International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

A Novel Deep Learning Model to Enhance Network Traffic Monitoring for Cybersecurity

Abhijit Das[1], Pramod[2]

Submitted: 06/06/2022 **Accepted:** 10/09/2022

Abstract

The data amount flowing through computer networks at any specified period is referred to as network traffic. Data packets are broken down into networks traffic and transmitted over a network before being reconstructed by the receiving computers or devices. In the present time, network traffic has become a major problem of rapid increment in network devices which creates complexity in networking data. So, to overcome this problem, the author gives the method which is linked with deep learning methods and will also help to monitor the network traffic for cybersecurity. This paper gives the deep learning method which helps to find the network traffic as well as providing the cybersecurity to that network. The suggested method contains the deep learning method (DLM), convolutional neural network (CNN), recurrent neural network (RNN) and Long Short-Term Memory (LSTM). The method provides better accuracy results for observing the network traffic and also provides cybersecurity by using deep learning methods. This research shows that deep learning techniques can be used to build massive deep learning techniques for networks classification that can be applied in the real world where they can preserve classifying accuracy and increase classification speed considering restricted resource availability.

Keywords: Cyber Security, Deep Learning, Monitoring, Networks, Traffic.

1. Introduction

Over the past few decades, Internet Service Providers (ISPs) around the world have seen a rapid increase in network activity. Our communities have become increasingly entwined with multiple networking networks in sequence to carry out their various daily operations activities. Promising innovations like 5G are making rapid progress in the development of connections among our computers. With every passing year, this process will accelerate the evolution of network communications infrastructure [1]. Because of the high dependency on information networks, the technology has become a prime threat to the privacy of cyber security, which can also have a greater effect. Our community cannot depend on conventional malware detection and other scanning methods, which are becoming outdated in a complex and massive amount of network traffic scenarios, to provide reliable classifications in networks protection systems.Deep learning methods are particularly better from a large number of named samples for networking. Training a large deep learning method necessitates a considerable amount of computing power. The field of controlled learning has expected a lot of attention and study in the last decade. In the actual world, supervised models simplify well, if the system is identical with the o[1]ne in which the end-to-end models are trained, so it assumes common data and computing resources that sustain its output. The natural world is non-deterministic, with an infinite amount and pattern that the deep learning model cannot see [2]. To navigate through such settings and execute with the best precision and tempo, learning techniques would need prior knowledge of the tasks and related domains. With the exponential increment of the Internet, the number of cyber-attacks on networks and information infrastructure has skyrocketed. Intrusion prevention mechanisms are used in network infrastructure to protect against these threats Intrusion Detection Systems (IDS) [3]. Though IDSs are becoming more important in defending against increased network threats, payload-based IDSs have optimal control drawbacks, leading to increased networks speed and traffic. Cyber threats on networks and information infrastructure have escalated dramatically in tandem with the exponential development

[1] Research Scholar, VTU, PESITM, Shimoga-577205, Department of CSE, Karnataka, INDIA, Email ID: abhijit.tec@gmail.com

[2] Associate Professor, PESITM, Shimoga-577205, VTU, Department of ISE, Karnataka, INDIA, Email ID: pramod741230@gmail.com

of the Internet. (IDS) are used in network infrastructure to protect against these threats. With the speedy growth of the Internet, the cyber-attack on network and communication technology has increased significantly. To protect against these attacks, network architecture employs intrusion detection systems (IDS) [4]. While IDSs have become more critical in combating increased network attacks, payload-based IDSs have limitations in terms of optimization, resulting in increased networks speed and traffic.

Cyber security refers to a set of laws, strategies, technology, and procedures that operate together to ensure the secrecy, privacy, and availability of computer infrastructure, networks, software systems, and records. At the programme, network, host, and data levels, cyber security mechanisms exist. Firewalls, antivirus applications, intrusion detection systems (IDSs), and intrusion protected systems are only few techniques that operate in tandem to block threats and track security breaches. Many attackers, on the other hand, seem to have an edge because they just need to locate one flaw in the networks that need to be protected [5]. The attacking chances grow as the number of World Wide Web structures grows, posing a greater threat of attack. Additionally, attackers are getting more advanced, creating zero-day bugs and malware that disable security measures and enable them to operate for long durations without being detected. Zero-day vulnerabilities are threats that have never been used before but are frequently variants of a proven threat [1]. To make matters worse, attack strategies are being reformed, allowing for accelerated deployment without requiring knowledge of how to create exploits.

