Deep Learning Techniques to Detect DoS Attacks on Industrial Control Systems: a Systematic Literature Review

Abdalkarim R. Seyam, Ali Bou Nassif, Qassim Nasir,
Bushra Al Blooshi and Manar Abu Talib

August 5, 2021

Deep Learning Techniques to Detect DoS Attacks on Industrial Control Systems: A Systematic Literature Review

Abdalkarim RM Seyam

University of Sharjah, U17105813@sharjah.ac.ae

Ali Bou Nassif

University of Sharjah, anassif@sharjah.ac.ae

Qassim Nasir

University of Sharjah, nasir@sharjah.ac.ae

Bushra Al Blooshi

Dubai Electronic Security Center, bushra.alblooshi@desc.gov.ae

Manar Abu Talib

University of Sharjah, mtalib@sharjah.ac.ae

Cyber Physical Systems (CPS) security is crucial demand within industrial fields. The deployment of these systems within critical infrastructure is increasing day by day. CPS applications include smart grid, Industrial Control Systems (ICS), Aerial Systems and Intelligent Transportation Systems (ITS). The complexity, heterogeneity, and diversity evolved with these CPS systems. In addition, the inter-connectivity of these systems over cyberspace has increased their attack surface. This research paper provides a survey on deep learning detection techniques for the Denial of Service (DoS) attack, which is considered the most critical and major attack on CPS. Moreover, the survey study demonstrates the most used deep learning techniques in the research articles of traditional IT networks and ICS networks. It also explains their used datasets as training sources and their most common evaluation matrix that is used to benchmark their performance against each other. In addition, the research gaps that are related to classifier efficiency are identified, while considering modern datasets related to ICS protocols. Moreover, consider the actual cyberspace attack traffic collected from passive monitoring sensors. This would resolve the need for using less features provided over outdated and publicly available dataset.

Keywords: Deep Learning, DoS, ICS, Passive Monitoring.

ACM Reference Format:

Abdalkarim RM Seyam, Ali Bou Nassif, Qassim Nasir, Bushra Al Blooshi, Manar Abu Talib. 2021. Deep Learning Techniques to Detect DoS Attacks on Industrial Control.

1 INTRODUCTION

Industrial Control Systems (ICS) are the fundamental base of industrial critical infrastructure and have been utilized for a long time to oversee industrial machines [1]. Supervisory Control and Data Acquisition (SCADA) frameworks regularly include the ICSs systems and are considered as the biggest subset of these frameworks [2]. Fundamental parts of these frameworks are to perform real-time checking, manage interactively these ICS, analyze their information, and record their alerts, and incidents within the framework. Initially, ICS was running their own restrictive protocols, therefore, ICS was less exposed to cyberattacks. Recently, ICS network is integrated in various industrial fields to supply fundamental needs. This has generated a new type of traffic generated from heterogeneous critical infrastructure. As a result, this has increased the attack surface [3].

These networks are having rapid expansion of traffic that is generated from several developed technologies. Existing network filtration mechanism is not able to cope with security demands to protect these networks. Traditional ways of detecting threats and attacks, using signature are not sufficient with evolving attack techniques [4]. Hence, a need for more efficient way to detect the behavioral of these attacks based on a good source of cyberspace intelligence attack [5], [6]. Many literature surveys consider the deep learning implementation for intrusion detection. Our research review is different from other survey studies in different perspectives: (i) focusing on deep learning techniques that are used for detecting DoS/DDoS attacks in industrial control systems. (ii) considering articles for dataset that are related to industrial control system networks. (iii) considering datasets with feature selection that are related to DoS/DDoS attack.

The remaining of research paper is divided in different sections as follow: Section 2 provides literature review on related work. Section 3 describes the adopted methodology in this research study. Section 4 tabulates the results and discusses the answers to the research questions. We conclude and introduce the research gabs and opportunities as future work in Section 5.

