A Survey on Network Intrusion Detection using Convolutional Neural Network

Antanios Kaissar[1] Ali Bou Nassif[2] MohammadNoor Injadat[3]

[1] *Computer Engineering Dept. University of Sharjah, Sharjah, UAE. U19200543@sharjah.ac.ae*
[2] *Computer Engineering Dept. University of Sharjah, Sharjah, UAE. anassif@sharjah.ac.ae*
[3] *Electrical & Computer Engineering Dept. University of Western Ontario, London, ON, Canada. minjadat@uwo.ca*

ABSTRACT
Nowadays Artificial Intelligence (AI) and studies dedicated to this field are gaining much attention worldwide. Although the growth of AI technology is perceived as a positive development for the industry, many factors are being threatened. One of these factors is security, especially network security. Intrusion Detection System (IDS) which provides real-time network security has been recognized as one of the most effective security solutions. Moreover, there are various types of Neural Networks (NN) approaches for IDS such as ANN, DNN, CNN, and RNN. This survey mainly focuses on the CNN approach, whether individually used or along with another technique. It analyses 81 articles that were carefully investigated based on a specific criterion. Accordingly, 28 hybrid approaches were identified in combination with CNN. Also, it recognized 21 evaluation metrics that were used to validate the models, as well as 12 datasets.

Keywords: *Convolutional neural network, Intrusion detection system, Network security.*

1. INTRODUCTION

With the rapid evolution of the Internet and communication technologies, it has become a crucial aspect in almost every part of our life. This has significantly increased the amount of data being generated and dealt with, which in turn had led us to the era of "big data" [1]. Henceforth, it has become a challenging task to protect this data and its connection. Considering any corruption or lack of security during data transmission may lead to serious problems for individuals and organizations. Moreover, the variation of attack methods and the complexity of the network system have increased the difficulty of such task [2]. Therefore, researchers are investigating all the possible techniques and methods that could secure the continuous connection. An Intrusion Detection System (IDS) is one of the ideal solutions [3].

There are two main classes of IDS, the first one is Network-Based Intrusion Detection Systems (NIDS). This monitors the network traffic and alerts the network administrator whenever an attack is detected. While the second one is Host-Based Intrusion Detection Systems (HIDS). The HIDS scans each host device independently (not the network), it alerts the host in case of any suspicious packet detection [4]. This research is primarily concerned with NIDS which is divided into two main methods, misuse detection and anomaly detection. The misuse detection system must be pre-equipped with a set of attack signatures to detect them. Hence, it is not able to detect unknown attacks [5]. On the other hand, the anomaly detection system operates based on the normal usage patterns which allow it to detect the unknown attacks. Nonetheless, due to the process of defining multiple normal use patterns, the anomaly detection system has high false alarms. In other words, using a technique that can learn by itself such as Deep Learning (DL) models would enhance the anomaly detection system's ability to determine the normal use patterns. This will also be beneficial in reducing false alarms [6].

Fig. 1. [5] illustrates all machine learning algorithms where it's split into shallow and deep learning. CNN is a supervised deep-learning algorithm alongside other neural network types. It was used for the first time in intrusion detection by R. Upadhyay and D. Pantiukhin in 2017 [7]. Starting from that article until July 2021, this survey lists 81 articles that utilize CNN for IDS whether it was used alone or combined with another shallow or DL technique. To the best of our knowledge, no prior survey has addressed CNN specifically out of all the other DL techniques.

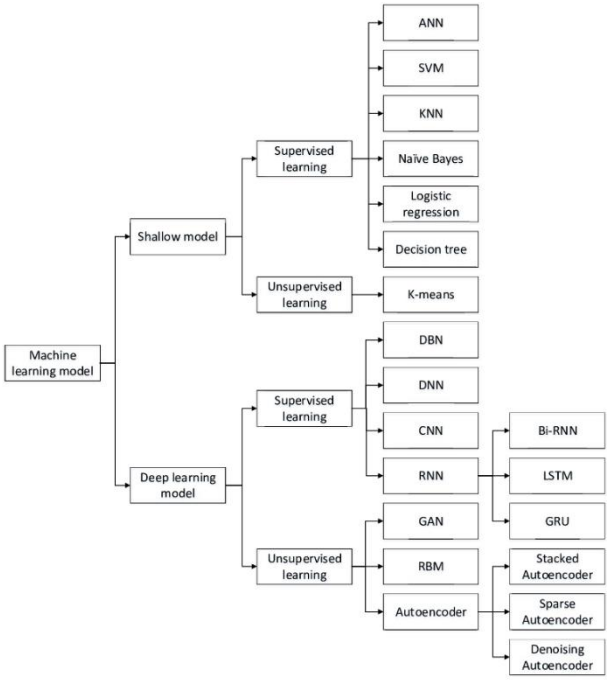

Figure 1 Machine learning algorithms [5].

2. RELATED WORK

There are several surveys that discussed intrusion detection using any DL or shallow techniques as shown in Fig. 1. There are more than 10 techniques, and many of them could be combined with other methods to come up with a hybrid model. Authors in [8] have discussed DL for cyber security intrusion detection. They reviewed 45 papers in total, 7 of them were using CNN. However, only 3 of them were specifically for network intrusion detection. S. Gamage and J. Samarabandu [9] have summarized 10 surveys as well as 41 articles, only 3 of them using CNN. Authors in [10] have investigated network attack detection methods. They reviewed 38 articles, 8 of them are using CNN, but only 5 of them are for intrusion detection. Authors in [3] have reviewed a total of 34 articles that uses neural networks for intrusion detection. However, CNN was present in one article only. L. Mahmoud and R. Praveen have discussed Artificial Neural Networks (ANN) for intrusion detection. They reviewed 8 articles in total, two of them used CNN. Ali et al. [11] summarized 22 articles that use DL techniques for intrusion detection. Nevertheless, CNN was available in two articles only.