Instead of external attacks, safeguards must also protect against cyber threats by persons or groups within an entity that exploit their permitted access. There are markers of vulnerability in an attack's lifespan, and there can also be major warnings of an imminent attack [6]. The difficulty lies in locating these markers, which can be dispersed in the community. Machine-to-machine and human-to-machine communications produce vast data from apps, servers, mobile devices, and several cyber-enabled infrastructures [7]. Cyber protection tools, including the Security Information Event Management (SIEM) scheme, generate a lot of data, and can easily confuse a security analyst with event notifications [8]. The application of data science to computer security will aid in the correlation of incidents, the identification of trends, and the detection of anomalous activity, both of which can serve to strengthen the security culture of any defense programme. We are starting to see the cyber security systems that use data mining evolve [9]. Network intrusion detection systems (NIDS), for example, are changing from certain signature-based systems that monitor well-known threats to the anomaly-based programs that detect anomalies from a "standard" activity profile.

This paper discusses the Deep Learning model to enhance Network Traffic Monitoring for cybersecurity. Deep Learning is a modern and more dynamic process of learning, still being a subfield of machine learning. As a result, a detailed explanation of the Deep learning methods is provided, as well as comparisons to major works with each Deep Learning method. Highly cited papers were given special attention because they explain widely used methods. However, since this focus might lead to the omission of important new and evolving techniques, some lesser-known papers were selected as well. Overall the paper discusses the deep learning techniques which help to enhance network trafficking and monitoring cyber security issues.

2. Literature Review

Mahwish Amjad et al. discussed a deep learning system that can distinguish both identified and non-identified threats with a precision of up to 82 percent. In addition, the suggested structure would disclose the specific type of known attacks. The proposed architecture combines two deep learning algorithms, LSTM and Autoencoder, to create an efficient intrusion detection scheme. In this paper, the author proposed architecture in a real-time network would strengthen the future internet's stability [10]. Harsh Dhillon et al. explained the using different deep learning approaches. The main objective of this paper was to offer a new approach to designing a network intrusion detection system (NIDS). Authors use deep learning approaches to develop this proposed method to make it operative in real-world environments. Author transfer the information gained by their framework in a neural network with abundant computing and data assets to a feature space with restricted availability from both resources [11]. By using the UNSW-15 dataset, the suggested approach obtained a 98.30 percent classifying accuracy rate in source domains and an enhanced 98.43 percent classification accuracy of the target domain with the speed increase [12].

Wenjuan Wang et al. discussed the utilization of deep learning to retrieve relevant critical attributes representations and achieve high detection efficiency. For unsupervised features extraction, a stacked contractive Autoencoder (SCAE) scheme is introduced. The SCAE approach can be used to automatically extract better and more stable low-dimensional functionality from raw networks traffic [13]. The Support Vector machine (SVM) and the SCAE classification techniques were used to build a cloud network security scheme. The SCAE+SVM strategy blends shallow and deep learning approaches, maximizing their benefits to dramatically minimize

computational overhead [14]. Sultan Zavrak et al. discussed the research is to use the unsupervised approaches for deep learning along with a semi-supervised approach for learning to detect abnormal networks traffic through the flow dependent data. To detect attack patterns using flow characteristics, the Autoencoder methods and the Variational Autoencoder methods have been used. Flow-based functionality derived from the network's traffic data, involving traditional and specific kinds of attacks, has been used in the research. These techniques' Receiver Operating Characteristics (ROC) and areas under the ROC curve were determined and juxtaposed to the One-Class Support Vector Machine [15]. Daniel S. Berman et al. discussed the Deep Learning approaches for computer security applications that are defined in this survey paper. Deep Autoencoder, recurrent neural networks, restricted Boltzmann machines generative adversarial network, and other Deep Learning methods are all given a brief tutorial-style definition. After that, the author goes into how every one of the Deep Learning approaches is used in security applications. Malware, spam, internal attacks, network intrusions, fake data intrusion, and fake domain names that use malware are only a few of the threat vectors authors protect [16].

