges in interpreting them.
- *Resource Intensiveness:* Deep learning models can be resource-intensive to train and implement, requiring a large amount of memory and processing power.

D. Enhancing Network Intrusion Detection System Security with Deep Learning

A crucial part in identifying and reducing cybersecurity risks in computer networks is played by network intrusion detection systems or NIDS. The efficiency, accuracy, and adaptability of NIDS can be significantly increased by integrating deep learning approaches. Intricate patterns and features found in network traffic data are particularly well-represented by deep learning models, such as neural networks. Deep learning can be added to NIDS to improve its security in the following ways:

- *Improved Detection Accuracy*: Deep learning models excel at recognizing intricate patterns in large datasets, making them highly effective at detecting subtle and evolving cyber threats that might be missed by traditional rule-based systems.
- *Anomaly Detection*: Deep learning can help create models that learn the normal behaviour of network traffic and identify anomalies, such as new attack vectors or zero-day threats. Anomalies can be detected even without explicit rules, allowing NIDS to adapt to new threats.
- *Feature Extraction:* Human feature engineering is no longer necessary because deep learning networks are able to automatically extract pertinent features from unprocessed network data. This makes it possible for the NIDS to react to evolving attack strategies faster.
- *Deep Packet Inspection:* Deep learning can be used for deep packet inspection, allowing the NIDS to analyze the content of data packets for signs of malicious payloads, obfuscated code, or command and control communication.
- *Behavioural Analysis:* Deep learning models can be trained to recognize normal user and system behaviors, enabling the NIDS to detect deviations that might indicate compromised accounts or unauthorized activities.
- *Multi-Protocol Support:* Deep learning models are adaptable enough to be trained to understand the subtleties of different network protocols, making them useful for threat detection over a range of communication channels.

II. Literature Survey

NIDS using deep learning is an advance in detecting and mitigating network security threats. Deep learning techniques, particularly DNN, can be applied to NIDS for more robust and accurate intrusion detection. NIDS represents a Cutting-edge approach to enhancing cybersecurity. These systems harness the power of deep learning, a subset of artificial intelligence to safeguard networks from unauthorized access and cyber threat by analyzing network traffic patterns and continuously learning from data. NIDS can quickly detect anomalies and potential security breaches, providing a proactive defense against evolving cyber threats.

A. NIDS in Terms of Security

A deep neural network model was proposed by Zhou and colleagues [1] for the classification of cyberattacks. Data pre-processing, data acquisition (DAQ), and deep neural network classification are the three separate phases that make up the system's operation. With an accuracy of 0.963, the SVM model with a learning rate of 0.01 and 10 training epochs demonstrated a slight improvement over traditional machine learning techniques like k-nearest neighbour, random forest, and linear regression. In a different study, a DNN model was presented for analysing network traffic patterns within the context of the electric power grid. What distinguishes a secure electric power system is its state estimation, which is necessary for fundamental control operations. False data injection attacks on state estimates are hard to spot because a skilled hacker with insider knowledge of system topology may behave surreptitiously. When paired with genuine signals and Gaussian noise, injected data values can lead to erroneous state estimates and potentially cause widespread power grid failures. To ensure closed control loops in the power grid and to comply with physical process monitoring requirements, it

becomes imperative to identify the injected data. An attempt was made to tackle the intrusion detection challenge by using a binary classification task that minimized both false positives and false negatives. Every hacked vector is guaranteed to have elements characteristic of a false data injection attack thanks to the methodology. Four deep neural network (DNN) models and a set of measurement vectors were built in a pre-determined amount of time. Among these models were variations in the number of neurons in each layer and hidden layers: one model did not have L1 regularization. The training process combined the traditional stochastic gradient descent method with the back-propagation technique.

The best performing of the four models was the DNN model with three hidden layers, each with 150 neurons and no L1 regularization. Specifically, it outperformed additional DNN models, a distributed random forest classifier, gradient boosting machines, and generalized linear models. This particular DNN model achieved impressive results with recall, F1 score, and precision values of 0.9895, 0.9852, and 0.9802, respectively, while maintaining a low false alarm rate of 0.1840. Notably, its applicability in a simulated IEEE 14-bus power grid was validated using real datasets from Real-time Digital Simulation (RTDS) and physical testbeds, all without requiring extensive testing. An intrusion detection system (IDS) using deep learning techniques was introduced by Tang *et al*., [2] In the context of software-defined networking (SDN). This IDS system efficiently requests network statistics and monitors all OpenFlow switches since it is integrated into the SDN controller. Their study covered four attack categories: DoS attacks, R2L attacks, U2R attacks, and Probe attacks. It used the NSL-KDD dataset for a 2-class classification (normal and anomaly classes). The best Receiver Operating Characteristic (ROC) curve (AUC), outperforming alternative options, was obtained at a learning rate of 0.001, according to experimental results.