Salo et al. [12] investigated data mining techniques in IDS covering 95 articles starting in year 2007 until 2016. Nonetheless, CNN was not present in any article of that SLR. Authors in [13] have discussed NIDS models and datasets in details by explaining each ML & DL technique separately. Their summary enclosed 35 articles that used various techniques for NIDS. However, only 5 of these articles used CNN. Zeeshan et al. [14] investigated both DL and ML techniques for intrusion detection. They reviewed 39 articles in total, 6 of them were using CNN. To that end, this SLR contribution can be summarized as follows:

1. It targets precisely the CNN technique for NIDS even if it was used alongside another technique.
2. It covers all the articles starting from the first article ever to use CNN for NIDS in 2017 until July 2021.
3. It summarizes the outcomes of selected articles to benefit the researchers in their future studies.

3. METHODOLOGY

Based on [15], the methodology of this survey is composed of three main stages which are planning, conducting, and reporting. The following subsections present the detailed implementation of this methodology. Fig. 2. illustrates the overall framework.

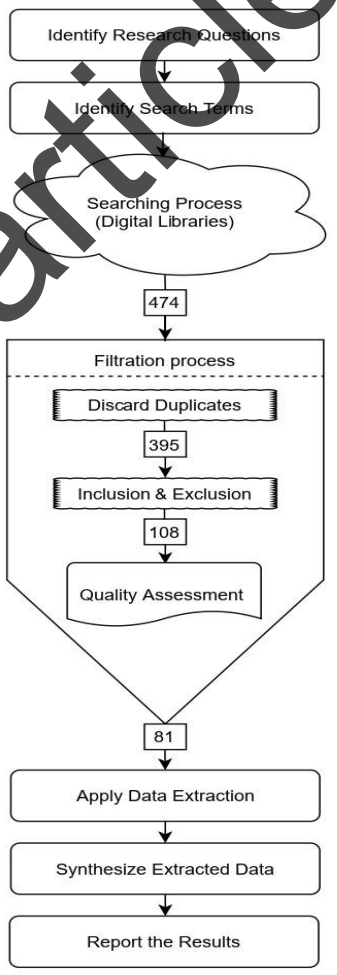

Figure 2 Research methodology.

3.1. Research Questions

To achieve our goal and analyze the articles successfully, we identified 3 research questions: RQ1: What are the hybrid techniques used in combination with CNN? RQ2: What are the datasets used to evaluate the model? RQ3: What are the evaluation metrics that are used to validate the technique?

3.2. Study Selection

This survey involves a comparative analysis of the related articles. The initial search across the digital libraries returned 474 articles. Then we started the filtration process by removing the duplicates. After that, we removed the unrelated articles by applying our inclusion and exclusion criteria. The inclusion rules are: 1) Include the articles that use CNN for NIDS even if it was combined with another method. 2) Include the articles during the period between Jan 2016 and July 2021. On the other hand, the exclusion rules are: 1) Exclude the articles that use CNN for IDS but for other systems such as surveillance, Internet of Vehicles (IOV), human/ animal detection, or any other irrelevant applications. 2) Exclude the articles that involve IDS in IoT environments. 3) Exclude any article that is not classified as peer-reviewed. After following this filtration process, we ended up with 108 articles that are ready for the quality assessment phase.

3.3. Quality Assessment Rules (QAR)

To classify the quality of the articles, we selected 10 questions where each of them is answered with a score maximum of 1 as "Excellent", 0.5 as "Good", and 0 as "Not explained". Q1: Is the research problem clearly described? Q2: Is the IDS idea clearly pinpointed? Q3: The authors have discussed related works? Q4: Is the used dataset clearly defined? Q5: Is the design of the proposed algorithm/architecture clearly explained? Q6: Is the algorithm/architecture presented precisely in figures and graphs? Q7: Are the reasons/justifications given for the selected parameters in the model? Q8: Does the research cover accurate evaluation parameters? Q9: Are there comparisons with other algorithms/models in terms of result accuracy? Q10: Is the future work pinpointed?

Based on these assessment questions, the 108 articles were evaluated to assure a sufficient result. The article with a score of 5 or above was selected for the next stage. Hence, a total of 81 articles were chosen for the data extraction stage.

3.4. Extract and Synthesize Data

The objective of this stage is to extract the required information to answer our research questions. We used methods obtained from [15] to present the collected information for answering the RQs. For all RQs, narrative synthesis was used. Moreover, the data was presented using bar charts and tables.

Table 1. Selected articles

Paper ID	Year	Ref.
P1	2017	[7]
P2	2017	[16]
P3	2017	[17]
P4	2017	[18]
P5	2018	[19]
P6	2018	[20]
P7	2018	[21]
P8	2018	[22]
P9	2018	[23]
P10	2018	[24]
P11	2018	[25]
P12	2018	[26]
P13	2018	[27]
P14	2018	[28]
P15	2019	[29]
P16	2019	[30]
P17	2019	[31]
P18	2019	[32]
P19	2019	[33]
P20	2019	[34]
P21	2019	[35]
P22	2019	[36]
P23	2019	[37]
P24	2019	[38]
P25	2019	[39]
P26	2019	[40]
P27	2019	[41]
P28	2019	[42]
P29	2019	[43]
P30	2019	[44]
P31	2020	[45]
P32	2020	[46]
P33	2020	[47]
P34	2020	[48]
P35	2020	[49]
P36	2020	[50]
P37	2020	[51]
P38	2020	[52]
P39	2020	[53]
P40	2020	[54]
P41	2020	[55]
P42	2020	[56]
P43	2020	[57]
P44	2020	[58]
P45	2020	[59]
P46	2020	[60]
P47	2020	[61]
P48	2020	[62]
P49	2020	[63]
P50	2020	[64]
P51	2020	[65]
P52	2020	[66]
P53	2020	[67]
P54	2020	[68]
P55	2020	[69]