2 LETRATURE REVIEW:

Although researchers published several studies on deep learning for network Denial of Service (DoS) detection, we observed that only few papers discuss about deep learning detection in the context of ICS. DoS is the highest ranked ICS vulnerabilities reported in 2016 [7], and it is considered the highest ranked attack strategy due to the accessibility of unsupervised numerous Internet of Things (IoT) devices as seen within the Mirai Botnet [8]. Some research papers discussed the deep discriminative models, which are more suitable to learn boundaries that separate data into different classes. Some research papers used Convolutional Neural Network (CNN) ([9], [10], [11], [12,][13], [14], [15], [16]), since it gives better accuracy, but takes more computational time. While other research papers discuss Deep Neural Networks (DNN) ([17], [18], [19], [20]) as DNN is considered scalable with capability to learn more features, but it is considered weak in learning time series dependencies to detect DoS attack. Other research papers discussed generative/ unsupervised models. They are more suitable to model the distribution of individual classes and also can find the hidden parameters of that distribution, such as Recurrent Neural Network (RNN) ([21], [22]). It is suitable for temporal data learning or sequential data, but it has a problem of disappearing gradient, which mean it has difficulty to keep long term dependencies. Long Short-Term Memory (LSTM) in ([1], [23], [24], [2]) has solved the problem of disappearing gradient in RNN, which makes it a good candidate to predict time series of data with better accuracy. Other techniques used such as Restricted Boltzmann Machine (RBM) ([3], [10], [27]), was used less frequent than others. Deep Belief Network (DBN) ([28], [32]), used in multi-classifier model. Some research papers are using binary classifier for either normal or attack traffic ([25], [3], [8]) and others using multi-classifier for different types of attacks ([4], [26], [27]). Some research papers didn't use the testing time as metric for performance evaluation ([27], [28], [16]). Testing time is important and critical for DoS fast detection. Most of the research papers within IT networks used NSL-KDD dataset, where it has limited feature compared with modern attacks. Moreover, there are research papers in ICS domain, which are using Modbus TCP ([26], [29], [30]) for the commonly used protocol in ICS dataset. On the other hand, there are other papers, which use their own testbed for data acquisition ([4], [31]) for lack of much more comprehensive ICS dataset. Well known dataset for DoS attack such as CICIDS2017 is used in several research studies ([32], [33], [34]) while, UNSW-NB15 is used in some other research papers ([35], [36]).

3 METHODOLOGY

Our Systematic Literature Review (SLR) methodology is based on proposed guidelines for Kitchenham and Charters [37]. Planning process has an important role to identify our needs for this review to have a better detection mechanism for ICT attacks, using deep learning approach. Planning process also considers the objective of this review to gather information in this domain and to create a review protocol. The following sections provide details of the review protocol that is used in this literature review.

3.1 RESEARCH QUESTIONS (RQs)

We tackle research questions about analyzing deep learning techniques and their implementation to detect and classifying the ICS network attacks from 2014 till 2021 inclusive. As a result, the following questions are developed for this objective:
RQ1- What are the used deep learning techniques for attack detection on ICT environment?
RQ2- Which datasets are used for DoS detection in the literature?
RQ3- What are the common evaluation metrics used in research papers?
RQ4- What are the strengths are weaknesses of the implemented techniques?

3.2 SEARCH STRATEGY

The search terms are deduced from the research questions, for example, “deep learning”, “Denial of Service (DoS)”, “attack detection”, “Industrial Control System” domain. Moreover, we considered similar attack detection in IT domain for common DoS attack behavior on both IT and ICT domain. In addition to other search terms created for spelling variants, or similar keywords used, and boolean logic added like (OR, AND, etc.) to make result more relevant.

3.3 QUALITY ASSESSMENT (QA)

Overall score varies from 0 to 5 to indicate each paper quality. If the score equal or more than 3, the paper is considered in our research study. Quality assessment indicator considers whether we have the objectives of the article demonstrated with acceptable details. Do the paper experiments relate to our scope of this literature review? Did the authors explain the used deep learning approach clearly? Have the research results been obtained by deep learning technique for detection mechanism and been measured properly? Is the dataset or data source suitable for the objective outlined for ICT attack detection? Did the authors report the results and findings clearly?