Public Datasets:

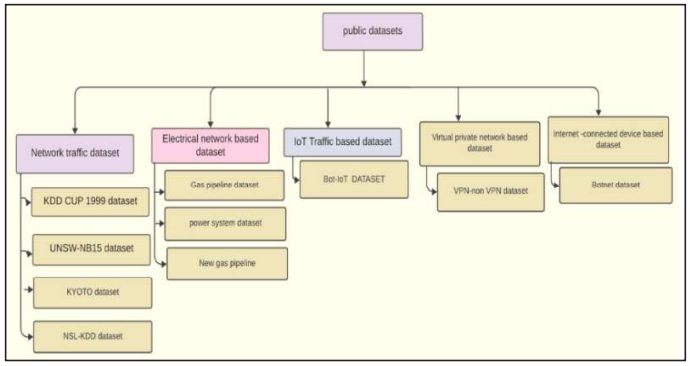

Fig. 1: Public Datasets

B. Dataset Based on Virtual Network Traffic Dataset

According to [3], the KDD Cup'99 dataset is made up of network traffic data that was gathered over a period of seven weeks, or roughly 4,900,000 vectors. The DARPA'98 Intrusion Detection System (IDS) evaluation program is where this dataset first appeared. It includes four different types of simulated attacks: 1) R2L (Remote to Local); 2) U2R (User to Root); 3) DoS (Denial of Service) attacks; and 4) probing attacks.

There are 41 features in the KDD Cup 1999 dataset that are divided into three classes: 1) Basic functions that pull vital data from a TCP/IP connection; features related to traffic, further divided into "same host" and "same service" categories; 3) Content features: these pertain to detecting anomalous activity within the data segment. It is important to note that this dataset is one of the most widely used choices for testing intrusion detection systems [4]. UNSW-NB15 dataset-This collection of tool-generated attack types, which includes DoS, Exploits, Generic, Reconnaissance, Shellcode, and Worms, was created using the Argus, Tcpdump, Bro-IDS, and IXIA Perfect Storm tools. The UNSW-NB15 dataset consists of roughly 2,540,044 vectors with 49 features. Moustafa *et al*. [5] divided the dataset into two groups: a testing set with 82,332 vectors and a training set with 175,341 vectors.

- *KYOTO Repository:* [6] This dataset was created with four different tools: web crawlers, email servers, darknet sensors, and honeypots. It is based on actual traffic data that was gathered over a three-year period. With the addition of 10 new features and 14 features taken from the KDD Cup 99 dataset, the KYOTO dataset has 24 statistical features in total.
- *Dataset NSL-KDD:* [7] As Tavallaee *et al*. [8] suggest, this dataset should be used to address some of the intrinsic problems with the KDD'99 dataset. Comparing the NSL-KDD dataset to the original KDD dataset reveals a number of benefits. These benefits consist of: 1) Record Selection: To enable experimentation with various data portions, the NSL-KDD dataset offers subsets of records arranged as a percentage of the original records (e.g., KDDTrain+_20Percent.ARFF); 2) No Redundancy: The dataset is more organized and effective because it does not contain redundant or duplicate records; 3) Better Balance: The dataset shows a more equitable and realistic assessment of intrusion detection techniques due to its improved record distribution balance. It is interesting to note that many research papers in intrusion detection combine the NSL-KDD dataset and the KDD Cup 1999 dataset for performance evaluations, frequently concluding that the NSL-KDD dataset produces better results.

C. Dataset Based on Electrical Networks

Dataset on ICS cyberattacks**:** [9] This dataset consists of three separate datasets: Gas pipeline datasets; 2) New pipeline for gas; 3) The Power System dataset, comprising 37 scenarios classified into the following categories: Eight events are natural; one is a no event; and twenty-eight are attack events that are

further divided into three categories: 1) Attacks using data injection; 2) Attacks using remote tripping command injection; and 3) Attacks using relay setting changes. Cybersecurity breaches can be identified using these datasets by industrial control systems [10, 11, 12, 13, 14, [12], and [13].

