Paper ID: 331

Survey on Deep learning based Network Intrusion Detection and Prevention Systems

MAT Padmasiri, VVV Ganepola, RKHMSD Herath, LP Welagedara, GANS Ganepola and P Vekneswaran#

Informatics Institute of Technology, No.57, Ramakrishna road, Colombo 06, Sri Lanka

veknesp@westminister.ac.uk

Abstract: Where world is moving towards digitalization, it is crucial that network intrusions detection and prevention is addresses in ordered to create a secured network. This paper covers why deep learning was considered and what are the deep learning approaches for network intrusion detection. For each approach the challenges, missed elements and the unique features that are found in current domain state are also highlighted. As a conclusion this paper highlights why CNN and LSTM would be successful approach for intrusion detection and why in the current domain context it is required to create scalable solution with both intrusion detection and prevention involved.

Keywords: Network Intrusion Detection and Prevention System, Deep Learning, NSL-KDD

Introduction

Introduction and evolution of network technologies in the past decades have resulted in a massive growth in Internet technologies. As a result, the ways for intruders to tamper and obstruct the consumers in their day to day network-based activities have increased as well. (Alom, Bontupalli and Taha, 2015) Intrusive behavior is when the confidentiality, integrity and availability of a network resource is exposed and hindered to its intended user. Network Intrusion Detection and Prevention System (NIDPS) come into the picture when providing a defense against any activity that compromises the three factors mentioned above. It can be classified into two categories based on the deployment (Samrin and Vasumathi, 2017) location.

- Host Intrusion Detection System (HIDS)
- Network Intrusion Detection System (NIDS)

HIDS (e.g. Commercial Anti-Virus Software) is deployed in its host and is capable of processing specific data. (i.e. Operating System's audit trails and system logs). HIDS suffers from high resource usage leading to performance drop in the host machine. NIDS on the other hand, performs better being deployed as an external access point.

NIDS is extended further to use Anomaly Detection and Signature Based Detection. Anomaly Based Detection is the analysis of network data to classify whether the data is intrusive (anomaly) or non-intrusive(normal). Signature based detection is based on prior knowledge, where unique patterns of intrusions are generated and updated for intrusion detection daily.

Paper "Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification" specifies that current research lacks explanation of proactive measures that are taken to handle Denial of Service intrusions (Chandre, Mahalle and Shinde, 2018). Paper "Adaptive Fuzzy Neural Network Model for intrusion detection" highlights that the domain lacks a solution which can handle a large flow on network data and detection, hence it is required to

focus on a scalable solution. (Kumar and Mohan, 2014)

Methodology

The paper aimed at analyzing existing research of the domain in order to gain the domain knowledge and understand the current state of the domain. Existing research has been analyzed based on different machine learning paradigms such as deep learning, shallow learning and autoencoders. It was done to understand the current domain context and therefore to identify which approach suits more for intrusion detection. This information would be elaborated further in section III. In this paper, existing approaches based on Supervised and Unsupervised learning have been discussed mainly. Different algorithms falling under these 2 categories are extensively researched to arrive into the conclusion.

Related Works

When analyzing related works, it is required to understand the relevant datasets that are being used in the context of the domain and what data science approaches were used.

A. Datasets in the domain

There are several datasets that were identified in the analysis such as NSL-KDD, UNSW-NB15, KDD CUP 99, CICIDS2017, CTU-UNB, CIDDS-001 etc. Out of them, NSL-KDD was widely used across the research. NSL-KDD (Alom, Bontupalli and Taha, 2015) dataset is an improvement of KDD CUP 99 dataset, which has solved some issues such as duplication of data and such as in its predecessor. NSL-KDD dataset provides 41 attributes depicting different features in network flow. 125973 and 22544 records are available on NSL-KDD training and testing dataset respectively. NSL-KDD dataset's (Rama Devi and Abualkibash, 2019) 42nd feature which would provide the class specifying if it is a normal class or the attack type class which are mentioned below.