P56	2020	[70]
P57	2020	[71]
P58	2020	[72]
P59	2020	[73]
P60	2020	[74]
P61	2020	[75]
P62	2020	[76]
P63	2020	[77]
P64	2020	[78]
P65	2021	[79]
P66	2021	[80]
P67	2021	[81]
P68	2021	[82]
P69	2021	[83]
P70	2021	[84]
P71	2021	[85]
P72	2021	[86]
P73	2021	[87]
P74	2021	[88]
P75	2021	[89]
P76	2021	[90]
P77	2021	[91]
P78	2021	[92]
P79	2021	[93]
P80	2021	[94]
P81	2021	[95]

4. RESULTS AND DISCUSSION

4.1. RQ1: What are the hybrid techniques used in combination with CNN?

The main objective of this question is to look for hybrid models. Therefore, the articles that considered improved CNN by adding specific layers or changing the activation function will not be discussed. Overall, we identified 28 techniques that were combined with CNN. The techniques are: Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), Bi-directional Long Short-term Memory (BiLSTM), Gated Recurrent Unit (GRU), Support Vector Machine (SVM), 1-Nearest Neighbor (1-NN), Genetic Algorithm (GA), Batch Normalization algorithm with Inception model, Synthetic Minority Oversampling combined with Edited Nearest Neighbors (SMOTE-ENN), Channel Boosted and Residual learning (CBR), gcForest, Stacked Denoising Autoencoder (SDA), Mean Convolution Layer (MCL), Multilayer Perceptron (MLP), (SGM-CNN) which is a combination of SMOTE with under-sampling for clustering based on Gaussian Mixture Model (GMM), Naive Bayes with Self Organizing Maps (SOM), Grey Wolf Optimization (GWO), eXtreme Gradient Boosting algorithm (XGBoost), Bayesian CNN (BCNN), Random Forest (RF), Dimensionality Reduction (DRCNN), Split Convolution Module (SPC-CNN), Adaptive Synthetic Sampling (ADASYN), Nondominated Neighbour Immune Algorithm (NNIA), Generation Adversarial Network (GAN), Residual Learning and Focal Loss (RLF), Convolutional Block Attention Module (CBAM), Packet Byte (PBCNN). Table II summarizes which articles used the hybrid models.

Table 2. Hybrid Models

Paper ID	Algorithm used
P2, P17, P74	CNN-RNN
P2, P4, P23, P28, P34, P36, P41, P44, P51, P58, P81	CNN-LSTM
P40	CNN+BiLSTM
P2, P44, P60	CNN-GRU
P12, P63	CNN-SVM/1-NN
P13, P38, P56	CNN-GA
P19	Batch Normalization algorithm with Inception model
P20, P67, P76	SMOTE
P21	CBR-CNN
P22	CNN + gcForest
P26, P50	CNN+SDA
P33	CNN-MCL
P42	CNN-MLP
P43	SGM-CNN
P45	Naive Bayes + SOM
P48	GWO + TreeCNN
P49	CNN-XGBoost
P54	Bayesian CNN
P60	Random Forest
P61	DRCNN
P64	AS-CNN & SPC-CNN
P65	CNN-NNIA
P71	RLF-CNN
P77	CNN+CBAM
P80	PBCNN

This table presents 41 articles that used hybrid models with CNN, which is approximately 50% of the total articles. Some articles used more than one hybrid model such as P2, P44, and P60. The most used hybrid model was CNN-LSTM in 11 articles. The rest 40 articles used CNN only, this includes different combinations of layers and activation functions.

4.2. RQ2: What are the datasets used to evaluate the model?

All the algorithms were tested on at least one dataset for IDS or more to evaluate the proposed model. There were 12 different datasets as presented in Fig. 3. used among all the 81 articles, these datasets are classified into three categories as follows[96]:

1. Virtualized: This type of dataset is developed artificially to perform a specific task, as most of its features are virtual or abstract such as the DARPA dataset [97].

2. Synthesized: This type of dataset is developed to meet particular conditions which could not be available in realistic datasets. Accordingly, it is very beneficial because the realistic datasets face privacy concerns.

3. Realistic: This type of dataset is collected from real-world traffic, which could be classified as private or public.

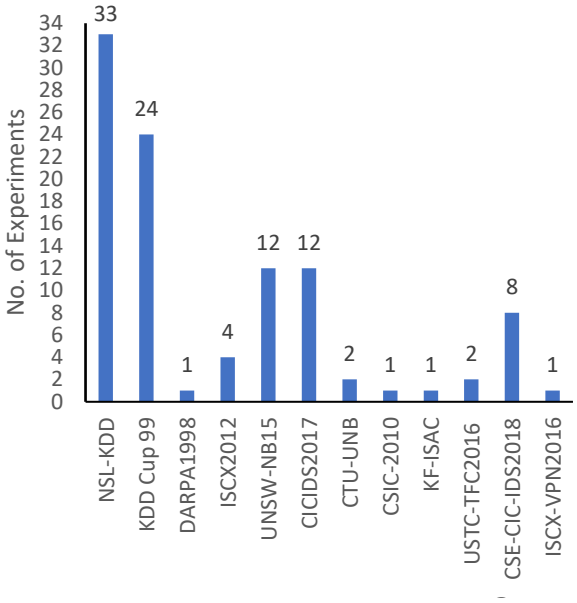

Figure 3 Utilized datasets

Some articles like P4, P17, P34, P40, P43, P44, P52, P80, P81 have used more than one dataset to test their algorithm. Therefore, the total number is 101 which is more than the number of articles. The most used dataset is NSL-KDD with 32.67% followed by KDD Cup 1999 with 23.76% of the total experiments. However, both are derived from DARPA, which represents 56.4% of the total experiments.