D. A Dataset Based on IoT traffic

Dataset for Bot-IoT**:** In [15] With over 72,000,000 records, this dataset covers a broad spectrum of attacks, including DDoS, DoS, OS and Service Scan, Keylogging, and Data Exfiltration. The Bot IoT dataset was introduced by Koroniotis *et al.* [16] and is tailored specifically for the Internet of Things (IoT) environment, setting it apart from previous datasets. The Node-RED tool was used by the authors to simulate the network behavior of Internet of Things devices. The lightweight MQTT protocol is used in this dataset to facilitate machine-to-machine (M2M) communication. The testbed simulates five different Internet of Things scenarios: a smart refrigerator, a weather station, motion-activated lights, a remotely operated garage door, and a smart thermostat.

E. Private Network

VPN-dataset without a VPN: The virtual private network (VPN) session and the standard network session [17] are the two distinct session types that make up this dataset, which was initially introduced by Draper *et al.* [18]. The dataset contains labeled data related to a wide range of activities, such as Web browsing (e.g., Firefox), email (e.g., SMPTS), chat (e.g., Skype), streaming (e.g., YouTube), file transfer (e.g., SFTP), VoIP (e.g., Hangouts voice calls), and peer-to-peer (P2P) activities (e.g., uTorrent). The VPN and non-VPN dataset is comprised of these actions collectively.

F. Dataset Based on Devices Connected to the Internet

1) The Botnet dataset [19] first presented by Beigi *et al*. [20], this dataset consists of seven and sixteen distinct types of botnets, respectively, and is split into training and test datasets. Many botnet types, such as Zeus, SMTP Spam, Rbot, VI rut, NSIS, Neris, and Zeus control (C&C), are included in the training dataset as well. Botnet types like Neris, R bot, Menti, Sogou, and others are included in the test dataset. The botnet topologies include distributed (P2P), centralized, and random architectures. Four categories-byte-based, packet-based, time-based, and behavior-based-are used to group the features. We use two recently released real traffic datasets, the Bot IoT dataset, and the CSE-CIC-IDS2018 dataset, in our comparative analysis.

G. Deep learning-based CT NIDS relying on datasets, the model's ability to accurately detect attacks is evaluated. The quality of the data is the primary determinant of any Network Intrusion Detection System's (NIDS) effectiveness. The NSL-KDD dataset is specifically designed to address some of the shortcomings present in the original KDD'99 dataset and is intended for use with network-based intrusion detection systems (IDS). These IDS's main goal is to evaluate system security and send out alerts when intrusions are discovered.NSL-KDD, UNSW-NB15, and KDD Cup'99 are the three datasets being examined in this context. With regard to intrusion detection research, each of these datasets has unique attributes and features.

H. UNSW-NB15 Dataset

The University of New South Wales (UNSW) created the UNSW-NB15 dataset, which has become well-known as a frequently used dataset for network intrusion detection, especially in the deep learning subfield of network security. Its main goal is to evaluate how well IDS and machine learning algorithms work together to detect and neutralize network threats. It explores the relationship between deep learning and the UNSW-NB15 dataset in the context of network security in comparison to the KDD'99 dataset, the UNSW-NB15 dataset,which was introduced in 2015, offers a more recent dataset with nine attack types it as opposed to the 14 in the KDD'99 dataset,it covers a wider variety of modern attacks. This dataset, which includes both benign and malicious activities, consists of 2,540,044 records with 49 features and class labels. 321,283 entries in these records are linked to attacks, whereas 221,876 entries are regular. As a result, the UNSW-NB15 dataset is a current and thorough resource for assessing intrusion detection systems, particularly in light of the constantly changing field of network security.

The UNSW-NB15 dataset's features are arranged into six different classes: Additional Generated Features, Content Features, Flow Features, Time Features, and Labeled Features. Features that fall into these classes are classified as connection features if their number is between 41 and 47, and general-purpose features if they are between 36 and 40. Additionally, nine distinct attack categories are covered by the dataset: fuzz, backdoors, reconnaissance, generic attacks, Denial of Service (DoS) exploits, analysis, shellcode, and worms. The goal of current network intrusion detection research is to improve detection accuracy in security applications while maintaining scalability and real-time processing capabilities. This is especially true for deep learning research on the UNSW-NB15 dataset. Scholars are currently engaged in the development of novel deep learning models, exploring a variety of architectures.