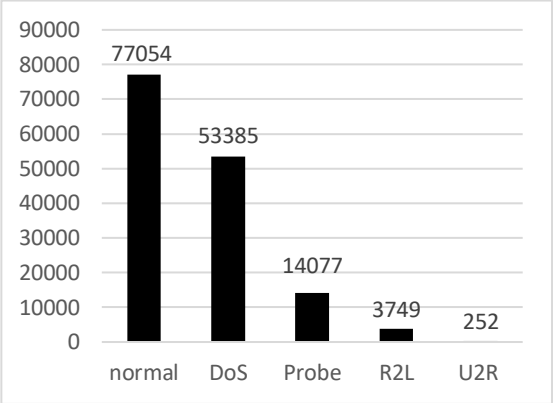


Figure 1: NSL-KDD dataset

"Intrusion detection using deep belief networks" (Alom, Bontupalli and Taha, 2015) provides more information relating to each dataset that are available in the current domain such as CICIDS, CAIDA. "Feature selection in UNSW-NB15 and KDDCUP'99 datasets" (Janarthanan and Zargari, 2017) provides details about UNSW-NB15 which is said to provide more features on modern attack types than NSL-KDD.

B. Data Science Approaches

This survey is based on deep learning approaches due to certain facts identified during early research. Shallow learning model, the counterpart of deep learning models as mentioned in "A comparison between shallow and deep architecture classifiers on small dataset" (Pasupa and Sunhem, 2016) does not tend to perform well with larger dataset size whereas deep learning models do. "MLSEC - Benchmarking Shallow and Deep Machine Learning Models for Network Security" compares both shallow models and deep learning models where it has showed that deep learning model managed be up to par with other shallow learning models. (Casas et al., 2019) Deep learning models can be either be Supervised or Unsupervised learning approach.

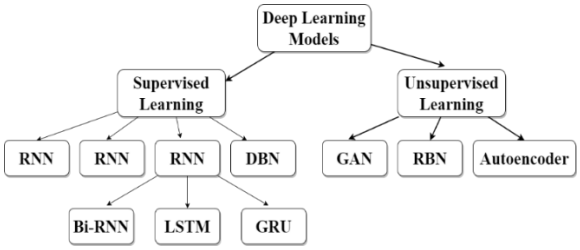


Figure 2: Taxonomy in use of Deep learning in Intrusion Detection

Existing works of Intrusion detection domain can be mainly categorized into two based on the approach.

1) Supervised Learning: In supervised learning, the model is trained and validated on a labelled dataset. There, algorithms will understand and learn the data based on patterns. After training the model, it determines which label is to be given for the new raw data based on the patterns identified during the training phase (Alom, Bontupalli and Taha, 2015). Deep Belief Network (DBN), Deep Neural Network (DNN), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM) and other variations of RNN such as Gated recurrent units (GRU) and Bi-RNN are based on supervised learning.

DBN contains both multiplayer unsupervised network and a supervised network which are Restricted Boltzmann Machine and Back-propagation respectively. "An Intrusion Detection Model Based on Deep Belief Networks" uses a Network Intrusion Detection Model Based on DBN utilizing KDD CUP 1999. Results of this research provides an accuracy of 93.49% and true positive rate of 92.33% and false positive rate of 0.76 (Gao et al., 2014). "Intrusion Detection using Deep Belief Network" research paper utilized NSL-KDD dataset where 97.5% testing accuracy was yielded. (Alom, Bontupalli and Taha, 2015)

"Deep Learning Approach for Network Intrusion Detection in Software Defined Networking", this research paper provides results of a DNN model using NSL-KDD dataset, accuracies of the proposed model were 75.75% for 5 intrusions class classification. Researchers conclude lower accuracy rate could be as a result of lack of proper features selection. (Tang et al., 2016)