4 RESULTS AND DISCUSSION

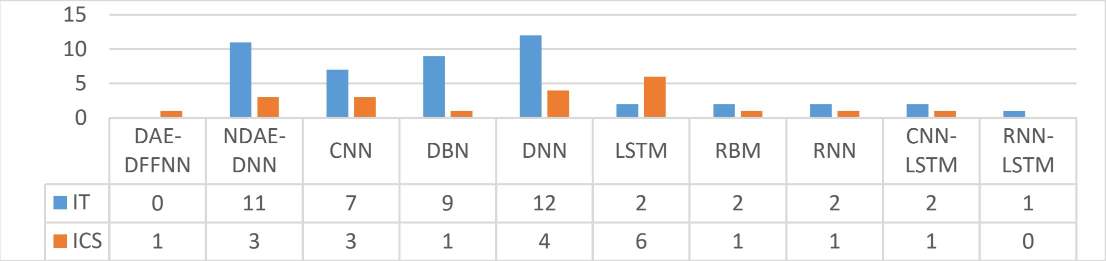
We have addressed four critical research questions and discussed and analyzed them on 50 research papers from 2014 to 2021. Our selected 50 research papers belong to conferences and journals. The most relevant paper to our search terms, was identified starting from 2014 and filtered upon quality assessment indicator.

Table 1: Summary of Results and Findings

Year	Type	Environment	Attack Types	Deep Learning	Dataset
[10], 2020	Journal	Network Security	Probe,DOS	CNN, DBN, DNN, RBM	CSE-CIC-IDS2018
[11], 2020	Journal	Network Security	Probe,DOS, U2R,R2L	CNN, RNN	CSE-CIC-IDS2018
[19], 2020	Journal	Network Security	Probe,DOS	NDAE+DNN, DNN	UNSW-NB15
[33], 2020	Journal	Network Security	Probe,DOS	NDAE+DNN	UNSW-NB15, CICIDS2017, KDD
[14], 2020	Journal	Network Security	Probe,DOS	CNN, LSTM	NSL-KDD
[15], 2020	Journal	Network Security	Probe,DOS	CNN, DNN	UNSW-NB15, KDD
[2], 2020	Journal	Industrial OT	Probe,DOS	LSTM	Testbed
[21], 2020	Journal	Smart Grid	Probe,DOS	RNN	CICIDS2017
[9] ,2019	Journal	Network Security	Probe,DOS,	CNN, LSTM, CNN+LSTM	CTU, CICIDS2017
[3], 2019	Journal	Sensors Network	Probe,DOS, U2R,R2L	RBM	KDD
[27], 2019	Journal	IoT Based	Probe,DOS, U2R,R2L	DBN, RBM	NSL-KDD
[8], 2019	Journal	Network Security	normal/attack	CNN+LSTM	ISCX2012, UST-2016
[17], 2019	Journal	Network Security	Probe,DOS	DNN	Kyoto 2006, NSL-KDD
[18], 2019	Journal	Network Security	Probe,DOS	DNN	UNSW-NB15, CICIDS2017
[35], 2019	Journal	Network Security	Probe,DOS	NDAE+DNN	UNSW-NB15, KDD
[34], 2019	Journal	Network Security	Probe,DOS	NDAE+DNN	Kyoto 2006+
[28], 2019	Journal	Network Security	Probe,DOS, U2R,R2L	DBN	NSL-KDD
[12], 2019	Journal	Network Security	Probe,DOS, U2R,R2L	NDAE+DNN, CNN	KDD
[13], 2019	Journal	Network Security	Probe,DOS	CNN	UNSW-NB15, CICIDS2017
[16], 2019	Journal	Industrial OT	Probe,DOS	NDAE+DNN, CNN	BATADAL, SWaT
[20], 2019	Journal	Industrial OT	Probe,DOS	DNN	Testbed
[24], 2019	online	Industrial OT	Probe,DOS	LSTM	SWaT
[4], 2018	Conference	Smart Grid	Probe,DOS, U2R,R2L	DNN	Data Acquisition
[36], 2018	Journal	Industrial IoT	Probe,DOS	DAE-DFFNN	UNSW-NB15, KDD
[26], 2018	Journal	Network Security	Probe,DOS, U2R,R2L	DNN	KDD, NSL-KDD
[32], 2018	Journal	Network Security	Probe,DOS	DBN	UNSW-NB15
[30], 2018	Journal	Industrial OT	Probe,DOS	NDAE+DNN	SWaT
[23], 2018	Conference	Industrial OT	Probe,DOS	LSTM	Testbed
[29], 2018	Conference	Industrial OT	Probe,DOS	DNN	Modbus TCP
[22], 2017	Journal	Network Security	Probe,DOS, U2R,R2L	RNN	NSL-KDD
[1], 2017	Conference	Industrial OT	Probe,DOS	LSTM	Gas Pipeline
[25], 2016	Conference	SDN Networking	Probe,DOS, U2R,R2L	DNN	NSL-KDD
[31], 2016	Online	SDN Networking	Probe,DOS	NDAE+DNN	Data Acquisition