4.3. RQ3: What are the evaluation metrics that are used to validate the technique?

All the models must be validated using specific measurements, which demonstrates how well the model performed. Each of these measurements requires these values: true negative (TN), true positive (TP), false negative (FN), false positive (FP). We found a total of 21 metrics which are: Accuracy (Acc), True Positive Rate (TPR), Precision, F-measure (FM), False Positive Rate (FPR), Efficiency (EF), Error Rate (ER), ROC curve (ROC) which represents accuracy against FPR, Area under ROC curve (AUC), Effectiveness Measure (EM), precision-TPR curve, mean average precision (mAP), Confusion Matrix (CM), False Negative Rate (FNR), True Negative Rate (TNR), support, Specificity, loss value, Matthews Correlation Coefficient (MCC), Kappa, and CAP metric [98].

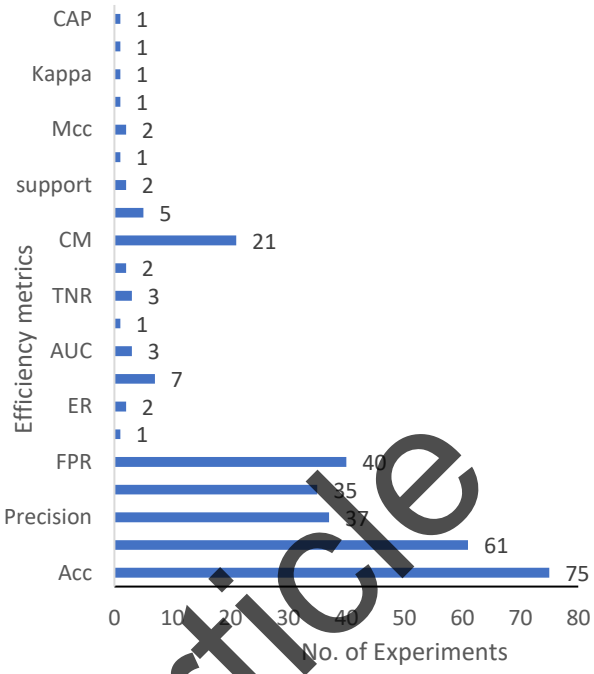

Figure 4 Evaluation metrics

Fig. 4, Shows the frequency of the metrics among the articles. Since most of the articles used more than one metric, the total is 302. The most used metric is accuracy which was utilized in 92.59% of the articles. Followed by TPR and FPR with 75.3% and 49.38% respectively.

5. CONCLUSIONS AND RECOMMENDATIONS

We performed this SLR to explore the NIDS using CNN specifically, whether alone or combined with another technique. We manually examined the initial 474 articles, choosing only 81 relevant articles after applying our selection criteria. This work provides a closer look at employing CNN for NIDS, which helps and aids the researchers towards utilizing CNN to obtain better results. The conclusion could be summarized as follows:

RQ1: We found 28 different hybrid approaches that were combined with CNN. Among them, the most used hybrid model was CNN-LSTM in 11 articles out of 41. The second most used hybrid model is split equally into 4 models that are CNN-RNN, CNN-GRU, CNN-GA, and CNN-SMOTE where each of them is used in 3 articles.

RQ2: We spotted 12 datasets that were used for validating the models. The DARPA dataset represented 56.4% of experiments as the total number of experiments was 101 in all the articles.

RQ3: There were 21 different evaluation metrics used in all the articles. The most used metrics were accuracy, TPR, and FPR that were used in 75, 61, and 40 articles respectively.

Based on this SLR results, considering that almost half of the selected articles relied only on CNN. We recommend using more hybrid models for NIDS which will open the opportunities to explore better outcomes not only in terms of detection efficiency but also in the model performance. The hybrid models have shown a remarkable boost in terms of model efficiency and performance. Furthermore, many articles used only one or two efficiency metrics which might not be enough to evaluate the model. Additionally, the most used dataset was NSL-KDD followed by KDD Cup 99 which is relatively old, it is recommended to use more up-to-date datasets that accommodate the real network traffic data. This will serve the model to produce better results when it's applied in a real-world network.

Regarding future work, it would benefit the researchers more to add the attack types that each mode can detect as well as the data pre-preprocessing technique that was used in each article. Besides that, we might also consider adding models that used CNN for IDS in other applications such as industrial control systems, surveillance systems, and database IDS. Nonetheless, these applications most likely will be using different types of datasets, pre-processing techniques, and evaluation metrics.

REFERENCES

[1] F. Salo, M. Injadat, A. B. Nassif, and A. Essex, "Data Mining with Big Data in Intrusion Detection Systems: A Systematic Literature Review," in *International Symposium on Big Data Management and Analytics 2019, BIDMA 2019,* 2020.

[2] S. Venticinque and A. Amato, "Smart Sensor and Big Data Security and Resilience," in *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*, Elsevier, 2018, pp. 123–141.

[3] A. Drewek-Ossowicka, M. Pietrołaj, and J. Rumiński, "A survey of neural networks usage for intrusion detection systems," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 1, pp. 497–514, 2020, doi: 10.1007/s12652-020-02014-x.

[4] K. Kim and M. E. Aminanto, "Deep learning in intrusion detection perspective: Overview and further challenges," in *Proceedings - WBIS 2017: 2017 International Workshop on Big Data and Information Security*, 2017, pp. 5–10, doi: 10.1109/IWBIS.2017.8275095.

[5] H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems : A Survey," *Appl. Sci.*, vol. 9, pp. 1–28, 2019, doi: 10.3390/app9204396.

[6] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, "CNN-based network intrusion detection against denial-of-service attacks," *Electron.*, vol. 9, no. 6, pp. 1–21, 2020, doi: 10.3390/electronics9060916.

[7] R. Upadhyay and D. V. Pantiukhin, "Application of Convolutional neural networks to intrusion type recognition," 2017.

[8] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, p. 102419, 2020, doi: 10.1016/j.jisa.2019.102419.

[9] S. Gamage and J. Samarabandu, "Deep learning methods in network intrusion detection: A survey and an objective comparison," *J. Netw. Comput. Appl.*, vol. 169, no. July, p. 102767, 2020, doi: 10.1016/j.jnca.2020.102767.

