International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

The Empirical Analysis on Proposed Ids Models based on Deep Learning Techniques for Privacy Preserving Cyber Security

Dr. Rohith Vallabhaneni,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA.
rohit.vallabhaneni.2222@gmail.com

Dr. Srinivas A Vaddadi,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. Vsad93@gmail.com

Sravanthi Dontu,

PhD Research Student, Department of Information Technology, University of the Cumberlands, USA.
sravanthi.dontu13@gmail.com

Dr. Abhilash Maroju,

Ph.D. Research Graduate, Department of Information Technology, University of the Cumberlands , USA.
doctorabhilashmaroju@gmail.com

ABSTRACT

In AI, the deep learning (DL) method of machine learning (ML) places an emphasis on large-scale, scalable models that can learn distributed representations from their input data. The scope and effectiveness of these techniques are demonstrated in this thesis through a number of case studies pertaining to cyber security. By the end of each study, the neural network models had been fine-tuned and expanded to provide better results. The key arguments presented and discussed in this thesis are as follows: 1) Creating an all-inclusive database for domain name detection using domain generation algorithms (DGAs) and a new architecture to improve DGA domain name detection overall performance. 2) Constructing a hybrid intrusion detection warning system that incorporates deep neural networks (DNNs) to examine host-level and network-level behaviours within an Ethernet LAN. thirdly, analysing data from social media platforms, email, and URLs to create a single DL-based framework for detecting spam and phishing. 4) ScaleMalNet, a novel hybrid framework proposal, is part four. This is a two-step process: first, we use static and dynamic analysis to determine if the executable file is malicious or not. Then, we categorise the malicious executable file into the appropriate malware family. Malware and ransomware analysis for Android is accomplished using a hybrid DL framework that is comparable to this one.

1. INTRODUCTION

The distribution of water and gas, hospitals, and energy suppliers are all examples of critical national infrastructures (CNIs) that are increasingly under cyber assault. Industrial control systems, often known as supervisory control and data acquisitions (SCADA), are the backbone of production management for CNIs. Organisational, national, and European-level consideration of the need to safeguard ICSs and CNIs has grown in importance. For example, Europe has produced a slew of legislation and directives in recent years in an effort to provide a consistent framework for protecting networks, data, and electronic communications in the face of the growing threat of CNIs. To address the many facets of cyber security, including the legal, organisational, capacity building, and technical components, additional security measures are required in addition to rules, regulations, and policies [1].

A computer can solve a problem by first writing an algorithm that effectively handles the problem and then implementing this algorithm into its hardware or software. Since not every

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

problem has an algorithm, a direct programming technique will not work when the algorithm is unknown. By providing an opportunity to find solutions in situations when algorithms cannot be constructed manually, machine learning (ML) broadens the capacity to work with computers. Using examples of correct behaviour, an algorithm can be defined as non-constructive. By this definition, ML algorithms are meta-algorithms that produce algorithms based on given knowledge about what those algorithms should construct. These algorithms give a significantly better way to interface with computers by just providing data for computation, rather than strategies for computation itself.

The second line of defence for every system is an intrusion detection system (IDS) [2]. Combining intrusion detection systems (IDSs) with additional security measures including authentication procedures, encryption methods, and access control can make systems far more resistant to cyber assaults. Intrusion detection systems (IDSs) can distinguish between safe and harmful activities by looking for certain patterns in normal or benign traffic or activity, or by using specific criteria that identify an attack as malevolent [3].

While increasing computational capability is a worthy goal, it should not be the sole motivation for pursuing ML education. Learning teaches people to understand what can be practically computed, and vice versa: studying computation can teach people about learning. The study of how computers learn new tasks is known as machine learning (ML). We learn more about the mind when we try to solve problems with computational models of learning, and we can use what we discover to motivate the development of ML models.

Studying ML has scientific value since it sheds light on computing and learning. Also, for science to be meaningful, it ought to have a good impact on society. The best way to boost ML research is to make a difference, and one way to accomplish that is to maintain a connection with pressing practical challenges. Machine learning (ML) approaches can address a wide range of specific problems with real-world and commercial implications. As researchers, our sole purpose is to push the field forward. To that end, we can either create a new method and then seek out a problem that it can solve, or we can pinpoint an issue and then find a solution to it. In both cases, we will undertake comprehensive research to understand the problem's essential parts and the advantages and disadvantages of existing frameworks. Using deep learning (DL) methods to tackle Cyber Security issues is the main focus of this thesis.