RQ1: What are the used deep learning techniques for attack detection on ICT environment?

The review resulted to identify different main deep learning techniques that are applied to detect DoS attacks. The research papers have considered the traditional IT networks ([3], [8], [9], [10], [11], [12], [13], [14], [15], [17], [18], [19], [25], and ICS networks domain ([1], [2], [4], [16], [20], [21], [23], [24], [27], [29], [30], [36]), where both are subject to similar DoS attack characteristic. The most used technique in ICS is LSTM, where in IT networks the DNN is mostly used.



	DAE-DFFNN	NDAE-DNN	CNN	DBN	DNN	LSTM	RBM	RNN	CNN-LSTM	RNN-LSTM
🟦 IT	0	11	7	9	12	2	2	2	2	1
🟧 ICS	1	3	3	1	4	6	1	1	1	0

DAE-DFFNN: Deep Autoencoder- Feed forward Neural Network, NDAE-DNN: Non-symmetric Deep Auto-encoder RBM: Restricted Boltzmann Machine.
Figure1: The frequencies of each DL techniques used in each research paper (IT and ICS). LSTM is the mostly used in ICS environment.

RQ2: Which datasets are used for DoS detection in the literature?

Deep learning techniques discussed in the research papers, have been implemented to detect different types of attacks in ICS. They fall into 3 main cyber threat categories. The highest category has considered the interruption attack using DoS techniques and targeting availability of ICS. Main datasets are NSL-KDD [38] with 23.73% , UNSW_NB15 [39] with 13.56%, and CICIDS 2018 [40] with 11.86%.

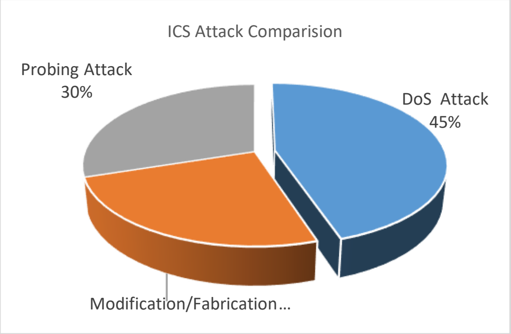


Figure 2: The percentage of DoS attacks in collected papers' dataset versus other type of attacks

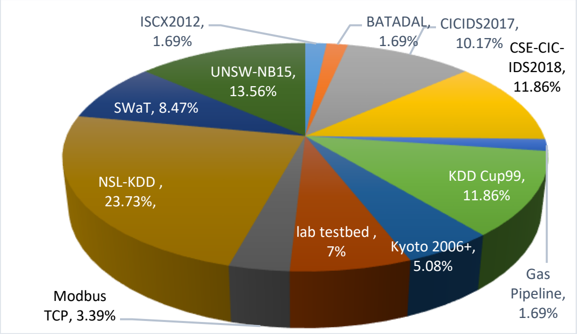
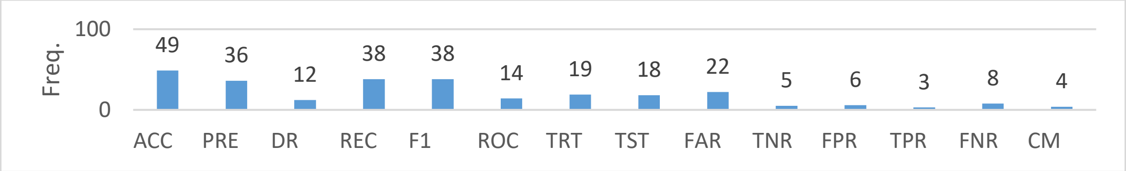


Figure 3: Dataset usage percentage in collected research papers

RQ3: What are the common evaluation metrics used in research papers?