CNN can be used for both feature extraction and network packet classification (Hsu et al., 2019). "Intrusion detection Algorithm Based on Convolutional Neural Network" research paper (Liu, Liu and Zhao, 2018) provided detection rate of 99.96%. Considering "an Intrusion Detection System Based on Convolutional Neural Network" paper proposed a CNN model which used One Hot Encoding (OHE) encoding for feature matrix. One Hot Encoding is where rather than integer encoding where a unique integer is set for each category in categorical data, it provides a binary representation whether the specific category exists OHE provided more stable feature set resulting in 99% detection rate and false alarm rate of the mode low than 0.1%. According to the researcher, One Hot Encoding has improved the feature set which has provided higher accuracies than earlier feature set. (Liu, 2019)

"A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks" provides an RNN model for both binary and 5 class classification on NSL-KDD dataset.

68.55% and 64.67% detection accuracies on binary and multi class classifications respectively. (Yin et al., 2017) "Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection" paper RNN model proposed a training method (Hessian Free Optimization). (Kim et al., 2016). KDD CUP 99 resulting in accuracy of a 95.37% and false alarm rate was 2.1%. Later RNN was further extended down with improvements, namely those are LSTM, GRU and Bi-RNN (Cui et al., 2018).

Even though results of these models were promising, KDD CUP 99 as mentioned contains redundant data and opting RNN for its improved predecessor LSTM which would be explained below.

As mentioned earlier RNN was improved in solving vanishing gradient and exploding gradient problem, LSTM which can learn long-term dependencies was one of these improvements. (Hsu et al., 2019) LSTM uses activation function layers which act as gates which allows the LSTM to remember previous information. "Long Short-Term Memory Recurrent Neural Network Classifier for Intrusion Detection" (Kim et al., 2016) proposed LSTM-RNN with KDD Cup 99 dataset resulted in 10.08% false alarm rate and accuracy of 96.93%. "LSTM for Anomaly-Based Network Intrusion Detection" (Althubiti, Jones and Roy, 2018) proposed an LSTM model using CIDDS-001 for a multi-class classification which provided results of accuracy of 0.8483 and precision of 0.8514 and false alarm rate of 0.172.

LSTM as said can retain dependencies in its memories, according to the researchers' opinion this feature should be very valuable in a network intrusion domain where varying packers could flow and ability to retain its patterns should provide a performance gain. The above statement could be verified in a real-world end to end product which can capture live traffic and detect intrusions through said model but referenced research doesn't provide any implementation of such.

2) Unsupervised Learning: Unsupervised is based on unlabeled data, these algorithms work without any pre known Dataset (Rama Devi and Abualkibash, 2019). Autoencoders, Generative Adversarial Network (GAN) and Restricted Boltzmann machine (RBN) algorithms analyses how unsupervised learning was utilized in detection.

"Network Anomaly Detection with Stochastically Improved Autoencoder Based Models" (Aygun and Yavuz, 2017) specifies that Autoencoders can be categorized further down as stacked, sparse and denoising autoencoders and autoencoders relies on encoding and decoding phases in classifying. Above mentioned research proposed denoising autoencoder based on NSL-KDD which has resulted accuracy of 88.65%." Network Intrusion Detection through Stacking Dilated Convolutional Autoencoders" (Yu, Long and Cai, 2017) proposed method was a convolutional based autoencoder model which used CTU-UNB dataset. This approach has shown capability in processing huge volume of traffic data with 98.62% accuracy. As mentioned, the above research has addressed the issue in handling large network volumes, which was not addressed or considered in other researches.

"Efficient GAN-Based Anomaly Detection" (Zenati et al., 2019) proposed a GAN model which relies on generator (ability to generate data) and discriminator (verifying and validating generated data based on real data) concept in classifying which provides a precision of 0.92, recall and F1 score of 0.9582 and 0.9372 respectively. While considering the analysis on unsupervised algorithms such as GAN and Autoencoders there weren't ample research available. It is believed that due to the availability of multiple datasets supervised learning can be adapted easily and that it would be reliable to use a dataset which already provides intrusions rather than relying on an unlabeled approach with unsupervised learning.