III. Architecture of Cyber Security

Integrating various architectural elements is necessary to achieve effective intrusion detection while taking security concerns into account when developing a deep learning-based

cyber threat detection system. An outline of the architecture for a safe deep learning-based NIDS is provided below:

- Data gathering and pre-processing**:** Gathering information about network traffic, including logs, network packets, and other relevant data.
- The process of removing pertinent features from the pre-processed data so that deep learning models can utilize them is known as feature extraction. Session data, payload content, packet headers, and other relevant data are examples of these features.
- When choosing a deep learning model, pick the top deep learning architectures for intrusion detection. The available options include long short-term memory (LSTM) networks, transformer-based models, recurrent neural networks (RNNs), and convolutional neural networks (CNNs).
- Training the Model: Divide the dataset into sets for testing, validation, and training.

Utilizing the training data, train the deep learning model and observe how it performs on the validation set. Use appropriate optimization algorithms (e.g., Adam, RMSprop) and loss functions (e.g., binary cross-entropy for binary classification).

Implement techniques like early stopping and learning rate scheduling to prevent overfitting.

Security Measures: Implement security mechanisms to protect the model and data:

- *Model Encryption***:** Encrypt the deep learning model to prevent reverse engineering and unauthorized access.
- *Secure Data Storage:* Storing training and testing data securely to prevent data leakage.
- *Secure Communication:* Use encryption and authentication to protect data transmission between components.

Model Evaluation and Test Conduct thorough testing, including adversarial attacks, to assess the model's robustness against potential threats.

- *Real-Time Deployment and Monitoring:* For continuous, ongoing monitoring, deploy the trained model in a real-time network environment. Implemented mechanisms for continuous model updates and retraining to adapt to evolving cyber threats.
- *Intrusion Alerting and Response:* Configure the system to generate alerts or notifications when potential intrusions are detected. Integrate the NIDS with other security systems to enable automated responses, such as blocking suspicious traffic.

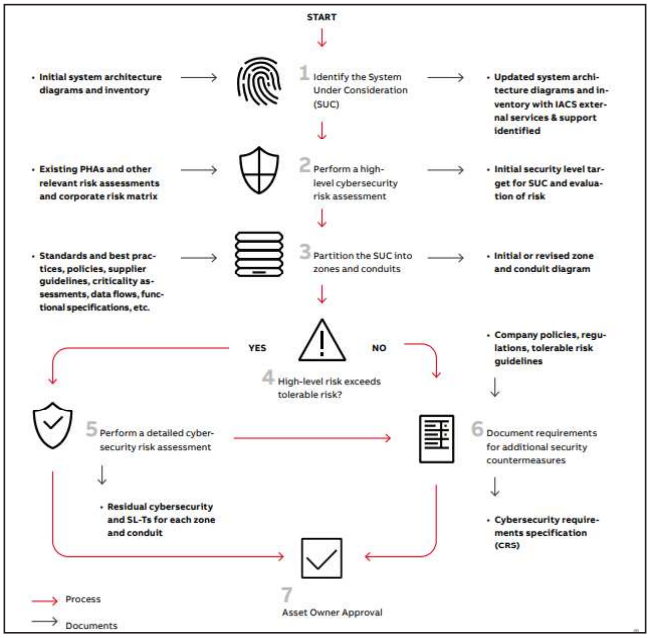

Fig. 2: Systematic Mechanism of DL for Cyber Security

CNN: Convolutional Neural Network;

DNN: Deep Neural Network;

RNN: Recurrent Neural Network;

DBN: Deep Belief Network;

RBM: Restricted Boltzmann Machine;

ReNN: Replicator Neural Network;

DA: Deep Auto-encoder; DML:

Deep Migration Learning;

STL: Self-Taught Learningis represented in Fig. 2.

IV. Cyber Threats with Deep Learning

Cyber threats involving deep learning algorithms can take various forms, and they often exploit the capabilities of these algorithms for malicious purposes. Here are some common cyber threats associated with deep learning:

- *Advanced Malware:* Malicious actors can use deep learning to create advanced malware that can evolve and adapt to evade detection by traditional antivirus and intrusion detection systems.
- *Phishing Attacks:* Deep learning can be employed to generate highly convincing phishing emails and websites, making it difficult for users to discern between legitimate and fake communication.

- *Credential Attacks:* Deep learning models can be used to crack passwords, conduct brute-force attacks, or guess authentication credentials more effectively by learning from patterns in user behaviour.
- *Automated Attacks:* Distributed Denial of Service (DDoS) attacks are among the cyberattacks that adversaries can automate with deep learning. Online services could become overloaded by these attacks, which would cause disruptions and service outages.
- *Data Manipulation:* Deep learning techniques can be used to manipulate or generate fake data, which can be exploited in various cyberattacks to deceive systems or users.
- *Privacy Invasion:* Deep learning-based facial recognition, voice recognition, and biometric identification methods can infringe upon individual privacy when used without consent or for malicious purposes.