2. LITERATURE REVIEW

Using a deep learning detection model and a packet capture tool, the plug-and-play device proposed by Feng et al. (2019) [4] may identify privacy threats and Denial of Service (DoS) in ad hoc networks. For the purpose of detecting SQL and XSS attacks, the proposed model makes use of a CNN and an LSTM. To detect DOS attacks, the proposed approach makes use of a deep neural network. Based on the KDD CUP 99 dataset, which is split into a training set of 70% and a testing set of 30%, the research was conducted. In addition, the research showed that XSS attack detection accuracy was 0.78% for convolutional neural networks and 0.57% for deep neural networks.

Zhang et al. (2018) [5] introduced CAN IDS, a two-stage intrusion detection system, to detect hostile attacks on autonomous vehicles. A robust rule-based approach is used in the first stage, and a deep learning network is used in the second stage to detect outliers. The three datasets used to measure performance include US, Asian, and Honda vehicles. The training data consists solely of legitimate traffic from these three datasets, while the testing data contains malicious traffic from five distinct attack types: drop, random, zero ID messages, replay, and spoofing.

Data and system security has become more important as the usage of digital technology in our daily lives continues to expand. To acquire data and information while it is in transit or stored, hackers have developed a number of new intrusion techniques [6]. People, computers, or other entities that attempt and are successful in violating or engaging in unauthorised actions on a computer network are commonly referred to as intruders. Intruders can come from within or from outside. The first group describes an effort at illicit activity by a group of persons who have legitimate access to a system. The second group consists of intruders who do not have authorization to enter the system. After collection, the IDS compares the packets with a trusted database of known signatures to determine which ones are legitimate and which ones are based on anomalies. The firewall, which keeps tabs on data transfers both within and between networks, is also connected to these systems.

An incursion could be defined as any unauthorised activity or traffic on a network or system. Intrusion detection systems are tools or programmes that keep an eye on a network for any suspicious activity or policy breaches and then send out alerts when they find them. Although there are challenges to implementing intrusion detection systems (IDS), the authors of [7] state that they are a potential solution to cybersecurity difficulties. An anomaly-based intrusion detection system typically has a high false positive (FP) rate and requires a lot of computing power.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

To identify and avoid such damaging assaults, the authors of [8] presented a new intelligent intrusion detection system (IDS) with two stages. Presented here is a two-stage architecture that relies on ML methods. The IDS employs a two-stage attack identification process: first, using the K-means clustering method, and second, using the supervised learning algorithm to classify attacks and decrease false positives. By using this method, an IDS is created that is efficient in terms of computing and can accurately identify and classify threats while producing few false positives.

Researchers in IDS have achieved remarkable levels of accuracy in automatically detecting normal and abnormal data by employing ML-based techniques. Hidden dangers can be detected. In order to define and distinguish between ML-based and DL-based IDS, the authors of [9] suggest an ontology for intrusion detection systems (IDS) that relies on data objects as its primary identifier. The concept of IDSs and how they are classified is initially defined in the survey. Afterwards, the metrics, benchmark datasets, and machine learning algorithms commonly utilised by intrusion detection systems are utilised. Major IDS concerns can be addressed utilising ML- and DL-based techniques, with the taxonomy system serving as a baseline.

Using a genetic algorithm (GA) and fuzzy C-means clustering (FCM), the authors of [10] presented a new approach to NIDS that exhaustively searched for an improved feature subset. The suggested hybrid approach made use of an improved feature subset, which was enhanced by FCM to calculate new features. Through the integration of GA with five-fold cross-validation, the strategy selects the CNN model structure, and it also finds that the bagging classifier is an effective extractor. Feature subsets are provided to classifiers via deep learning CNN models, and their performance is validated using five-fold cross-validation. [11-12] Using a three-layered feature architecture that combines GA, FCM, and CNN extractors significantly enhances the final detection accuracy. This improvement is further supported by a hybridised CNN and bagging BG learning approach.