Research Questions

- What is the need for deep learning to monitor network trafficking?
- How do deep learning techniques provide cyber security to network trafficking?

3. Methodology

Deep learning CNNs, ANNs, Intrusion Prevention Systems (IPS) and Intrusion Detection System (IDS) have positive findings to search for suspicious behaviour in an analysis of Hypertext Transfer Protocol (HTTP) networks traffic[17]. It is useful for dealing with several cyber challenges like injections of structured Query Language (SQL) and Disk Operating System (DOS) attacks. Figure 1 shows the data analyzing process.

Figure 1. This diagram shows the data analyzing process that defines the goals, collect the data, preprocesses the data and after that selects the features of the data.

3.1 Intrusion Detection and Prevention Systems (IDS/IPS)

This identifies programmes and avoids malicious network operations and the use of intruders. Usually, recognized signatures and generic modes of attack are remembered. Threats such as data hacks are valuable for these data breaches. Machine Learning algorithms have traditionally been used for this role [18]. However, these algorithms created many false positives in the method, development and excessive exhaustion caused fastidious work for security firms. Deep learning, Convolutional neural network (CNN) and recurring neural network can be used to develop intelligent Intrusion Detection and Prevention Systems systems by providing a more precise analysis of traffic, decreasing the number of fake alarms and assisting security teams to distinguish positive and negative events in the network [19].

3.2 Deep Learning

Deep learning belongs to the wider field of artificial intelligence as a phenotype of machine learning (ML). Deep learning depends on artificial neural networks (ANNs) that imitate neurons in the human brain function and communication. Deep learning is named because of the fact that it uses larger networks than other Artificial Intelligence approaches such as ML[20]. The number of layers in an ANN sets the network's width. For example, a CNN utilized for many machine viewing activities is one of the most popular forms of ANNs. Different approaches have been tested for deep learning. An amalgamation of CNN, DNN and RNN was the finest prediction model [21].

3.3 Convolutional Neural Network

The author has utilized this metaphor for images processing to extend the technology for particular datasets. To do this, the matrix generated by the time series of the characteristic vector is used as an image. The image pixel is locally associated; likewise, function vectors relative to successive time slots are associated with local behaviour [22]. A multi-dimensional array is generated for each layer, where the image dimensions are reduced but a new dimension is generated, which is proportional to the numbers of filters added to the images, for that new dimension. The following CNN layer would further reduce the image proportions and improve the current dimensions [23]. The Tensor (primary data structure) has to be transformed to vectors to be the inputs for the ultimate fully associated levels in order to complete the model. A basic tensor flattening can be achieved to achieve this transformation (Figure 2).

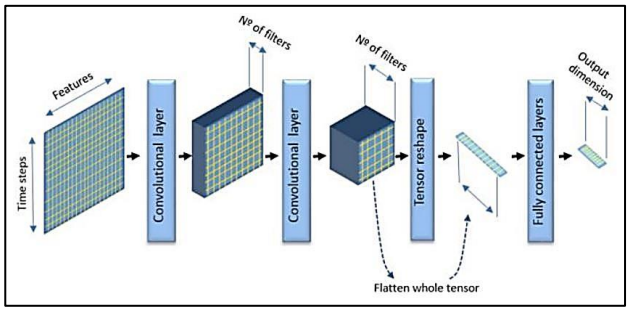

Figure 2. In this diagram shows the convolutional neural network with the tensor reshape fully connected and gives outputs of given dimensions [24].

3.4 Recurrent Neural Network

A single RNN was the first studied model (Figure 3). The author has used an RNN version called LSTM in particular, which is more convenient to train (it will assist in addressing the issues with fading gradients.). LSTM is formed with a two-dimensional matrix of value: the time dimension and characteristic vectors. LSTM is based on neural (cell) networks using the chronological character vectors and the two more cell and inner cell vectors. The cell's last hidden condition is its output value. Performance of LSTM layers is therefore similar to its hidden internal state in size (LSTM unit) [25]. Many completely related layer to the model of Figure. 3 at the top. When each and every node of the last layer is totally linked to each nodes of the successive layer, two layers are completely connected. Both versions have been completed with the completely linked layers.