Boltzmann machine (BN) is a bi-directional connected network probability processing unit. In BN each node can be categorized as visual or hidden. Visible nodes represent components of surveillance. Hidden nodes gather dependencies between the visible

node that cannot create pairwise interactions between visible nodes. In BN learning process is too slow to be utilized in real-world applications. A class of narrow connectivity in BNs that has newly gained widespread attention is the Restricted Boltzmann machine (RBN). In RBN each hidden node is only connected to visible nodes. (Aldwairi, Perera and Novotny, 2018). When considering "An Evaluation of the Restricted Boltzmann Machines as a Model for Anomaly Network Instruction Detection" research paper evaluates the RBM machine learning model for a NIDS. To test this, researchers have used contrastive divergence (CD) algorithm and persistent contrastive divergence (PCD) algorithm. ISCX dataset using for validation, perform training and testing. According to a research result for CD and PCD were respectively as follows 88.6% and 89.7% as accuracy. 88.4% and 84.2% for the true positive rate. (Aldwairi, Perera and Novotny, 2018)

C. Notable Existing Research Analysis

Considering the above findings, furthermore relevant researches were scoped down that has shown promising results for network intrusion detection which were analyzed and summarized below.

Table 1: Notable Existing Research Analysis

LSTM for Anomaly-Based Network Intrusion Detection (Althubiti et al., 2018, p1–3)	Method	Model was evaluated using CIDDS 001 dataset which contains data from 13 features. Data from 10 of those features were used in this study. LSTM model was composed with input layer of 10 neurons corresponding to the 10 features, a hidden layer with 10 neurons and an output layer with 5 neurons. The hyper parameters set includes 0.01 learning rate, 6 hidden layers, 200 epochs and a batch size of 500 has being used. For this model optimizer called "rmsprop" has been used which is suitable for large datasets and efficient calculations. An Algorithmic comparison was performed using Precision, Recall, False positive rate (FPR) and Accuracy.
	Results	LSTM achieved 0.8713 training accuracy and 0.8483 testing accuracy. SVM, NB and MLP gained testing accuracy 0.7942, 0.7756, 0.8124 respectively. In LSTM FPR was higher than SVM and Naive bayes. LSTM performed well compared to Precision, Recall, Accuracy.
	Review	LSTM is a modified version of RNN which has resolved gradient descent problem. When compared with other Machine Learning models it is having the ability to learn long-term dependencies. In the research LSTM has performed better than SVM, Naive Bayes and MLP of large part due to its ability of learning long-term dependencies.
Using Long-Short-Term Memory Based Convolutional Neural Networks for Network Intrusion Detection (Hsu et al., 2019)	Method	Researchers have proposed two deep learning models that they have evaluated on NSL-KDD dataset. First model is a LSTM model and the other is a CNN-LSTM model.
	Results	CNN-LSTM model achieved higher accuracy compared to LSTM model for both binary classification and multiclass classification. Binary classification using KDDTest^{+} LSTM achieved an accuracy of 89.23% whereas the multi-class classification achieved 87.53%; KDDTest^{-21} binary and multiclass classification achieved an accuracy of 74.77% and 68.78% respectively. CNN-LSTM model achieved an accuracy of 94.12% and 88.95% for binary and multiclass classification. Using KDDTest^{+} Binary and multi-class classification achieved an accuracy of 79.37% and 70.13% for binary and multiclass classification. Both proposed models performed better than benchmarked RNN-IDS model.
	Review	CNN has been used for extracting feature vectors and passing it to the LSTM model as the input of the LSTM model. In this research, CNN has been used to learn spatial features in the data and LSTM has been used to learn temporal features.
A Deep Long Short-Term Memory based classifier for Wireless Intrusion Detection System (Kasongo and Sun, 2019)	Method	This DLSTM approach is compared to Feedforward Deep Neural Networks (FFDNNs), ANN, SVM, KNN, NB and RF. They have used NSL-KDD as the dataset and 18 features were selected.
	Results	DLSTM model achieved validation accuracy 99.51%, F1 score 99.43% and test accuracy 86.99% Model outperformed the LSTM-RNN IDS in "An Intelligent Network Attack Detection Method Based on RNN" (Fu et al., 2018) that had an accuracy of 97.52% on training data whereas the DLSTM RNN IDS achieved 99.51%.
	Review	In this research, they have done experiments between some of the shallow models and some deep DLSTM outperformed compared to all other models experimented in this solution. Based on the information revealed from the existing research analysis, DLSTM outperformed because of the algorithm logic and the structure. As per analysis, this model outperformed some of the other LSTM models like "An Intelligent Network Attack Detection Method Based on RNN" (Fu et al., 2018) due to the structure of the LSTM model. It consists of one LSTM layer and DLSTM model of this research consists of more than two LSTM layers such as three hidden layers.