3. DEEP LEARNING APPROACHES-BASED CYBER SECURITY ATTACKS DETECTION SYSTEMS

This section provides a full description of the intrusion detection systems that utilise deep learning techniques. As illustrated in Figure 1, eleven distinct deep learning algorithms are employed in cyber security intrusion detection. A few examples are: 10) replicator neural network, 7) deep auto-encoder, 8) deep migration learning, 9) self-taught learning, 3) recurrent neural network, 4) convolutional neural network, 5) restricted Boltzmann machine, 6) deep belief network, 7) deep neural network, 2) feed forward neural network, 3) recurrent neural network, 4) convolutional neural network.

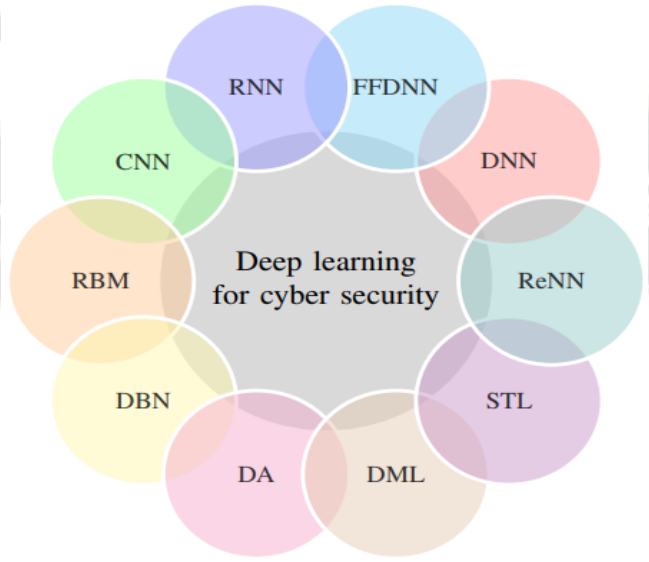


Fig. 1: Deep learning approaches used for cyber security intrusion detection.

A. Deep discriminative models

1) Deep neural networks (DNNs): A multi-layer perceptron (MLP) with additional layers is called a deep neural network (DNN). An MLP is a specific kind of feed forward artificial neural network, defined by its n successive layers (Figure 2).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

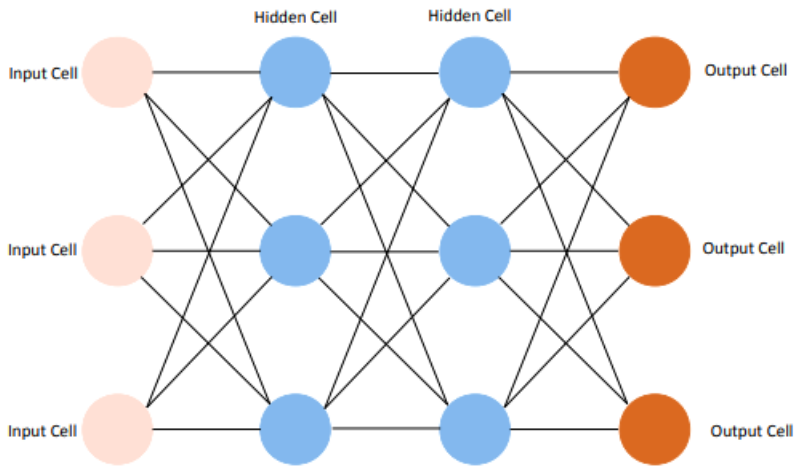


Fig. 2: Neural network with several layers.

Figure 2 displays the initial MLP-based deep neural network approach, approach 1.

Algorithm 1 DNN network based on MLP

1: Choose a learning pair $(x,\ c)$;
2: $h_0 = x$;
3: **for** $M = 1$ to N **do**
4: $g_M = n_M(h_{M-1}) = W_M \times h_{M-1} + b_M$;
5: $h_M = \alpha_M(g_M)$
6: **end for**

2) Recurrent neural networks (RNNs): Recurrent neural networks are networks of neurons that include at least one cycle in their connection graph. Several RNN types have been suggested, including Elman networks, Jordan networks, and Echo State networks. At the moment, the most popular RNN architecture is LSTM-based.

3) Convolutional neural networks (CNNs): Figure 3 shows an example of a convolutional neural network, which takes higher-resolution feature extraction and uses them to train a network with lower-resolution features that are more complicated. Numerous convolutional neural networks (CNNs) exist, with some examples being ResNet, GoogleNet, and ZFNet.