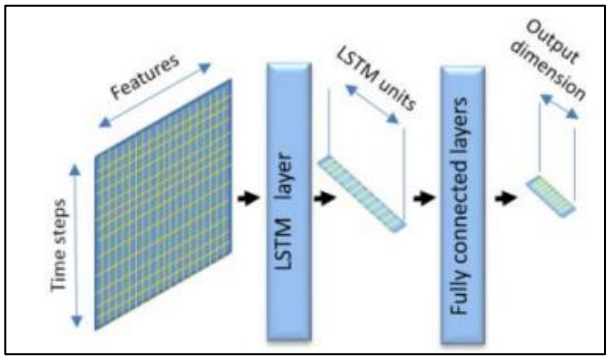

Figure 3. This diagram shows the recurrent neural network with the Long Short-Term Memory are fully connected layer gives the output dimension[24].

In this study, our selected profound education framework for the IDS/IPS contains the CNN, LSTM RNN and fully associated layer units for forecasting labels of category. In Figure 4, the proposed combined IDS models may use the benefits of the three distinct deep learning techniques to incorporate the ability to retrieve latent features, maintain memory and accurately classify them with the models implemented independently [26]. The combination of DNN, RNN, CNN and LSTM were studied in the past in which the frameworks are individually trained and later combined with their results. Researchers work together with every model to include the processed function performances as an input for the proposed algorithm in our approach.

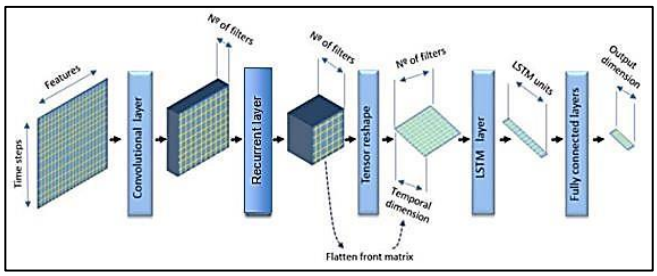

Figure 4. The above diagram shows the combination of the CNN, RNN and LSTM in which convolutional and recurrent layer tensors reshape to the LSTM layer and they all are fully connected.

These flow included 100 separate, strongly imbalanced frequency distribution labeling services. For various most common services, Figure 5 displays the identities and frequency distribution. The propagation of the frequencies is dependent on the flow rate of a given service. The networks stream contains all the packets sharing the single two-way mix of Internet Protocol (IP) addresses and port numbers for source and destination and transports: TCP (Transmission Control Protocol) and the UDP (User Datagram Protocol). Our packages are encrypted as algorithms do not depend on the payload contents considered.

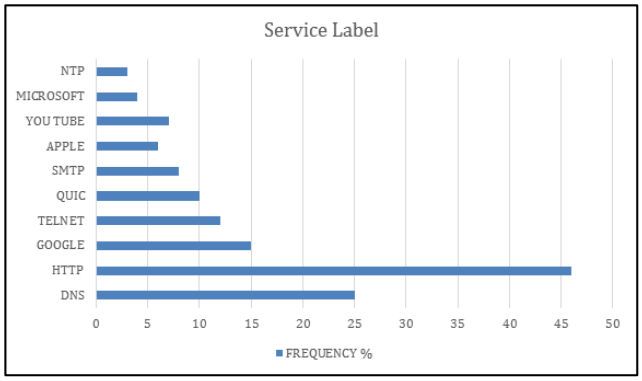

Figure 5. This graph shows the service label of different networking platforms and also shows the frequency percentage of the given services.

The author has a Virtual Machine cluster on the Google Cloud Platform (GCP) for our experimentation used in the n1-standard-16 VM Cluster Case, which has 16 vCPUs and a range of 30GB, Keras Frameworks with TensorFlow 1.15 in the back end for our profound learning libraries and used Scikit-learn and Pandas libraries for data preprocessing and manipulation. The tests were conducted with Jupyter integrated development environment (IDE)

and Python 3.7 notebook. The researcher used another domain to better replicate a scarce resource domain.