Most used metric among research paper in this domain are the accuracy, recall and F1-score.



ACC: Accuracy, PRE: Precision, DR: Detection Rate, REC: Recall, F1: F1-score, TRT: Training Time, TST: Testing Time, FAR: False Alarm Rate, TNR: True Negative Rate, FPR: False Positive Rate, TPR: True Positive Rate, FNR: False Negative Rate, CM: Matthews Correlation Coefficient, ROC: receiver operating characteristic
Figure 4: Plot frequencies of used evaluation metrices

RQ4: What are the strengths and weaknesses of the implemented techniques?

Multiple research papers have used DNN ([19], [20]), which is considered scalable with capability to learn more features, but it is considered weak in learning time series dependencies. Other studies have used CNN, which is considered good in feature learning by multiple scalable stacked convolutional layers and pooling layers ([12], [13], [14]). However, the more features it needs to learn, the more hidden layers are required. As a result, it demands more CPU processing, in addition to its weakness to process temporal information for sequential data. NDAE technique demonstrates good accuracy, and reduction in training time compared with other DBN and RBM based techniques. On the other hand, it will not be able to detect zero-day attack such as DoS, due to its limited capability to learn sequential time series data. The RNN ([21], [22]) technique can use its internal memory to process input sequences of arbitrary time series of data. As a result, it is suitable for temporal data learning or sequential data, but it has a problem of disappearing gradient, which means it has difficulty to keep long term dependencies. The LSTM ([23], [24]) has solved the problem of disappearing gradient in RNN, which makes it a good candidate to predict time series of data. The DBN ([28], [32]) is useful in normal traffic trending prediction, and capable to identify DoS attack. Moreover, it is a good scalable modeling, for better representation ability. The RBM technique has better capability than other techniques to reproduce different samples output for the used input, which is not considered important if we have huge DoS attack dataset. Consequently, this actual data is more important than sampled data. The CNN-LSTM ([15],[16]) determines the future state by the input and past states of its local neighbor, and it is considered faster than RNN-LSTM, but as CNN requires more CPU, it can lead to higher detection time.

5 CONCLUSIONS AND FUTURE WORK

In conclusion, our research paper analyzed 50 filtered research paper from 2014 to 2021 and showed that the current research papers demonstrate the efficiency of deep learning models for detecting DoS and DDoS in IT and ICS networks. However, the insufficient input for the malicious training data is a major shortcoming for the development and training of these approaches and models. This is a potential cause for over-fitting, which has negative impact on the model performance to learn new data. Hence, the proposed techniques will not be suitable against zero-day attacks. On the other side, some papers proposed techniques that carry additional processing and storing, which increase their delay and make them less suitable for real-time classification and detection. As future work, there are several research directions such as considering modern datasets related to ICS protocols to enhance the classifier training and efficiency. Moreover, future research work should consider the actual cyberspace attack traffic collected from passive monitoring sensors. This would resolve the need for using less features provided over outdated dataset.

ACKNOWLEDGEMENTS We would like to thank Dubai Electronic Security Center (DESC), OpenUAE Research & Development Group and University of Sharjah for their support in this cyber security research study.

REFERENCES

[1] C. Feng, T. Li, and D. Chana, “Multi-level Anomaly Detection in Industrial Control Systems via Package Signatures and LSTM Networks,” *Proceedings - 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017*, pp. 261–272, 2017, doi: 10.1109/DSN.2017.34.

[2] J. Gao *et al.*, “Omni SCADA Intrusion Detection Using Deep Learning Algorithms,” IEEE Internet of Things Journal, vol. 8, no. 2,

pp. 951–961, 2021, doi: 10.1109/JIOT.2020.3009180.0

[3] S. Otoum, B. Kantarci, and H. T. Mouftah, “On the Feasibility of Deep Learning in Sensor Network Intrusion Detection,” IEEE Networking Letters, vol. 1, no. 2, pp. 68–71, 2019, doi: 10.1109/lnet.2019.2901792.