D. Mitigation Approaches

Mitigation approach highlights the currently known and used approaches acting as a prevention mechanism for NIDPS. "A Practical Network-Based Intrusion Detection and Prevention System" model relies on Iptables Linux based tool that act as a firewall which can provide block and unblock rules for the system, hence after the detection it should either drop the packet or block the source IP address and port using IP Tables. (Wattanapongsakorn et al., 2012)

As mentioned, most of the research that was analyzed, did not contain a fully fetched end to end product which could be adapted to real world, hence few of the above said approaches were found in mitigation logics.

Conclusion

Above survey provides an overview of Deep learning models which are developed and evaluated on Intrusion Detection and Prevention domain. It is apparent that researched approaches do not focus much attention on proactive measures in prevention and early detection with real time for an end to end solution for the real world. Also, it is important to ensure NIDPS doesn't detect legitimate traffic as intrusions (False Positives) and vice versa the intrusions to be classified as legitimate traffic (False Negative).

Above facts shows that CNN and LSTM seems to provide higher accuracies and provides features such as LSTM being capable of remembering previous knowledge to improve its classifications. It is important to have a high accuracy as in a real-world scenario there would be massive amount of network traffic hence a drop-in accuracy of even 1 percent can reflect massive amount of missed detections. Usage of One Hot Encoding has improved the feature matrix and its stability during preprocessing as mentioned on CNN based model.

The main contribution of this paper is to review the existing research conducted on Network Intrusion Detection and Prevention Systems based on deep learning approaches, thus paving a pathway for researchers to conduct Future Research on this domain conveniently. This has been achieved by an effective classification of deep learning-based approaches, namely supervised and unsupervised learning.

Research has shown that as future work a scalable end to end solution can be implemented to detect and prevent intrusions and cover the drawbacks in this survey. The solution should answer the below mentioned research questions,

Can a machine learning/deep learning model for intrusion detection be used for live network traffic?

Is it possible for a real-time intrusion detection, if not what would be time taken for a detection?

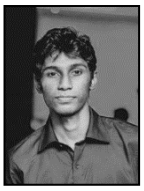
Acknowledgment

This research has benefited from numerous researches done prior in this field. We would specifically like to express our gratitude to Mr. Guhanathan Poravi, Mr Sharmilan Somasundaram, Mr. Malinda Kankanange and the faculty of Informatics Institute of Technology for providing expertise and guidance throughout this research.

Author Biographies

Prathieshna Vekneswaran ('93) received the B.Eng. Honours in Software Engineering (Sandwich) from IIT, Sri Lanka affiliated with UOW, UK in 2016 and pursued his Master of Science in Advanced Software Engineering in the same, completing it in 2018. He is currently working as a Senior Software Engineer in 99x Technology (Private) Limited, Colombo, Sri Lanka and been lecturing research methods

in various reputed Institutions in Sri Lanka in part time mode.



Avishka Thushan Padmasiri is a final year Software Engineering undergraduate at Informatics Institute of Technology, Sri Lanka. He currently works as a Software Engineer at Pearson Lanka (Private) Limited. He pursues research on Cyber Security and Machine Learning.