3.5 Performance Evaluation

So, in this to calculate the performance which is applied in the given model, the author will use procedures namely Confusion Matrix, Classification Accuracy and Recall curve briefly described as follows,

Accuracy: It is a metric used by classifications models since they equate the number of valid estimates to the overall number of predicted results. The consistency of classification can be indicated as,

$$Accurracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Confusion matrix: It is the graphic representation for the efficiency of a classifications algorithm, and uses four main categories to express the result of the method. True Positive corresponds to the expected value, which is positive and thus true. False-positive corresponds to the expected positive but the negative and therefore false values. Real negative applies to the expected negative value, which is negative and therefore valid. False negatives are the values that were expected to be positive and therefore false, but that is negative.

$$Confusion\ Matrix = \frac{TP}{TP + FP}$$

Recall curve: It is a design with two dimensions compared, true positives and false positives. The curve of recall. True positive rates, also called as model sensitivity, calculate the proportions of positive values that were properly defined by the model as positive.

$$Recall = \frac{TP}{TP + FN}$$

4. Result And Discussion

The findings obtained during multiple deep neural networks are presented in this section at network traffic classifier (NTC). The effect and the numbers of data packets retrieved from network traffic are analyzed, especially: model infrastructure, the feature vectors and the number of data packets. In Table 1 the architectures are defined and in Figure 6 the output measurements are presented. From Figure 6, the best results for the precision and the F1 can be seen from the model CNN+DNN+RNN-2a. Table 1 gives the following architectural description: of the model used in network traffic for monitoring with different deep learning techniques like CNN, DNN, RNN and LSTM.

Table 1. The Given Table Shown the Deep Learning Models Which Is Applied on the Network Traffic Classifier.

Model Used in Network Traffic for Monitoring
RNN-1
CNN-1
DNN-1
CNN+RNN+DNN-2
CNN+RNN+DNN-2a
CNN+RNN+DNN-3
CNN+RNN+DNN-3a
CNN+RNN+DNN-4
CNN+RNN+DNN-5

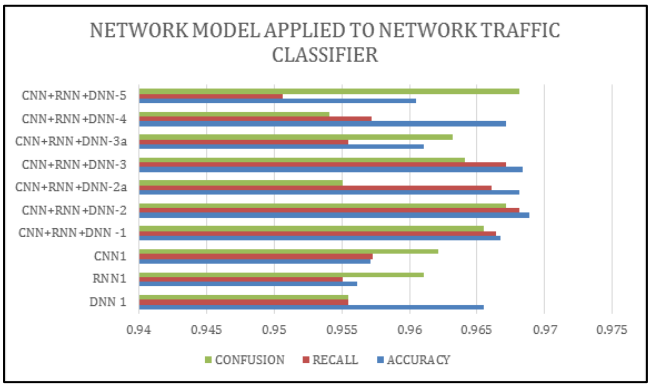

Figure 6. The Above Graph Shows the Classification Performance of the Network Model Which Is applied On the Network Traffic Classifier By Using Different Deep Learning Models.

Accuracy 0.9632 precision, 0.9644 recall, 0.9663 precision, and a 0.9712 reminder (model CNN&RNN-2a) were achieved by the proposed accuracy. Through analyzing data, it shows good results for the identification of both accuracy and consistency of a single model, consisting of two CNN layers accompanied by an LSTM layer with two completely connected layers at the bottom. Batch normalization in between the CNN layer and the incorporation at the end of the network of certain dropout layers enhance the performance. They have 108 separate service tags to identify this issue. This is a challenge with multiple classes. The author carried out a benchmark analysis on three profound learning models: CNN, RNN, DNN and LSTM for choosing the IDS root data structures. Our results showed a 94.16% overall accuracy of CNN model on the input data validation dataset, while an 89.66% accuracy of DNN architecture. A 98.30 percent precision range that exceeds other models was seen by CNN's architecture of LSTM layers in its secret layers. Author selected the model RNN, CNN-LSTM to enhance the network traffic and provide that network cybersecurity.