[10] Y. Wu, D. Wei, and J. Feng, "Network attacks detection methods based on deep learning techniques: A survey," *Secur. Commun. Networks*, 2020, doi: 10.1155/2020/8872923.

[11] A. A. A. Lateef, S. T. F. Al-Janabi, and B. Al-Khateeb, "Survey on intrusion detection systems based on deep learning," *Period. Eng. Nat. Sci.*, vol. 7, no. 3, pp. 1074–1095, 2019, doi: 10.21533/pen.v7i3.635.

[12] F. Salo, M. Injadat, A. B. Nassif, A. Shami, and A. Essex, "Data mining techniques in intrusion detection systems: A systematic literature review," *IEEE Access*, vol. 6, pp. 56046–56058, 2018, doi: 10.1109/ACCESS.2018.2872784.

[13] G. Kocher and G. Kumar, "Machine learning and deep learning methods for intrusion detection systems: recent developments and challenges," *Soft Comput.*, vol. 25, no. 15, pp. 9731–9763, 2021, doi: 10.1007/s00500-021-05893-0.

[14] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 1, pp. 1–29, 2020, doi: 10.1002/ett.4150.

[15] Barbara Kitchenham and S. Charters, "Guidelines for performing Systematic Literature Reviews in Software Engineering," 2007, doi: 10.1145/1134285.1134500.

[16] R. Vinayakumar, K. P. Soman, and P. Poornachandrany, "Applying convolutional neural network for network intrusion detection," in *2017 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2017*, 2017, vol. 2017-Janua, pp. 1222–1228, doi: 10.1109/ICACCI.2017.8126009.

[17] Y. Liu, S. Liu, and X. Zhao, "Intrusion Detection Algorithm Based on Convolutional Neural Network," in *4th International Conference on Engineering Technology and Application (ICETA 2017)*, 2017, vol.

37, no. 12, pp. 1271–1275, doi: 10.15918/j.tbit1001-0645.2017.12.011.

[18] W. Wang *et al.*, "HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection," *IEEE Access*, vol. 6, pp. 1792–1806, 2017, doi: 10.1109/ACCESS.2017.2780250.

[19] L. Mohammadpour, T. C. Ling, C. S. Liew, and C. Y. Chong, "A Convolutional Neural Network for Network Intrusion Detection System," in *Proceedings of the Asia-Pacific Advanced Network*, 2018, vol. 46, no. 0, pp. 50–55.

[20] W.-H. Lin, H.-C. Lin, P. Wang, B.-H. Wu, and J.-Y. Tsai, "Using convolutional neural networks to network intrusion detection for cyber threats," in *Proceedings of 4th IEEE International Conference on Applied System Innovation 2018, ICASI 2018*, 2018, pp. 1107–1110, doi: 10.1109/ICASI.2018.8394474.

[21] S. Naseer and Y. Saleem, "Enhanced network intrusion detection using deep convolutional neural networks," *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 10, pp. 5159–5178, 2018, doi: 10.3837/tiis.2018.10.028.

[22] Y. Ding and Y. Zhai, "Intrusion detection system for NSL-KDD dataset using convolutional neural networks," in *ACM International Conference Proceeding Series*, 2018, pp. 81–85, doi: 10.1145/3297156.3297230.

[23] K. Wu, Z. Chen, and W. Li, "A Novel Intrusion Detection Model for a Massive Network Using Convolutional Neural Networks," *IEEE Access*, vol. 6, pp. 50850–50859, 2018, doi: 10.1109/ACCESS.2018.2868993.

[24] S. Naseer *et al.*, "Enhanced network anomaly detection based on deep neural networks," *IEEE Access*, vol. 6, pp. 48231–48246, 2018, doi: 10.1109/ACCESS.2018.2863036.

[25] S. Behera, A. Pradhan, and R. Dash, "Deep Neural Network Architecture for Anomaly Based Intrusion Detection System," in *2018 5th International Conference on Signal Processing and Integrated Networks, SPIN 2018*, 2018, pp. 270–274, doi: 10.1109/SPIN.2018.8474162.

[26] M. M. U. Chowdhury, F. Hammond, G. Konowicz, C. Xin, H. Wu, and J. Li, "A few-shot deep learning approach for improved intrusion detection," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2017*, 2018, vol. 2018-Janua, pp. 1–7, doi: 10.1109/UEMCON.2017.8249084.

[27] R. Blanco, J. J. Cilla, P. Malagón, I. Penas, and J. M. Moya, "Tuning CNN input layout for IDS with genetic algorithms," *Springer Int. Publ. AG, part Springer Nat. 2018*, vol. 10870 LNAI, pp. 197–209, 2018, doi: 10.1007/978-3-319-92639-1_17.

[28] S.-N. Nguyen, V.-Q. Nguyen, J. Choi, and K. Kim, "Design and implementation of intrusion detection system using convolutional neural network for DoS detection," in *International Conference on Advanced Machine Learning and Soft Computing (ICMLSC)*, 2018, pp. 34–38, doi: 10.1145/3184066.3184089.

[29] A. K. Verma, P. Kaushik, and G. Shrivastava, "A Network Intrusion Detection Approach Using Variant of Convolution Neural Network," in *Proceedings of the 4th International Conference on Communication and Electronics Systems, ICCES 2019*, 2019, pp. 409–416, doi: 10.1109/ICCES45898.2019.9002221.

[30] R. U. Khan, X. Zhang, M. Alazab, and R. Kumar, "An improved convolutional neural network model for intrusion detection in networks," in *Proceedings - 2019 Cybersecurity and Cyberforensics Conference, CCC 2019*, 2019, no. Ccc, pp. 74–77, doi: 10.1109/CCC.2019.000-6.

[31] P. Wu and H. Guo, "LuNet: A Deep Neural Network for Network Intrusion Detection," in *2019 IEEE Symposium Series on Computational Intelligence, SSCI 2019*, 2019, pp. 617–624, doi: 10.1109/SSCI44817.2019.9003126.