Vayangi Vishmi Vishara Ganepola is a final year Software Engineering undergraduate at Informatics Institute of Technology, Sri Lanka. She currently works as a Scholar at Applied Research and Development Team at Pearson Lanka (Private) Limited. She pursues research on Machine Learning and AI.

RKHM Salitha Dilshan Herath is a final year Software Engineering undergraduate at Informatics Institute of Technology, Sri Lanka. He currently works as a Senior Software Engineer (iOS) at Spemai (Private) Limited. He pursues research on Machine learning, Mobile and IOT.

Lahiru Welagedara is a final year Software Engineering undergraduate at Informatics Institute of Technology, Sri Lanka. He currently works as an Associate Software Engineer (Scholar) at IFS R&D International (Private) Limited. He pursues research on Machine Learning, Blockchain, Edge Computing and IOT.

GA Nipuna S Ganepola is a final year Computer Science undergraduate at Informatics Institute of Technology, Sri Lanka. Hs research interests include Cyber Security and Machine Learning.

References

Aldwairi, T., Perera, D. and Novotny, M. A. (2018) 'An evaluation of the performance of Restricted Boltzmann Machines as a model for anomaly network intrusion detection', Computer Networks, 144, pp. 111–119. doi: 10.1016/j.comnet.2018.07.025.

Alom, Md. Z., Bontupalli, V. and Taha, T. M. (2015) 'Intrusion detection using deep belief networks', in 2015 National Aerospace and Electronics Conference (NAECON). NAECON 2015 - IEEE National Aerospace and Electronics Conference, Dayton, OH, USA: IEEE, pp. 339–344. doi: 10.1109/NAECON.2015.7443094.

Althubiti, S. A., Jones, E. M. and Roy, K. (2018) 'LSTM for Anomaly-Based Network Intrusion Detection', in 2018 28th International Telecommunication Networks and Applications Conference (ITNAC). 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), Sydney, NSW: IEEE, pp. 1–3. doi: 10.1109/ATNAC.2018.8615300.

Aygun, R. C. and Yavuz, A. G. (2017) 'Network Anomaly Detection with Stochastically Improved Autoencoder Based Models', in 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 193–198. doi: 10.1109/CSCloud.2017.39.

Casas, P. et al. (2019) 'MLSEC - Benchmarking Shallow and Deep Machine Learning Models for Network Security', in 2019 IEEE Security and Privacy Workshops (SPW). 2019 IEEE Security and Privacy Workshops (SPW), pp. 230–235. doi: 10.1109/SPW.2019.00050.

Chandre, P. R., Mahalle, P. N. and Shinde, G. R. (2018) 'Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification', in 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN). 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India: IEEE, pp. 135–140. doi: 10.1109/GCWCN.2018.8668618.

Cui, J. et al. (2018) 'WEDL-NIDS: Improving Network Intrusion Detection Using Word Embedding-Based Deep Learning Method', in Torra, V. et al. (eds) Modeling Decisions for Artificial Intelligence. Cham: Springer International Publishing (Lecture Notes in Computer Science), pp. 283–295. doi: 10.1007/978-3-030-00202-2_23.

Fu, Y. et al. (2018) 'An Intelligent Network Attack Detection Method Based on RNN', in 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou: IEEE, pp. 483–489. doi: 10.1109/DSC.2018.00078.

Gao, N. et al. (2014) 'An Intrusion Detection Model Based on Deep Belief Networks', 2014 Second International Conference on Advanced Cloud and Big Data, pp. 247–252.

Hsu, C.-M. et al. (2019) 'Using Long-Short-Term Memory Based Convolutional Neural Networks for Network Intrusion Detection', in Chen, J.-L. et al. (eds) Wireless Internet. Cham: Springer International Publishing (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), pp. 86–94. doi: 10.1007/978-3-030-06158-6_9.