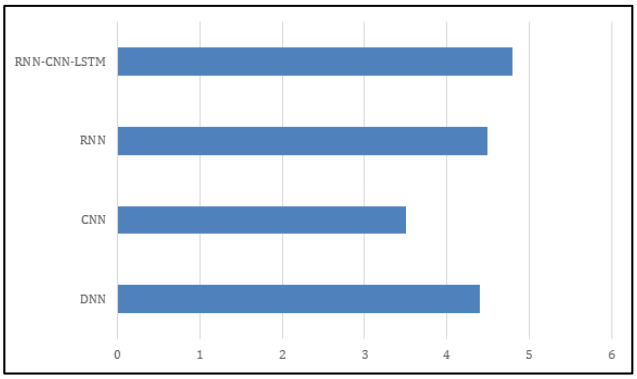

Figure 7. The above graph shows the accuracy of the deep learning models for the initial source which are CNN, RNN and LSTM.

Accuracy alone cannot be the best success assessment method. Authors have thus used the RNN, CNN-LSTM architecture uncertainty matrix to analyze the profound effects of classification. The RNN, CNN-LSTM models show a 1.47 percent false-positive and 0.79 percent false-negative score, according to the uncertainty matrix. False categories have been important for IDS because systems may incorrectly identify malicious files as regular ones and lead to effective infrastructure infiltration scenarios. The author uses the RNN, CNN-LSTM model structure in the source domain, along with its focus on understanding, and passes them to the models in the target domain for the implementation of information in the destination region. In this domain, the Researcher can use the unexamined test data collection to represent the IDS model in a true framework where new information is found. This helps to assess the reaction of the framework as it is implemented in a real-world infrastructure. Our tests show that by using trained sources, the average efficiency and speed of systems in the target field is increased. A better precision score of 89% was seen in the Deep Neural Network structure, compared to a 93.88% precision score for the CNN architecture. The accuracy of 98.43 percent of our CNN-LSTM nominee model is better than other simulations used in this field. Figure 8 shows the accuracy of the deep learning models for the destination source which are CNN, RNN and LSTM.

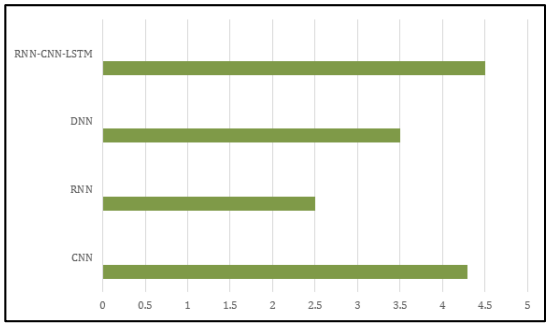

Figure 8. The above graph shows the accuracy of the deep learning models for the destination source which are CNN, RNN and LSTM.

The CNN-LSTM model also showed improved outcomes with a general decrease in the and false-negative and false-positive rates. The complete model has a false-positive 0.96%, and false-negative 0.64% rates, which improves packet identification. Table 2 provides the overview of the performance of the three learning algorithms, CNN, DNN, RNN and CNN-RNN-LSTM for our benchmark research. From our results, researchers found that RNN, CNN-LSTM conducted other implemented model with a 99.03 percent accuracy score in the source domain and an accuracy of destination score of 99.42 percent in the aim domain. Currency management represents the capacity of the model to use and implement the weights acquired from the source domain on an unseen test dataset. Despite the virtual data and computing resources' lack of the target domain, test speed also increased.

Table 2. This table shows the accuracy of the given model which helps to find the accuracy by applying the CNN, RNN, DNN AND LSTM.

	Source		**Destination**	
Deep Learning Methods	**Accuracy**	**Speed**	**Accuracy**	**Speed**
RNN	89.99%	30.8s	89.6%	12.01s
CNN	93.17%	130.1s	93.1%	17.3s
DNN	89.67%	31.2s	89.6%	1.15s
RNN-CNN-LSTM	99.03	175.8s	99. 42%	21.1s