V. Deep Learning Approaches

Various deep learning approaches are discussed in deep neural networksto identify n layers as follows**:**

- Deep neural networks, or DNNs, are made up of multilayer perceptron (MLP) that have three or more layers. As seen in Fig. 3, MLPs are a type of feedforward artificial neural network that is identified by the n layers that make up the network and are arranged in succession [24].

Algorithm 1: DNN Network Based on MLP
1. Select a pair for learning (x, c);
2. x = h0;
3. do with M = 1 to N
4. hM = αM (gM) ;
5. hM = nM (hM-1) = WM × hM-1 + bM-
6. finish for

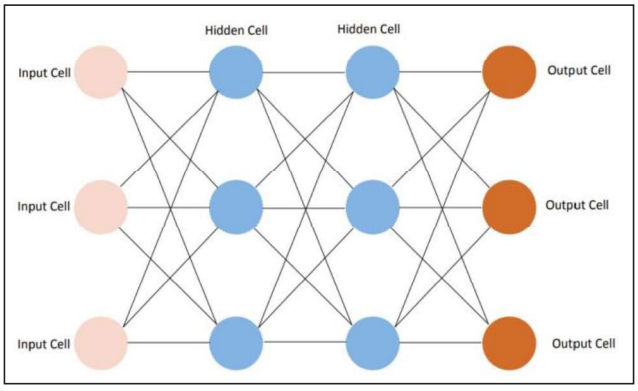

Fig. 3: Deep Neural Network

- A recurrent neural network, or RNN for short, is a network of neurons with at least one cycle in the graph of connections [25].

Algorithm 2: Recurrent Neural Network
1. Choose a pair to learn
2. From (x(t), c(t)).
3. For every t in the interval [1, tf], initialize the hidden state at time t (h0(t)) as the input x(t).
4. Repeat steps 1 through N over M: a. Repeat from 1 to tf over t:
5. Utilizing the formula gM(t) = WM × hM-1(t) + VWM × hM(t-1) + bM, calculate gM(t).
6. Apply the activation function αM(gM(t)) to update hM(t).
7. end for
8. end for

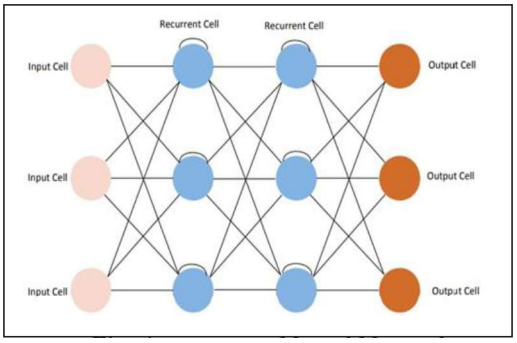

Fig. 4: Recurrent Neural Network

In Fig. 5, a CNN is a kind of neural network that uses a higher resolution to capture features at first, then a coarser resolution to transform them into more detailed features. Numerous CNN models have been developed, such as ZF Net (described by [26]), Google Net (described by [27]), and Res Net [28].

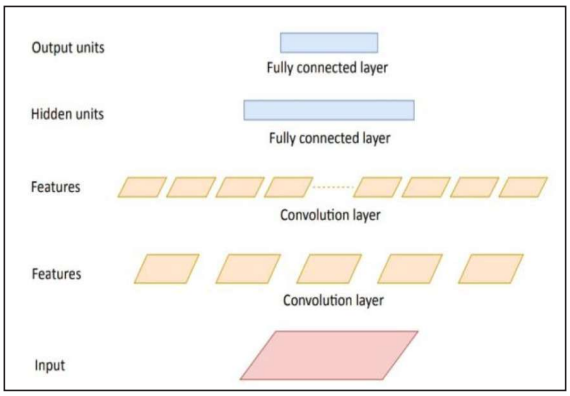

Fig. 5: Convolutional Neural Network

VI. Performance Metrics

We make use of critical performance indicators, such as detection rate (DR), false alarm rate (FAR), and accuracy. Table I presents the four possible outcomes of correct and incorrect classifications.

$$DR_{Attack} = \frac{TP_{Attack}}{TP_{Attack} + FN_{Attack}}$$

$$TNR_{BENIGN} = \frac{TN_{BENIGN}}{TN_{BENIGN} + FP_{BENIGN}}$$

$$FAR = \frac{FP_{BENIGN}}{TN_{BENIGN} + FP_{BENIGN}}$$

$$Accuracy = \frac{TP_{Attack} + TN_{BENIGN}}{TP_{Attack} + FN_{Attack} + TN_{BENIGN} + FP_{BENIGN}}$$

TABLE I: CONFUSION MATRIX

		Predicted Class	
		Negative Class	*Positive Class*
Class	Negative Class	True Negative (TN)	False Positive (FP)
	Positive Class	False Negative (FN)	True Positive (TP)

A. Deep Discriminative Models

The deep discriminative model refers to a discriminative model that employs deep neural networks as shown in Fig. 6. These networks have multiple layers, allowing them to learn intricate and hierarchical features from the input data. Common architectures for deep discriminative models include feedforward neural networks, CNNs, and RNNs.