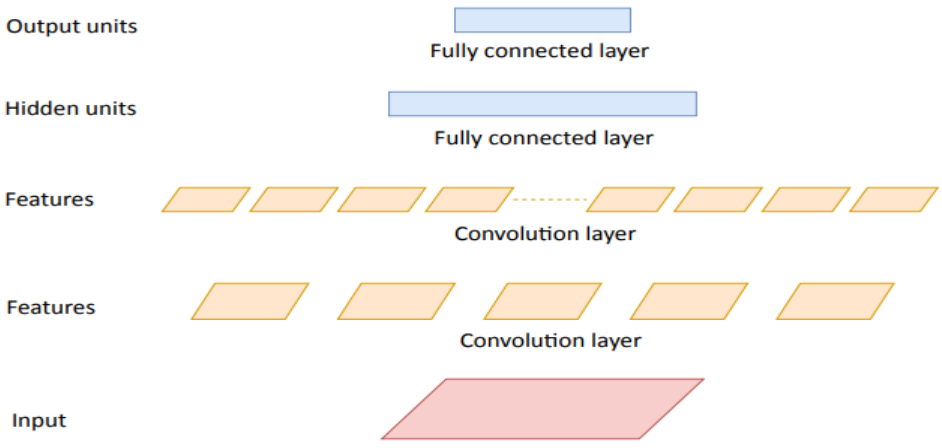


Fig. 3: Convolutional neural network.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

2) Deep belief networks (DBNs): The DBN, depicted in Figure 4, is a multi-layer belief network with Restricted Boltzmann Machines as its individual layers. The DBN consists of two layers: one with visible units and one with concealed units. The data is represented by the visible unit layers. A feature representation is learned by the layer of hidden units.

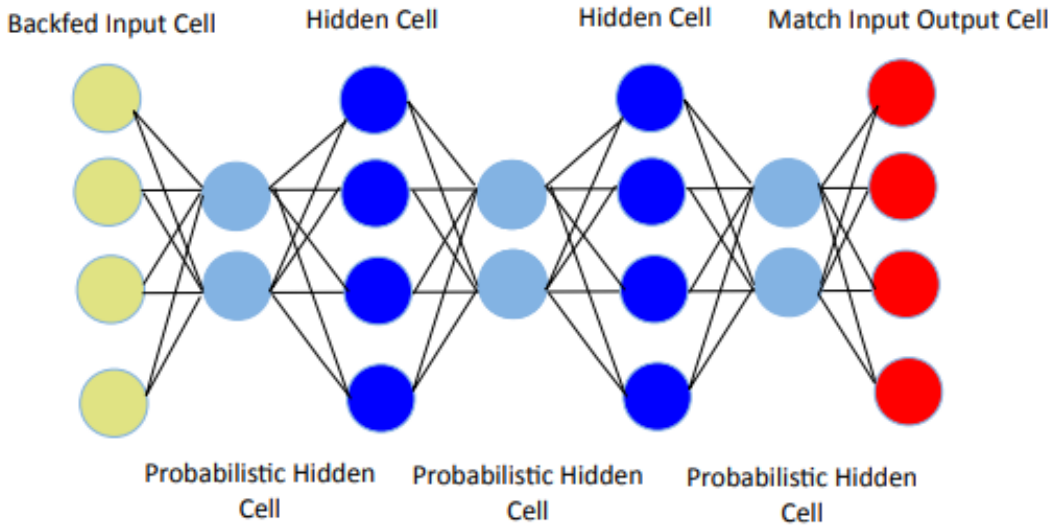
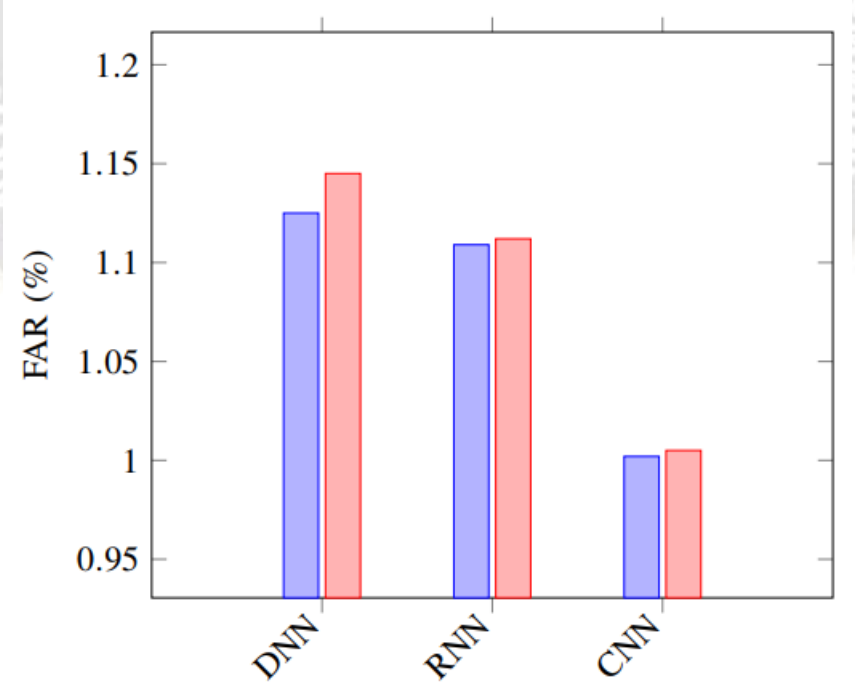