[32] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, "An Intrusion Detection Model Based on Feature Reduction and Convolutional Neural Networks," *IEEE Access*, vol. 7, pp. 42210–42219, 2019, doi: 10.1109/ACCESS.2019.2904620.

[33] Y. Li and B. Zhang, "An intrusion detection model based on multi-scale CNN," in *Proceedings of 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference, ITNEC 2019*, 2019, pp. 214–218, doi: 10.1109/ITNEC.2019.8729261.

[34] X. Zhang, J. Ran, and J. Mi, "An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic," in *Proceedings of IEEE 7th International Conference on Computer Science and Network Technology, ICCSNT 2019*, 2019, pp. 456–460, doi: 10.1109/ICCSNT47585.2019.8962490.

[35] N. Chouhan, A. Khan, and H.-U.-R. Khan, "Network anomaly detection using channel boosted and residual learning based deep convolutional neural network," *Appl. Soft Comput. J.*, vol. 83, 2019, doi: 10.1016/j.asoc.2019.105612.

[36] X. Zhang, J. Chen, Y. Zhou, L. Han, and J. Lin, "A Multiple-Layer Representation Learning Model for Network-Based Attack Detection," *IEEE Access*, vol. 7, pp. 91992–92008, 2019, doi: 10.1109/ACCESS.2019.2927465.

[37] C.-M. Hsu, H.-Y. Hsieh, S. W. Prakosa, M. Z. Azhari, and J.-S. Leu, "Using long-short-term memory based convolutional neural networks for network intrusion detection," in *11th EAI International Wireless Internet*

Conference, 2019, vol. 264, pp. 86–94, doi: 10.1007/978-3-030-06158-6_9.

[38] L. Zhang, M. Li, X. Wang, and Y. Huang, "An Improved Network Intrusion Detection Based on Deep Neural Network," in *IOP Conference Series: Materials Science and Engineering*, 2019, vol. 563, no. 5, doi: 10.1088/1757-899X/563/5/052019.

[39] P. Liu, "An intrusion detection system based on convolutional neural network," in *11th International Conference on Computer and Automation Engineering (ICCAE)*, 2019, pp. 62–67, doi: 10.1145/3313991.3314009.

[40] X. Xie, X. Jiang, W. Wang, B. Wang, T. Wan, and H. Yang, "An intrusion detection method based on hierarchical feature learning and its application," in *11th International Symposium on Cyberspace Safety and Security (CSS)*, 2019, vol. 11982 LNCS, pp. 13–20, doi: 10.1007/978-3-030-37337-5_2.

[41] B. Alsughayyir and A. M. Qamar, "Deep learning-based network attack detection using convolutional and recurrent neural networks," *Int. J. Eng. Res. Technol.*, vol. 12, no. 12, pp. 3027–3303, 2019.

[42] J. Zhang, Y. Ling, X. Fu, X. Yang, G. Xiong, and R. Zhang, "Model of the intrusion detection system based on the integration of spatial-temporal features," *Comput. Secur.*, vol. 89, 2019, doi: 10.1016/j.cose.2019.101681.

[43] L. Heng and T. Weise, "Intrusion Detection System Using Convolutional Neuronal Networks: A Cognitive Computing Approach for Anomaly Detection based on Deep Learning," in *Proceedings of 2019 IEEE 18th International Conference on Cognitive Informatics and Cognitive Computing, ICCI*CC 2019*, 2019, pp. 34–40, doi: 10.1109/ICCICC46617.2019.9146088.

[44] H. Yang and F. Wang, "Wireless network intrusion detection based on improved convolutional neural network," *IEEE Access*, vol. 7, pp. 64366–64374, 2019, doi: 10.1109/ACCESS.2019.2917299.

[45] X. Wang, S. Yin, H. Li, J. Wang, and L. Teng, "A Network Intrusion Detection Method Based on Deep Multi-scale Convolutional Neural Network," *Int. J. Wirel. Inf. Networks*, vol. 27, no. 4, pp. 503–517, 2020, doi: 10.1007/s10776-020-00495-3.

[46] S. Al-Emadi, A. Al-Mohannadi, and F. Al-Senaid, "Using Deep Learning Techniques for Network Intrusion Detection," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020*, 2020, pp. 171–176, doi: 10.1109/ICIoT48696.2020.9089524.

[47] L. Mohammadpour, T. C. Ling, C. S. Liew, and A. Aryanfar, "A Mean Convolutional Layer for Intrusion Detection System," *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8891185.

[48] A. Kim, M. Park, and D. H. Lee, "AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection," *IEEE Access*, vol. 8, pp. 70245–70261, 2020, doi: 10.1109/ACCESS.2020.2986882.

[49] G. Liu and J. Zhang, "CNID: Research of Network Intrusion Detection Based on Convolutional Neural Network," *Discret. Dyn. Nat. Soc.*, vol. 2020, 2020, doi: 10.1155/2020/4705982.

[50] P. Sun *et al.*, "DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system," *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8890306.

[51] H. Wang, Z. Cao, and B. Hong, "A network intrusion detection system based on convolutional neural network," *J. Intell. Fuzzy Syst.*, vol. 38, no. 6, pp. 7623–7637, 2020, doi: 10.3233/JIFS-179833.

[52] M. T. Nguyen and K. Kim, "Genetic convolutional neural network for intrusion detection systems," *Futur. Gener. Comput. Syst.*, vol. 113, pp. 418–427, 2020, doi: 10.1016/j.future.2020.07.042.

[53] W.-F. Zheng, "Intrusion Detection Based on Convolutional Neural Network," in *2020 International Conference on Computer Engineering and Application (ICCEA)*, 2020, pp. 273–277, doi: 10.1109/ICCEA50009.2020.00066.

[54] K. Jiang, W. Wang, A. Wang, and H. Wu, "Network Intrusion Detection Combined Hybrid Sampling with Deep Hierarchical Network," *IEEE Access*, vol. 8, pp. 32464–32476, 2020, doi: 10.1109/ACCESS.2020.2973730.