5. Conclusion

Our research shows that using a deep learning approach to create unified networks intrusion detection systems that manage and enhance classification speed and accuracy in a simulated real-world setting through information transfer is highly successful. A basic RNN model still produces excellent results, but it's worth noting when RNN models are paired with prior CNN models, the result increases even further. The ability to enhance results by using a CNN demonstrates our initial intuition, which helped us to integrate the vectors time-series derived from networks packets' attributes and CNNs are therefore suitable candidates for communicating with vectors time-series of comparable manner. Since deep learning methods are rich source of modern models. After verifying our model's performance, designers can move its design and learn weights to a neural network with less computing resources, where the author see that the framework retains its efficiency while improving testing speed. This simulates a real-world situation in which author are using a portion of the datasets that our models have never seen during their preparation and development. In future work, author

would like to incorporate feature extraction methods into the current deep learning methods and test the suggested model and techniques using a variety of modern networks intrusion datasets.

Acknowledgement

The authors whose works are cited and included in the references to this manuscript are acknowledged by the authors for their enormous assistance. The authors would also want to express their gratitude to the writers, editors, and publishers of all the books, papers, journals, and other sources used in the review and discussion of the literature for this work.

References

[1]. G. Nguyen, S. Dlugolinsky, V. Tran, and A. Lopez Garcia, "Deep learning for proactive network monitoring and security protection," *IEEE Access*, vol. 8, pp. 19696–19716, 2020, doi: 10.1109/ACCESS.2020.2968718.

[2]. I. Sohn, "Deep belief network based intrusion detection techniques: A survey," *Expert Systems with Applications*. 2021, doi: 10.1016/j.eswa.2020.114170.

[3]. M. Abbasi, A. Shahraki, and A. Taherkordi, "Deep Learning for Network Traffic Monitoring and Analysis (NTMA): A Survey," *Computer Communications*. 2021, doi: 10.1016/j.comcom.2021.01.021.

[4]. Y. Chen *et al.*, "An Optimizing and Differentially Private Clustering Algorithm for Mixed Data in SDN-Based Smart Grid," *IEEE Access*, 2018.

[5]. I. M. Venter, R. J. Blignaut, K. Renaud, and M. A. Venter, "Cyber security education is as essential as 'the three R's,'" *Heliyon*, 2019, doi: 10.1016/j.heliyon.2019.e02855.

[6]. M. S. Abu, S. R. Selamat, A. Ariffin, and R. Yusof, "Cyber threat intelligence – Issue and challenges," *Indones. J. Electr. Eng. Comput. Sci.*, 2018, doi: 10.11591/ijeecs.v10.i1.pp371-379.

[7]. M. Medvedeva, M. Vols, and M. Wieling, "Using machine learning to predict decisions of the European Court of Human Rights," *Artif. Intell. Law*, 2020, doi: 10.1007/ s10506-019-09255-y.

[8]. N. Miloslavskaya and A. Tolstoy, "New SIEM system for the internet of things," 2019, doi: 10.1007/978-3-030-16184-2_31.

[9]. A. Brogi *et al.*, "Survey High-Performance Modelling and Simulation for Selected Results of the COST Action IC1406 cHiPSet," *Futur. Gener. Comput. Syst.*, 2018.

[10]. M. Amjad, H. Zahid, S. Zafar, and T. Mahmood, "A novel deep learning framework for intrusion detection system," *2019 Int. Conf. Adv. Emerg. Comput. Technol. AECT 2019*, 2020, doi: 10.1109/AECT47998.2020.9194224.

[11]. G. Nguyen, S. Dlugolinsky, V. Tran, and A. Lopez Garcia, "Deep learning for proactive network monitoring and security protection," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2968718.

[12]. H. Dhillon and A. Haque, "Towards network traffic monitoring using deep transfer learning," *Proc. - 2020 IEEE 19th Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2020*, pp. 1089–1096, 2020, doi: 10.1109/TrustCom50675.2020.00144.

[13]. P. Guo, Z. Liu, H. Lu, and Z. Wang, "Hyperspectral Image Classification Based on Stacked Contractive Autoencoder Combined with Adaptive Spectral-Spatial Information," *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3095265.

[14]. S, R. D., L. . Shyamala, and S. . Saraswathi. "Adaptive Learning Based Whale Optimization and Convolutional Neural Network Algorithm for Distributed Denial of Service Attack Detection in Software Defined Network Environment". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 6, June 2022, pp. 80-93, doi:10.17762/ijritcc.v10i6.5557.