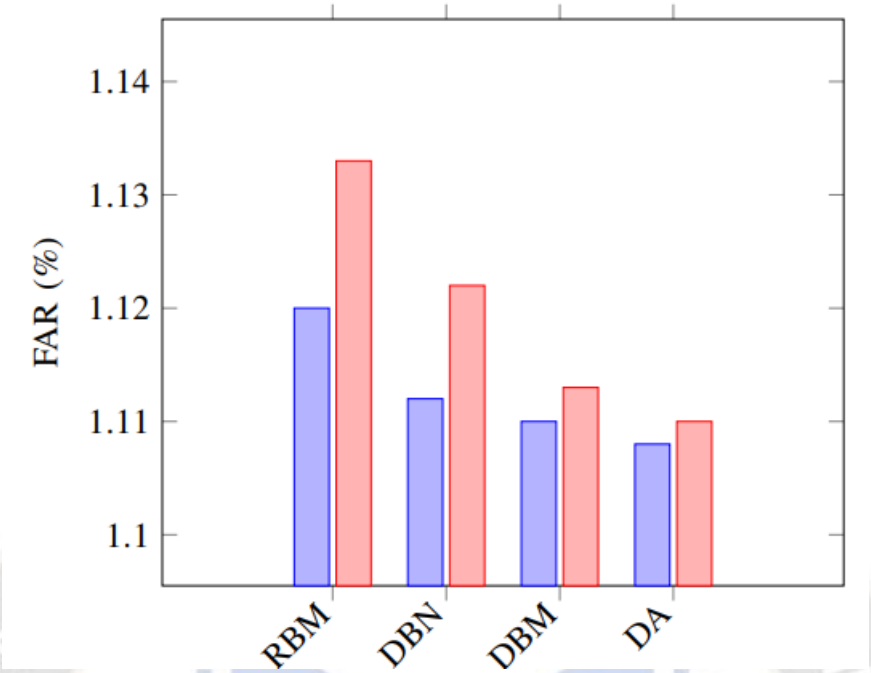
Fig. 4: Deep belief network.