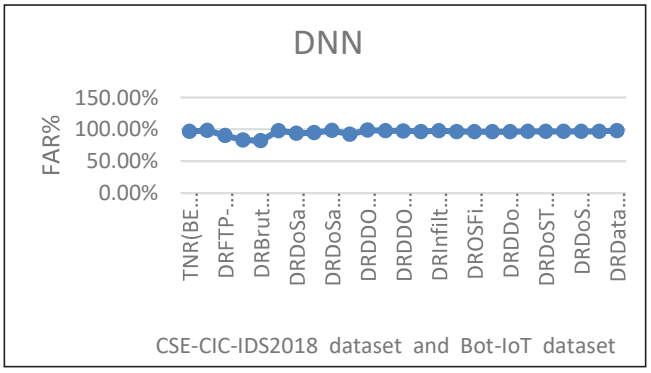

Fig. 6 (a): Deep Discriminative Models

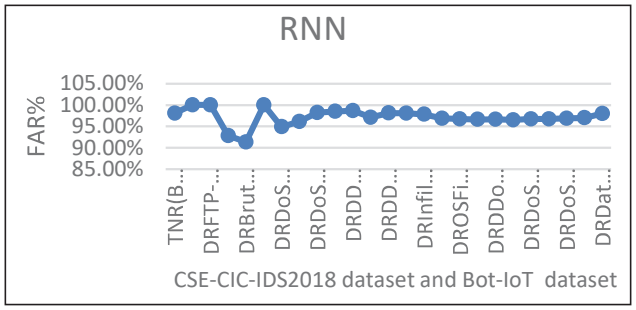

Fig. 6 (b): Deep Discriminative Models

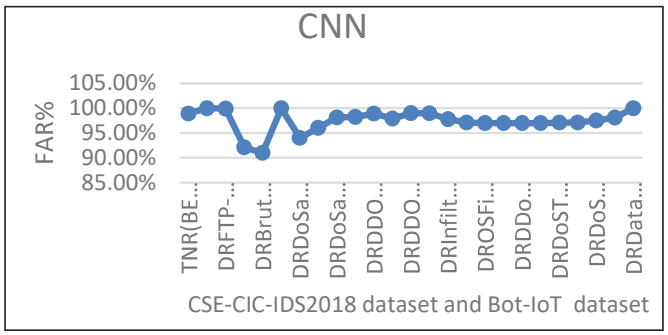

Fig. 6 (c): Deep Discriminative Models

Fig. 6 shows the DNN gives the highest true negative rate with 96.915%. The recurrent neural network gives the highest detection rate for seven attack types, namely, Brute Force -XSS 83.26%%, Brute Force - Web 82.22%, DoS Attacks-Hulk 93.53%, DoS attacks-SlowHTTPTest 94.81%, DoS attacks-Slowloris 98.16%%, DoS Attacks-GoldenEye 92.13%, and Infiltration 97.874%. CNN gives the highest detection rate for four attacks type, including, DDOS attack-HOIC 98.84%, DDOS attack-LOIC-UDP 97.55%, and DDOS attack-LOIC-HTTP 97.42%, and Botnet 96.44%.

B. Generative/Unsupervised Models

Generative models aim to model the underlying probability distribution of the training data as shown in Fig. 7.