[15]. W. Wang, X. Du, D. Shan, R. Qin, and N. Wang, "Cloud Intrusion Detection Method Based on Stacked Contractive Auto-Encoder and Support Vector Machine," *IEEE Trans. Cloud Comput.*, pp. 1–1, 2020, doi: 10.1109/tcc.2020.3001017.

[16]. Rosemaro, E. . (2022). Understanding the Concept of Entrepreneurship Management and Its Contribution in Organization. International Journal of New Practices in Management and Engineering, 11(01), 24–30. https://doi.org/10.17762/ijnpme.v11i01.159

[17]. S. Zavrak and M. Iskefiyeli, "Anomaly-Based Intrusion Detection from Network Flow Features Using Variational Autoencoder," *IEEE Access*, vol. 8, pp. 108346–108358, 2020, doi: 10.1109/ACCESS.2020.3001350.

[18]. D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A survey of deep learning methods for cyber security," *Inf.*, vol. 10, no. 4, 2019, doi: 10.3390/ info10040122.

[19]. Chaudhary, D. S. . (2022). Analysis of Concept of Big Data Process, Strategies, Adoption and Implementation. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(1), 05–08. https://doi.org/10.17762/ijfrcsce.v8i1.2065

[20]. M. Särelä, T. Kyöstilä, T. Kiravuo, and J. Manner, "Evaluating intrusion prevention systems with evasions," *Int. J. Commun. Syst.*, 2017, doi: 10.1002/dac.3339.

[21]. M. Hasan, M. M. Islam, M. I. I. Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet of Things (Netherlands)*, 2019, doi: 10.1016/j.iot.2019.100059.

[22]. X. Wang, S. Chen, and J. Su, "Real Network Traffic Collection and Deep Learning for Mobile App Identification," *Wirel. Commun. Mob. Comput.*, 2020, doi: 10.1155/ 2020/4707909.

[23]. H. Li, Z. Zhang, and Z. Liu, "Application of artificial neural networks for catalysis: A review," *Catalysts*. 2017, doi: 10.3390/catal7100306.

[24]. L. Wang, L. Zhang, and J. Jiang, "Duplicate Question Detection with Deep Learning in Stack Overflow," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2968391.

[25]. Paithane, P. M., & Kakarwal, D. (2022). Automatic Pancreas Segmentation using A Novel Modified Semantic Deep Learning Bottom-Up Approach. International Journal of Intelligent Systems and Applications in Engineering, 10(1), 98–104. https://doi.org/10.18201/ijisae.2022.272

[26]. M. Aazam *et al.*, "Fog computing - Glimps of Upcoming Research Area (#4)," *Futur. Gener. Comput. Syst.*, 2017.

[27]. J. Gu *et al.*, "Recent advances in convolutional neural networks," *Pattern Recognit.*, 2018, doi: 10.1016/j.patcog.2017.10.013.

[28]. Sally Fouad Shady. (2021). Approaches to Teaching a Biomaterials Laboratory Course Online. Journal of Online Engineering Education, 12(1), 01–05. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/43

[29]. M. Lopez-Martin, B. Carro, A. Sanchez-Esguevillas, and J. Lloret, "Network Traffic Classifier with Convolutional and Recurrent Neural Networks for Internet of Things," *IEEE Access*, vol. 5, pp. 18042–18050, 2017, doi: 10.1109/ACCESS.2017.2747560.

[30]. Degambur, L.-N., Mungur, A., Armoogum, S., & Pudaruth, S. (2022). Resource Allocation in 4G and 5G Networks: A Review. International Journal of Communication Networks and Information Security (IJCNIS), 13(3). https://doi.org/10.17762/ijcnis.v13i3.5116

[31]. L. Aziato and H. O. Antwi, "Facilitators and barriers of herbal medicine use in Accra, Ghana: An inductive exploratory study," *BMC Complement. Altern. Med.*, 2016, doi: 10.1186/s12906-016-1124-y.

[32]. M. Cai and J. Liu, "Maxout neurons for deep convolutional and LSTM neural networks in speech recognition," *Speech Commun.*, 2016, doi: 10.1016/j.specom.2015.12.003.