4. RESULTS AND DISCUSSION



(a) Deep discriminative models

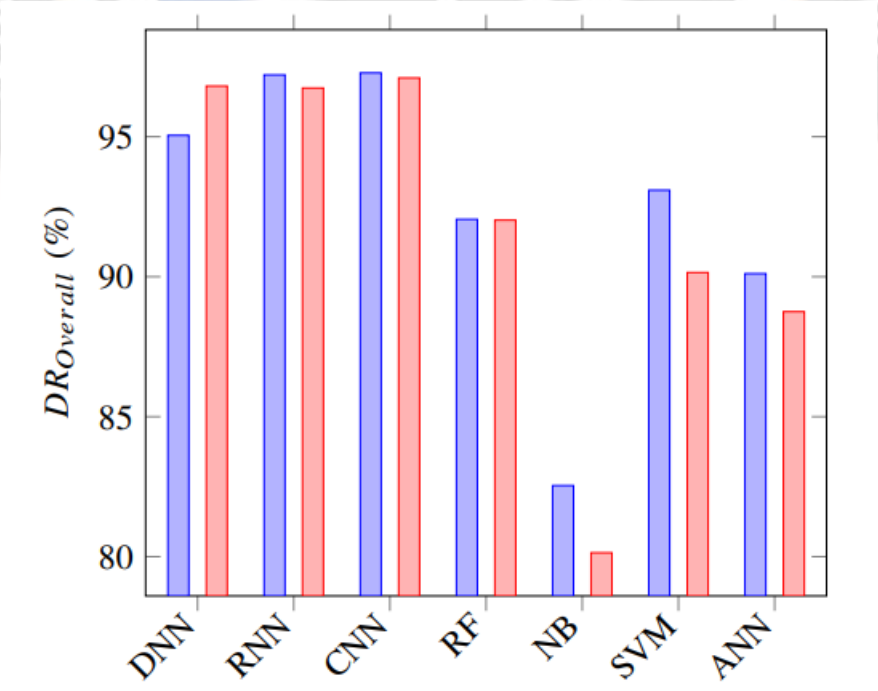
International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*



(b) Generative/unsupervised models

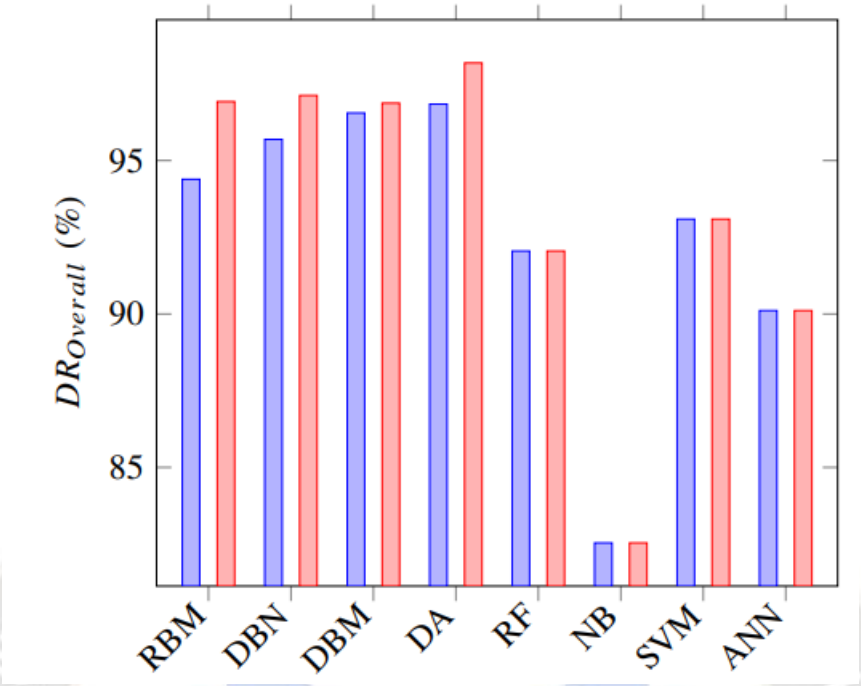
Fig. 5: The effectiveness of deep learning methods with respect to the number of false alarms

Figure 5 shows the results of deep learning methods in both the CSE-CIC-IDS2022 and Bot-IoT datasets with regard to the false alarm rate. When it comes to generative/unsupervised models, convolutional neural networks outperform deep and recurrent networks in terms of mean false alarm rate.



(a) Deep discriminative models

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*



(b) Generative/unsupervised models

Fig. 6: Results of several machine learning methods evaluated against deep learning methods in terms of global detection rate.