Janarthanan, T. and Zargari, S. (2017) 'Feature selection in UNSW-NB15 and KDDCUP'99 datasets', in 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE). 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), pp. 1881–1886. doi: 10.1109/ISIE.2017.8001537.

Kasongo, S. M. and Sun, Y. (2020) 'A Deep Long Short-Term Memory based classifier for Wireless Intrusion Detection System', ICT Express, 6(2), pp. 98–103. doi: 10.1016/j.icte.2019.08.004.

Kim, Jihyun et al. (2016) 'Long Short Term Memory Recurrent Neural Network Classifier for Intrusion Detection', in 2016 International Conference on Platform Technology and Service (PlatCon). 2016 International Conference on Platform Technology and Service (PlatCon), pp. 1–5. doi: 10.1109/PlatCon.2016.7456805.

Kumar, K. S. A. and Mohan, V. N. (2014) 'Adaptive Fuzzy Neural Network Model for intrusion detection', in 2014 International Conference on Contemporary Computing and Informatics (IC3I). 2014 International Conference on Contemporary Computing and Informatics (IC3I), pp. 987–991. doi: 10.1109/IC3I.2014.7019811.

Liu, P. (2019) 'An Intrusion Detection System Based on Convolutional Neural Network', in Proceedings of the 2019 11th International Conference on Computer and Automation Engineering - ICCAE 2019. the 2019 11th International Conference, Perth, WN, Australia: ACM Press, pp. 62–67. doi: 10.1145/3313991.3314009.

Liu, Y., Liu, S. and Zhao, X. (2018) 'Intrusion Detection Algorithm Based on Convolutional Neural Network', DEStech Transactions on Engineering and Technology Research, (iceta). doi: 10.12783/dtetr/iceta2017/19916.

Meena, G. and Choudhary, R. R. (2017) 'A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA', in 2017 International Conference on Computer, Communications and Electronics (Comptelix). 2017 International Conference on Computer, Communications and Electronics (Comptelix), Jaipur, India: IEEE, pp. 553–558. doi: 10.1109/COMPTELIX.2017.8004032.

Pasupa, K. and Sunhem, W. (2016) 'A comparison between shallow and deep architecture classifiers on small dataset', in 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE). 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE), pp. 1–6. doi: 10.1109/ICITEED.2016.7863293.

Rama Devi, R. and Abualkibash, M. (2019) 'Intrusion Detection System Classification Using Different Machine Learning Algorithms on KDD-99 and NSL-KDD Datasets - A Review Paper', International Journal of Computer Science and Information Technology, 11(03), pp. 65–80. doi: 10.5121/ijcsit.2019.11306.

Samrin, R. and Vasumathi, D. (2017) 'Review on anomaly based network intrusion detection system', in 2017 International Conference on Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT). 2017 International Conference on

Electrical, Electronics, Communication, Computer, and Optimization Techniques (ICEECCOT), Mysuru: IEEE, pp. 141–147. doi: 10.1109/ICEECCOT.2017.8284655.

Tang, T. A. et al. (2016) 'Deep learning approach for Network Intrusion Detection in Software Defined Networking', in 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM). 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Fez, Morocco: IEEE, pp. 258–263. doi: 10.1109/WINCOM.2016.7777224.

Wattanapongsakorn, N. et al. (2012) 'A Practical Network-Based Intrusion Detection and Prevention System', in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 209–214. doi: 10.1109/TrustCom.2012.46.

Yin, C. et al. (2017) 'A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks', IEEE Access, 5, pp. 21954–21961. doi: 10.1109/ACCESS.2017.2762418.

Yu, Y., Long, J. and Cai, Z. (2017) 'Network Intrusion Detection through Stacking Dilated Convolutional Autoencoders', Security and Communication Networks, 2017, pp. 1–10. doi: 10.1155/2017/4184196.

Zenati, H. et al. (2019) 'Efficient GAN-Based Anomaly Detection', arXiv:1802.06222 [cs, stat]. Available at: http://arxiv.org/abs/1802.06222 (Accessed: 25 June 2020).