[4] L. Zhou, X. Ouyang, H. Ying, L. Han, Y. Cheng, and T. Zhang, “Cyber-attack classification in smart grid via deep neural network,” ACM International Conference Proceeding Series, pp. 1–5, 2018, doi: 10.1145/3207677.3278054.

[5] S. Kumar, H. Vranken, J. Van DIjk, and T. Hamalainen, “Deep in the Dark: A Novel Threat Detection System using Darknet Traffic,” *Proc. - 2*019 IEEE International Conference on Big Data, Big Data 2019, pp. 4273–4279, 2019, doi: 10.1109/BigData47090.2019.9006374.

[6] C. Fachkha, “Cyber threat investigation of SCADA modbus activities,” 2019 10th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2019 - Proceedings and Workshop, no. August, 2019, doi: 10.1109/NTMS.2019.8763817.

[7] “us-cert.cisa.gov,” *ICS-CERT Annual Assessment Report FY2016*, 2016. https://us-cert.cisa.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf.

[8] R. H. Hwang, M. C. Peng, V. L. Nguyen, and Y. L. Chang, “An LSTM-based deep learning approach for classifying malicious traffic at the packet level,” Applied Sciences (Switzerland), vol. 9, no. 16, 2019, doi: 10.3390/app9163414.

[9] Y. Zhang, X. Chen, L. Jin, X. Wang, and D. Guo, “Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data,” *IEEE Access*, vol. 7, pp. 37004–37016, 2019, doi: 10.1109/ACCESS.2019.2905041.

[10] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” Journal of Information Security and Applications, vol. 50, p. 102419, 2020, doi: 10.1016/j.jisa.2019.102419.

[11] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, “CNN-based network intrusion detection against denial-of-service attacks,” Electronics (Switzerland), vol. 9, no. 6, pp. 1–21, 2020, doi: 10.3390/electronics9060916.

[12] 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.

[13] 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.

[14] 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.

[15] Y. Yu and N. Bian, “An Intrusion Detection Method Using Few-Shot Learning,” *IEEE Access*, vol. 8, pp. 49730–49740, 2020, doi: 10.1109/ACCESS.2020.2980136.

[16] M. Kravchik and A. Shabtai, “Efficient Cyber Attack Detection in Industrial Control Systems Using Lightweight Neural Networks and PCA,” *IEEE Trans. Dependable Secur. Comput.*, 2021, doi: 10.1109/TDSC.2021.3050101.

[17] F. Salo, A. B. Nassif, and A. Essex, “Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection,” Computer Networks, vol. 148, no. November, pp. 164–175, 2019, doi: 10.1016/j.comnet.2018.11.010.

[18] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, “Deep Learning Approach for Intelligent Intrusion Detection System,” *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.

[19] Y. Yang, K. Zheng, B. Wu, Y. Yang, and X. Wang, “Network Intrusion Detection Based on Supervised Adversarial Variational Auto-Encoder with Regularization,” *IEEE Access*, vol. 8, pp. 42169–42184, 2020, doi: 10.1109/ACCESS.2020.2977007.

[20] H. A. Khan, N. Sehatbakhsh, L. N. Nguyen, M. Prvulovic, and A. Zajić, “Malware Detection in Embedded Systems Using Neural Network Model for Electromagnetic Side-Channel Signals,” Journal of Hardware and Systems Security, vol. 3, no. 4, pp. 305–318, 2019, doi: 10.1007/s41635-019-00074-w.

[21] M. A. Ferrag and L. Maglaras, “DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart

Grids," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1285–1297, 2020, doi: 10.1109/TEM.2019.2922936.

[22] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, no. c, pp. 21954–21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[23] M. Russo *et al.*, "Anomaly Detection in Vehicle-to-Infrastructure Communications To cite this version : HAL Id : cea-01888831 Anomaly Detection in Vehicle-to-Infrastructure Communications," 2018.