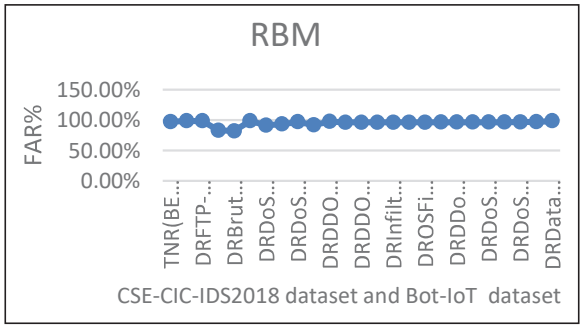

Fig. 7 (a): Generative/Unsupervised Models

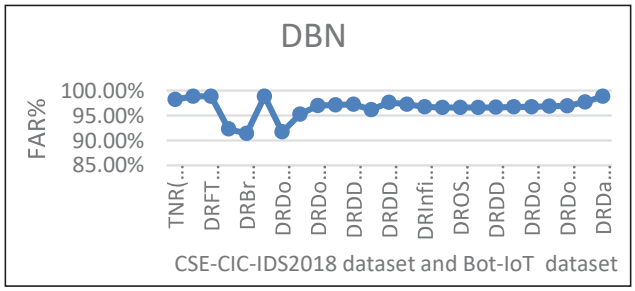

Fig. 7 (b): Generative/Unsupervised Models

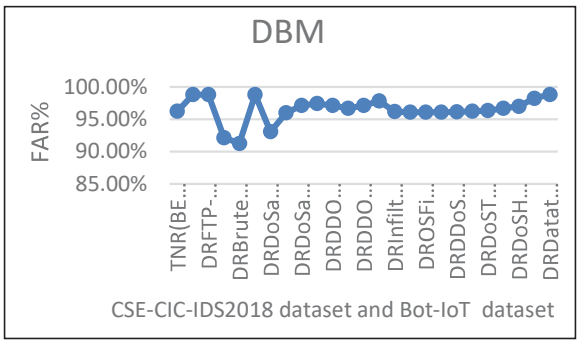

Fig. 7 (c): Generative/Unsupervised Models

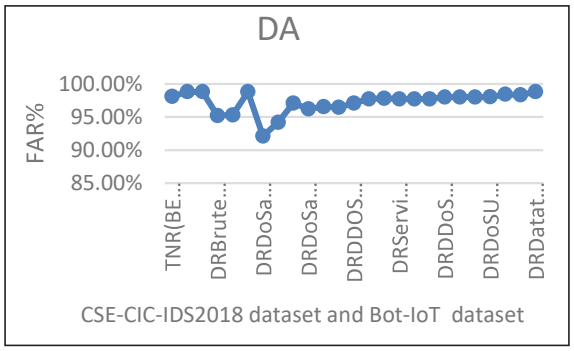

Fig. 7 (d): Generative/Unsupervised Models

Fig. 7 shows the deep belief network gives the highest true negative rate with 98.212% and the highest detection rate for four attacks type, namely, Brute Force -XSS 83.16%, Brute Force -Web 82.22%, DoS attacks-Hulk 91.32%, and DDOS attack-LOIC-HTTP 97.612%. The deep auto encoders give the highest detection rate for three attack types, namely, Brute Force -Web 91.43%, DoS attacks-Slowloris 96.99%, and Infilteration 96.71%. The deep Boltzmann machine gives the higest detection rate for five attack types, namely, DoS attacks-Hulk 93.072%, DoS attacks-SlowHTTPTest 95.993%, DoS attacks-GoldenEye 97.421%, DDOS attack-LOIC-UDP 96.654%, and Botnet 97.812%.

VII. Conclusion

In this work, a revolutionary development in the fight against cyber threats is the incorporation of Deep Learning into NIDS. Deep Learning has the potential to improve network security due to its ability to process large datasets and identify complex, unknown threats. This work evaluates deep-learning methods for DL-IDS system intrusion detection. UNSW-NB15, KDD Cup 1999, NSL-KDD, and four other datasets are used. Furthermore, seven public datasets covering network traffic, electrical networks, virtual private networks, internet traffic, traffic from Android apps, traffic from the Internet of Things, and traffic from internet-connected devices are included. These datasets combined deep discriminative models with generative/unsupervised models in a hybrid approach that integrated CNNs. The deep learning integration with NIDS is a potent weapon in the ongoing fight against cyberattacks, notwithstanding current obstacles, more investigation and improvement could lead to the creation of more resilient, flexible, and effective NIDS systems that could offer improved defence against the ever-changing landscape of cyber threats.

References

[1] L. Zhang, L. Shi, N. Kaja, and D. Ma, "A two-stage deep learning approach for CAN intrusion detection," in *Proc. Ground Vehicle Syst. Eng. Technol. Symp.,* pp. 1-11, 2018.

[2] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," *International Conference on Wireless Networks and Mobile Communications,* IEEE, 2016, pp. 258-263.