[55] C.-M. Hsu, M. Z. Azhari, H.-Y. Hsieh, S. W. Prakosa, and J.-S. Leu, "Robust Network Intrusion Detection Scheme Using Long-Short Term Memory Based Convolutional Neural Networks," *Mob. Networks Appl.*, 2020, doi: 10.1007/s11036-020-01623-2.

[56] V. Kumar, K. Rana, J. Malik, and A. Tomar, "Evaluating hybrid cnn-mlp architecture for analyzing novel network traffic attacks," *Int. J. Sci. Technol. Res.*, vol. 9, no. 3, pp. 4889–4896, 2020.

[57] H. Zhang, L. Huang, C. Q. Wu, and Z. Li, "An effective convolutional neural network based on SMOTE and Gaussian mixture model for intrusion detection in imbalanced dataset," *Comput. Networks*, vol. 177, 2020, doi: 10.1016/j.comnet.2020.107315.

[58] B. Wang, Y. Su, M. Zhang, and J. Nie, "A deep hierarchical network for packet-level malicious traffic detection," *IEEE Access*, vol. 8, pp. 201728–201740, 2020, doi: 10.1109/ACCESS.2020.3035967.

[59] P. Kumar, A. A. Kumar, C. Sahayakingsly, and A. Udayakumar, "Analysis of intrusion detection in cyber attacks using DEEP learning neural networks," *Peer-to-Peer Netw. Appl.*, 2020, doi: 10.1007/s12083-020-00999-y.

[60] V. Maheshwar Reddy, I. Ravi Prakash Reddy, and K. Adi Narayana Reddy, "An efficient intrusion detection system with convolutional neural network," *Adv. Comput. Intell. Informatics, Lect. Notes Networks Syst.*, vol. 119, pp. 177–185, 2020, doi: 10.1007/978-981-15-3338-9_22.

[61] W. Tao, W. Zhang, C. Hu, and C. Hu, "A Network Intrusion Detection Model Based on Convolutional Neural Network," *Adv. Intell. Syst. Comput.*, vol. 895, pp. 771–783, 2020, doi: 10.1007/978-3-030-16946-6_63.

[62] S. Mishra, R. Dwivedula, V. Kshirsagar, and C. Hota, "Robust Detection of Network Intrusion using Tree-based Convolutional Neural Networks," in *ACM International Conference Proceeding Series*, 2020, pp. 233–237, doi: 10.1145/3430984.3431036.

[63] D. Niu, J. Zhang, L. Wang, K. Yan, T. Fu, and X. Chen, "A Network Traffic anomaly Detection method based on CNN and XGBoost," in *Proceedings - 2020 Chinese Automation Congress, CAC 2020*, 2020, pp. 5453–5457, doi: 10.1109/CAC51589.2020.9327030.

[64] X. Xie *et al.*, "Research and application of intrusion detection method based on hierarchical features," *Concurr. Comput. Pract. Exp.*, 2020, doi: 10.1002/cpe.5799.

[65] M. Ahsan and K. E. Nygard, "Convolutional neural networks with LSTM for intrusion detection," *Epic Ser. Comput.*, vol. 69, pp. 69–79, 2020, doi: 10.29007/j35r.

[66] V. Pham, E. Seo, and T.-M. Chung, "Lightweight convolutional neural network based intrusion detection system," *J. Commun.*, vol. 15, no. 11, pp. 808–817, 2020, doi: 10.12720/jcm.15.11.808-817.

[67] S. Sriram, A. Shashank, R. Vinayakumar, and K. P. Soman, "DCNN-IDS: Deep Convolutional Neural Network Based Intrusion Detection System," *Commun. Comput. Inf. Sci.*, vol. 1213, pp. 85–92, 2020, doi: 10.1007/978-981-15-9700-8_7.

[68] J. Zhang, F. Li, and F. Ye, "An Ensemble-based Network Intrusion Detection Scheme with Bayesian Deep Learning," in *IEEE International Conference on Communications*, 2020, vol. 2020-June, doi: 10.1109/ICC40277.2020.9149402.

[69] M. Azizjon, A. Jumabek, and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," in *2020 International Conference on Artificial Intelligence in Information and Communication, ICAIIC 2020*, 2020, pp. 218–224, doi: 10.1109/ICAIIC48513.2020.9064976.

[70] S. Li, "Network Intrusion Detection Model Based on Improved Convolutional Neural Network," *Adv. Intell. Syst. Comput.*, vol. 1146 AISC, pp. 18–24, 2020, doi: 10.1007/978-3-030-43306-2_3.

[71] Y. Li, "Research on Application of Convolutional Neural Network in Intrusion Detection," in *Proceedings - 2020 7th International Forum on Electrical Engineering and Automation, IFEEA 2020*, 2020, pp. 720–723, doi: 10.1109/IFEEA51475.2020.00153.

[72] X. Han *et al.*, "STIDM: A spatial and temporal aware intrusion detection model," in *Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020*, 2020, pp. 370–377, doi: 10.1109/TrustCom50675.2020.00058.

[73] L. Chen, X. Kuang, A. Xu, S. Suo, and Y. Yang, "A Novel Network Intrusion Detection System Based on CNN," in *Proceedings - 2020 8th International Conference on Advanced Cloud and Big Data, CBD 2020*, 2020, pp. 243–247, doi: 10.1109/CBD51900.2020.00051.

[74] A. Andalib and V. T. Vakili, "An autonomous intrusion detection system using an ensemble of advanced learners," 2020, doi: 10.1109/ICEE50131.2020.9260808.

[75] V. Manikandan, K. Gowsic, T. Prince, R. Umamaheswari, B. F. Ibrahim, and A. Sampathkumar, "DRCNN-IDS Approach for Intelligent Intrusion Detection System," 2020, doi: 10.1109/ICCIT-144147971.2020.9213779.