[24] G. Zizzo, C. Hankin, S. Maffeis, and K. Jones, "Intrusion detection for industrial control systems: Evaluation analysis and adversarial attacks," *arXiv*, 2019.

[25] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for Network Intrusion Detection in Software Defined Networking," Proceedings - 2016 International Conference on Wireless Networks and Mobile Communications, WINCOM 2016: Green Communications and Networking, pp. 258–263, 2016, doi: 10.1109/WINCOM.2016.7777224.

[26] Y. Jia, M. Wang, and Y. Wang, "Network intrusion detection algorithm based on deep neural network; Network intrusion detection algorithm based on deep neural network," Journal of Information Security and Applications, vol. 13, no. 1, pp. 48–53, 2018

[27] Y. Zhang, P. Li, and X. Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network," *IEEE Access*, vol. 7, pp. 31711–31722, 2019, doi: 10.1109/ACCESS.2019.2903723.

[28] P. Wei, Y. Li, Z. Zhang, T. Hu, Z. Li, and D. Liu, "An optimization method for intrusion detection classification model based on deep belief network," *IEEE Access*, vol. 7, pp. 87593–87605, 2019, doi: 10.1109/ACCESS.2019.2925828.

[29] A. Hijazi, E. A. El Safadi, and J. M. Flaus, "A deep learning approach for intrusion detection system in industry network," CEUR Workshop Proceedings, vol. 2343, no. December, pp. 55–62, 2018.

[30] P. Schneider and K. Böttinger, "High-performance unsupervised anomaly detection for cyber-physical system networks," Proceedings of the ACM Conference on Computer and Communications Security, pp. 1–12, 2018, doi: 10.1145/3264888.3264890.

[31] Q. Niyaz, W. Sun, and A. Y. Javaid, "A Deep Learning Based DDoS Detection System in Software-Defined Networking (SDN)," ICST Transactions on Security and Safety, vol. 4, no. 12, p. 153515, 2017, doi: 10.4108/eai.28-12-2017.153515.

[32] N. Marir, H. Wang, G. Feng, B. Li, and M. Jia, "Distributed abnormal behavior detection approach based on deep belief network and ensemble SVM using spark," *IEEE Access*, vol. 6, pp. 59657–59671, 2018, doi: 10.1109/ACCESS.2018.2875045.

[33] G. Andresini, A. Appice, N. Di Mauro, C. Loglisci, and D. Malerba, "Multi-Channel Deep Feature Learning for Intrusion Detection," *IEEE Access*, vol. 8, pp. 53346–53359, 2020, doi: 10.1109/ACCESS.2020.2980937.

[34] R. K. Malaiya, D. Kwon, J. Kim, S. C. Suh, H. Kim, and I. Kim, "An Empirical Evaluation of Deep Learning for Network Anomaly Detection," in *2018 International Conference on Computing, Networking and Communications, ICNC 2018*, Jun. 2018.

[35] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "TSDL: A Two-Stage Deep Learning Model for Efficient Network Intrusion Detection," *IEEE Access*, vol. 7, pp. 30373–30385, 2019, doi: 10.1109/ACCESS.2019.2899721.

[36] M. AL-Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial internet of things based on deep learning models," Journal of Information Security and Applications, vol. 41, no. May, pp. 1–11, 2018,

[37] "CiteSeerX — Guidelines for performing Systematic Literature Reviews in Software Engineering." http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.117.471 (accessed May 18, 2021).

[38] "Add Record Form." http://205.174.165.80/CICDataset/NSL-KDD/ (accessed May 18, 2021).

[39] "UNSW_NB15/NUSW-NB15_features.csv at master · InitRoot/UNSW_NB15 · GitHub." https://github.com/InitRoot/UNSW_NB15/blob/master/NUSW-NB15_features.csv (accessed May 18, 2021).

[40] "IDS 2018 | Datasets | Research | Canadian Institute for Cybersecurity | UNB." https://www.unb.ca/cic/datasets/ids-2018.html.

[41] M. Injadat, A. Moubayed, A. B. Nassif and A. Shami, "Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection," in IEEE Transactions on Network and Service Management, vol. 18, no. 2, pp. 1803-1816, June 2021.