TABLE 1: Deep discriminative models' training times and accuracy across a range of learning rates and hidden nodes

Parameters	Accuracy and training time (s)	DNN	RNN	CNN
HN = 15 LR=0.01	ACC	96.446%	96.765%	96.900%
	Time	56.5	70.7	65.3
HN = 15 LR=0.1	ACC	96.651%	96.882%	96.912%
	Time	66.6	92.6	91.3
HN = 15 LR=0.5	ACC	96.651%	96.884%	96.910%
	Time	88.1	102.5	101.1
HN = 30 LR=0.01	ACC	96.611%	96.877%	96.919%
	Time	88.1	102.5	101.1
HN = 30 LR=0.1	ACC	96.655%	96.882%	96.921%
	Time	102.2	150.4	144.2
HN = 30 LR=0.5	ACC	96.661%	96.898%	97.101%
	Time	170.3	222.1	221.7
HN = 60 LR=0.01	ACC	96.766%	96.955%	97.102%
	Time	250.8	331.2	339.6
HN = 60 LR=0.1	ACC	96.922%	96.974%	97.212%
	Time	302.9	377.1	366.2
HN = 60 LR=0.5	ACC	97.102%	97.291%	97.881%
	Time	391.1	451.2	412.2
HN = 100 LR=0.01	ACC	97.221%	97.618%	97.991%
	Time	600.2	801.5	812.2
HN = 100 LR=0.1	ACC	97.501%	97.991%	98.121%
	Time	711.9	1001.8	1022.1
HN = 100 LR=0.5	ACC	98.221%	98.311%	98.371%
	Time	991.6	1400.6	1367.2

Table 1 displays the results of training deep discriminative models using the Bot-IoT dataset with varying learning rates and hidden nodes, along with their corresponding accuracy. An impressive 98.371% accuracy is achieved by a convolutional neural network when trained with 100 hidden nodes and a half-speed learning algorithm. On top of that, deep neural networks always have a shorter training period than similar approaches like recurrent neural networks and convolutional neural networks.

CONCLUSION

This study discusses the application of deep learning techniques to intrusion detection and compares two types of models: deep discriminative models and generative/unsupervised models. We zeroed down on seven distinct deep learning techniques, including recurrent neural networks, deep belief networks, deep convolutional neural networks, autoencoders, and deep Boltzmann machines. To compare these machine learning algorithms, we employ two new datasets, the CSE-CIC-IDS2022 dataset and the Bot-IoT dataset. We also use three critical performance measures, which are the false alarm rate, accuracy, and detection rate.

REFERENCES

1. [1] L. A. Maglaras, K.-H. Kim, H. Janicke, M. A. Ferrag, S. Rallis, P. Fragkou, A. Maglaras, and T. J. Cruz, “Cyber security of critical infrastructures,” ICT Express, vol. 4, no. 1, pp. 42–45, 2018.
2. [2] A. Ahmim, M. Derdour, and M. A. Ferrag, “An intrusion detection system based on combining probability predictions of a tree of classifiers,” International Journal of Communication Systems, vol. 31, no. 9, p. e3547, 2018.
3. [3] A. Ahmim, L. Maglaras, M. A. Ferrag, M. Derdour, and H. Janicke, “A novel hierarchical intrusion detection system based on decision tree and rules-based models,” arXiv preprint arXiv:1812.09059, 2018.
4. F. Feng, X. Liu, B. Yong, R. Zhou, and Q. Zhou, “Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device,” Ad Hoc Networks, vol. 84, pp. 82–89, 2019.
5. [19] S. Mahdavifar and A. A. Ghorbani, “Application of deep learning to cybersecurity: A survey,” Neurocomputing, 2019.
6. Jiang, K.; Wang, W.; Wang, A.; Wu, H. Network Intrusion Detection Combined Hybrid Sampling with Deep Hierarchical Network. *IEEE Access* **2020**, *8*, 32464–32476. [**Google Scholar**] [**CrossRef**]
7. Kaja, N.; Shaout, A.; Ma, D. An intelligent intrusion detection system. *Appl. Intell.* **2019**, *49*, 3235–3247. [**Google Scholar**] [**CrossRef**]
8. Liu, H.; Lang, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Appl. Sci.* **2019**, *9*, 4396. [**Google Scholar**] [**CrossRef**]
9. Nguyen, M.T.; Kim, K. Genetic convolutional neural network for intrusion detection systems. *Future Gener. Comput. Syst.* **2020**, *113*, 418–427.
10. Sinha, U.; Gupta, A.; Sharma, D.K.; Goel, A.; Gupta, D. Network Intrusion Detection Using Genetic Algorithm and Predictive Rule Mining. In *Cognitive Informatics and Soft Computing*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 143–156
11. Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW’16)
12. R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D. Dissertation.University of South Alabama