[3] Accessed: May 30, 2019. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[4] "Unsw-nb15 dataset." Accessed: May 30, 2019. [Online]. Available: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ ADFA-NB15-Datasets/

[5] N. Moustafa, J. Slay, and G. Creech, "Novel geometric area analysis technique for anomaly detection using trapezoidal area estimation on large-scale networks," *IEEE Transactions on Big Data*, 2017.

[6] "Nslkdd." Accessed: May 30, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/nsl.html

[7] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD cup 99 dataset," *IEEE Symposium on Computational Intelligence for Security and Defence Applications*, IEEE, 2009, pp. 1-6.

[8] U. Adhikari, S. Pan, T. Morris, R. Borges, and J. Beave, "Industrial control system (ICS) cyber-attack datasets." Accessed: Jun. 23, 2019. [Online]. Available: https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets

[9] S. Pan, T. Morris, and U. Adhikari, "Developing a hybrid intrusion detection system using data mining for power systems," *IEEE Transactions on Smart Grid*, vol. 6, pp. 3104-3113, 2015.

[10] S. Pan, T. Morris, and U. Adhikari, "Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data," *IEEE Transactions on Industrial Informatics*, vol. 11, pp. 650-662, 2015.

[11] J. M. Beaver, R. C. Borges Hink, and M. A. Buckner, "An evaluation of machine learning methods to detect

malicious SCADA communications," *International Conference on Machine Learning and Applications*, vol. 2, pp. 54-59, IEEE, 2013.

[12] T. Morris, A. Srivastava, B. Reaves, W. Gao, K. Pavurapu, and R. Reddi, "A control system testbed to validate critical infrastructure protection concepts," *International Journal of Critical Infrastructure Protection*, vol. 4, pp. 88-103, 2011.

[13] T. H. Morris, Z. Thornton, and I. Turnipseed, "Industrial control system simulation and data logging for intrusion detection system research," *7th Annual Southeastern Cyber Security Summit*, 2015, pp. 3-4.

[14] Accessed: May 30, 2019. [Online]. Available: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot_iot.php

[15] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 100, pp. 779-796, 2019.

[16] Accessed: Jun. 23, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/vpn.html

[17] G. Draper-Gil, A. H. Lashkari, M. S. I. Mamun, and A. A. Ghorbani, "Characterization of encrypted and VPN traffic using time-related," in *Proceedings of the 2nd International Conference on Information Systems Security and Privacy*, 2016, pp. 407-414.

[18] Accessed: Jun. 23, 2019. [Online]. Available: https://www.unb.ca/cic/datasets/botnet.html

[19] E. B. Beigi, H. H. Jazi, N. Stakhanova, and A. A. Ghorbani, "Towards effective feature selection in machine learning-based botnet detection approaches," in *2014 IEEE Conference on Communications and Network Security*, IEEE, 2014, pp. 247-255..

[20] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD cup 99 data set," *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, IEEE, 2009, pp. 1-6.

[21] G. Meena, and R. R. Choudhary, "IDS classification using KDD'99 and NSLKDD dataset in Weka," *International Conference on Computer, Communications and Electronics, IEEE*, 2017, pp. 553-558.

[22] N. Moustafa, and J. Slay, "UBSW-NB15: A comprehensive dataset for network intrusion detection systems (UNSW-NB15 network dataset)," in *Military Communications and Information Systems Conference*, IEEE, 2015, pp. 1-6.

[23] W. Liu, Z. Wang, X. Liu, N. Zeng, Y. Liu, and F. E. Alsaadi, "A survey of deep neural network architectures and their applications," *Neurocomputing*, vol. 234, pp. 11-26, 2017.

[24] G. Gelly, and J.-L. Gauvain, "Optimization of RNN-based speech detection," *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, vol. 26, no. 3, pp. 646-656, 2017.

[25] M. D. Zeiler, and R. Fergus, "Visualizing and understanding convolutional networks," in *European Conference on Computer Vision,* Springer, 2017, pp. 818-833.

[26] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, "Going deeper with convolutions," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2015.

[27] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition,* 2016, pp. 770-778.

[28] A. A. Aburomman, and M. B. I. Reaz, "A survey of intrusion detection systems based on ensemble and hybrid classifiers," *Computers & Security*, vol. 65, pp. 135-152, 2017.

[29] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, "Machine learning and deep learning methods for cybersecurity," *IEEE Access*, vol. 6, pp. 365-381, 2018.

[30] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection datasets," *Computers & Security*, 2019.

[31] G. Loukas, E. Karapistoli, E. Panaousis, P. Sarigiannidis, A. Bezemskij, and T. Vuong, "A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles," *Ad Hoc Networks,* vol. 84, pp. 124-147, 2019.