[76] Y. Zhou, X. Zhu, S. Hu, D. Lin, and Y. Gao, "Intrusion Detection Based on Convolutional Neural Network in Complex Network Environment," *Artif. Intell. China*, vol. 572 LNEE, pp. 229–238, 2020, doi: 10.1007/978-981-15-0187-6_26.

[77] M. Gamal, H. Abbas, and R. Sadek, "Hybrid Approach for Improving Intrusion Detection Based on Deep Learning and Machine Learning Techniques," in *Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2020)*, 2020, vol. 1153 AISC, pp. 225–236, doi: 10.1007/978-3-030-44289-7_22.

[78] Z. Hu, L. Wang, L. Qi, Y. Li, and W. Yang, "A novel wireless network intrusion detection method based on adaptive synthetic sampling and an improved convolutional neural network," *IEEE Access*, vol. 8, pp. 195741–195751, 2020, doi: 10.1109/ACCESS.2020.3034015.

[79] Y. Chen, S. Chen, M. Xuan, Q. Lin, and W. Wei, "Evolutionary Convolutional Neural Network: An Application to Intrusion Detection," in *2021 13th International Conference on Advanced Computational Intelligence, ICACI 2021*, 2021, pp. 245–252, doi: 10.1109/ICACI52617.2021.9435859.

[80] R. V. Mendonca *et al.*, "Intrusion Detection System Based on Fast Hierarchical Deep Convolutional Neural Network," *IEEE Access*, vol. 9, pp. 61024–61034,

2021, doi: 10.1109/ACCESS.2021.3074664.

[81] L. Tian and Y. Lu, "An intrusion detection model based on SMOTE and convolutional neural network ensemble," in *Journal of Physics: Conference Series*, 2021, vol. 1828, no. 1, doi: 10.1088/1742-6596/1828/1/012024.

[82] Q. Zhou, M. Tan, and H. Xi, "ACGANs-CNN: A Novel Intrusion Detection Method," in *Journal of Physics: Conference Series*, 2021, vol. 1757, no. 1, doi: 10.1088/1742-6596/1757/1/012012.

[83] W. Yue, J. Yiming, and L. Julong, "A Fast Deep Learning Method for Network Intrusion Detection without Manual Feature Extraction," in *Journal of Physics: Conference Series*, 2021, vol. 1738, no. 1, doi: 10.1088/1742-6596/1738/1/012127.

[84] S. Kabir, S. Sakib, M. A. Hossain, S. Islam, and M. I. Hossain, "A Convolutional Neural Network based Model with Improved Activation Function and Optimizer for Effective Intrusion Detection and Classification," in *2021 International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2021*, 2021, pp. 373–378, doi: 10.1109/ICACITE51222.2021.9404584.

[85] J. Man and G. Sun, "A Residual Learning-Based Network Intrusion Detection System," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/5593435.

[86] Y. Wang, Y. Jiang, and J. Lan, "FCNN: An Efficient Intrusion Detection Method Based on Raw Network Traffic," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/5533269.

[87] I. Al-Turaiki and N. Altwaijry, "A Convolutional Neural Network for Improved Anomaly-Based Network Intrusion Detection," *Big Data*, vol. 9, no. 3, pp. 233–252, 2021, doi: 10.1089/big.2020.0263.

[88] M. A. Khan, "HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system," *Processes*, vol. 9, no. 5, 2021, doi: 10.3390/pr9050834.

[89] K. He, "Study on Intrusion detection model based on improved convolutional neural network," in *2021 International Conference on Advances in Optics and Computational Sciences*, 2021, vol. 1865, no. 4, doi: 10.1088/1742-6596/1865/4/042097.

[90] H. Altunay and Z. Albayrak, "Network Intrusion Detection Approach Based on Convolutional Neural Network," *Eur. J. Sci. Technol.*, vol. 26, no. July, pp. 22–29, 2021, doi: 10.31590/ejosat.954966.

[91] Y. Liu, J. Kang, Y. Li, and B. Ji, "A Network Intrusion Detection Method Based on CNN and CBAM," 2021.

[92] S. Ho, S. Al Jufout, K. Dajani, and M. Mozumdar, "A Novel Intrusion Detection Model for Detecting Known and Innovative Cyberattacks Using Convolutional Neural Network," *IEEE Open J. Comput. Soc.*, vol. 2, no. October 2020, pp. 14–25, 2021, doi: 10.1109/ojcs.2021.3050917.

[93] A. Krishnan and S. T. Mithra, "A Modified 1D-CNN Based Network Intrusion Detection System," *Int. J. Res. Eng. Sci. Manag.*, vol. 4, no. 6, pp. 291–294, 2021.

[94] L. Yu *et al.*, "PBCNN: Packet Bytes-based Convolutional Neural Network for Network Intrusion Detection," *Comput. Networks*, vol. 194, no. March, p. 108117, 2021, doi: 10.1016/j.comnet.2021.108117.

[95] P. Rajesh Kanna and P. Santhi, "Unified Deep Learning approach for Efficient Intrusion Detection System using Integrated Spatial–Temporal Features[Formula presented]," *Knowledge-Based Syst.*, vol. 226, p. 107132, 2021, doi: 10.1016/j.knosys.2021.107132.

[96] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, "A survey of network-based intrusion detection data sets," *Comput. Secur.*, vol. 86, pp. 147–167, 2019, doi: https://doi.org/10.1016/j.cose.2019.06.005.

[97] S. T. Brugger and J. Chow, "An Assessment of the DARPA IDS Evaluation Dataset Using Snort," *Dept. Comput. Sci., UCDAVIS, Tech. Rep.*, vol. 1, pp. 1–19, 2005.

[98] G. Gu, P. Fogla, D. Dagon, W. Lee, and B. Skorić, "Measuring Intrusion Detection Capability: An Information-Theoretic Approach," in *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, 2006, pp. 90–101, doi: 10.1145/1128817.1128834.