Strengths and weaknesses of deep, convolutional and recurrent neural networks in network intrusion detection deployments

Marek Pawlicki
ITTI Sp. z o.o.
Poznań, Poland *marek.pawlicki@itti.com.pl*

Abstract

The escalating significance of cybersecurity, due to IoT's growth, demands robust security. As cyberattacks increase, machine learning-based network intrusion detection systems (NIDS) provide an effective countermeasure. This paper conducts experiments to optimize an NIDS pipeline using three artificial neural network (ANN) paradigms, demonstrating the importance of optimization and addressing computational time misconceptions. It assesses realistic datasets and compares performance metrics and execution times. Our main contribution is evaluating data processing pipelines for ANN application in NIDS, and benchmarking processing approaches' influence on advanced neural-network methods.
Keywords: Artificial Neural Networks, Real-Time Network Intrusion Detection, Cybersecurity, Artificial Intelligence, Information Security

1. Introduction

The scope of application of Internet of Things (IoT) devices grows and diversifies at a rapid pace, the number of connected devices inflates every year, and the ubiquity of IoT calls for adequate security measures. The emergence and the notoriety of the Mirai botnet, followed by the release of its source code in 2016, brought the issue of IoT cybersecurity to the forefront of public attention [19]. Currently, IoT technology is pervasive in every sector, including homes, offices, health monitoring, transportation, agriculture, surveillance and many other domains [1]. The immediately-apparent downside of the quick and widespread adoption of the premise of IoT is evident in the frequent data breaches and cyber-incidents. For instance, within the first two months of 2022, the US Department of Health and Human Services documented nearly 100 data breaches affecting between 500 to 1.3 million people each [25]. Furthermore, the authors of the IoT Cybersecurity in 2022 Report note that there were over 1.5 billion attacks on IoT in 2020 [5]. This underscores the importance of ensuring strong security measures for the safeguarding of IoT.

The H2020 ELEGANT project aims to manage the surge of IoT and the accompanying Big Data, proposing a unified framework for various use cases such as medical wearables, smart surveillance, large-scale metering, and secure smart riding. A significant aspect of the project is network security, with Machine-Learning-Based Network Intrusion Detection (NIDS) serving as a core element. This approach facilitates real-time management, like controlling IoT data stream rates based on energy consumption indicators.

The major contribution of this paper is in the evaluation of data processing pipelines for the use in the application of Artificial Neural Networks (ANNs) in Network Intrusion Detection Systems, and benchmarking of the influence of the processing approaches on the state-of-the-art neural-network-based methods.

The work compares the results of the different types of neural networks both in terms of classification metrics and in terms of actual execution time. The execution times are plotted in an informative set of figures, which compare the execution times for increasing numbers of samples. The best-performing models for each dataset are reported. Thus, the study aims

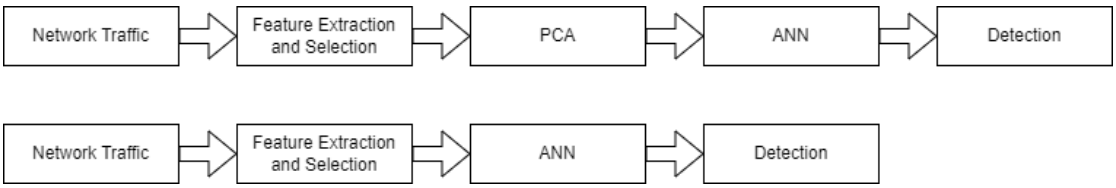

Fig. 1. Two evaluated NIDS pipelines

to answer the following research questions: **RQ1** - How does the use of Principal Component Analysis (PCA) for dimensionality reduction impact the performance and scalability of different ANN models in NIDS? **RQ2** - How do different ANN models (DNN, CNN, RNN) compare in terms of performance and scalability when used in real-time NIDS? **RQ3** - How does the choice of ANN model (DNN, CNN, RNN) influence the execution time during the testing phase in Network Intrusion Detection Systems (NIDS)?

The paper is arranged in the following manner: Section 2 delves into the related works and the methods utilized while Section 3 provides a comprehensive outline of the experimental setup, including the obtained results. Section 4 closes the paper with its conclusions.

2. Related Works, Methods and Materials

There is a vast realm of Artificial Neural Networks (ANNs) with an abundance of different paradigms, topologies and architectures. Multiple research pieces consider the application of different ANNs in the domain of Network Intrusion Detection (NIDS). In the pursuit of the goals of this work, the focus is on networks using the supervised learning paradigm, as presented in [6] [4] [2] [11] [3] [16] and [7], i.e., Deep Neural Networks (DNN), Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN). Drawing on the extensive bibliographic research on ANNs in NIDS detailed in [6], intersecting with our previous research contained in [13][12][14][22], the three most efficient ANN architectures were determined to be used as benchmarks for the use in a real-time ML-based network intrusion detection system.

The methods juxtaposed in this paper were meticulously picked based on their reported superiority in terms of performance metrics in the three identified major categories of supervised ANNs. Thus, the employed networks are: Multi-Layer Perceptrons (MLP), commonly referred to as plain vanilla ANNs (in particular the DNN3 network coming from [26]), convolutional neural networks (CNN), which have migrated from computer vision to numerous cybersecurity applications [27], and finally, recurrent neural networks (specifically LSTMs as disclosed in [18]), which are recognised for their ability to adeptly process sequences.

The authors acknowledge that aside from these approaches, there are different variations of Machine Learning (ML) techniques proposed in the literature In [9], a framework utilising unsupervised and supervised neural networks is described, reducing false positive rates. Unsupervised anomaly detection is discussed in [8], using sets of autoencoders for detecting anomalous traffic. [10] compares different ML approaches for network intrusion detection, providing valuable insights based on the CICIDS2018 dataset and identifying RandomForest as the best method. And then, there are many works which await adaptation to the NIDS domain, like locally specialized classifiers for one-class classification ensembles[15].

2.1. Proposed Evaluated Optimised Pipelines

The evaluated pipelines are broadly depicted in Fig.1. The traffic is collected and a set of flow-based features is extracted. For the training phase, the most informative values are chosen based on the ANOVA F-value metric during the feature selection process. The two evaluated processing pipelines diverge on the next step, where the selected features are subjected to further

Table 1. Artificial Neural Networks for Network Intrusion Detection in the Literature

Supervised Methods											
Deep neural network	[7]	[8]		[10]		[12]	[13]	[14]	[18]		
Recurrent neural network	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]			[20]
Convolutional neural network	[7]	[8]	[9]	[10]	[11]		[13]	[14]		[19]	
Radial Basis Function							[13]				
Unsupervised Methods											
Restricted Boltzmann machine	[7]	[8]	[9]	[10]	[11]	[12]	[13]				
Deep belief network	[7]	[8]	[9]			[12]	[13]				
Auto-encoder	[7]	[8]	[9]	[10]	[11]	[12]	[13]				
Deep migration learning	[7]										
Self-taught learning	[7]										
Replicator neural network	[7]										
Self-organizing map		[8]					[13]				

dimensionality reduction via the Principal Component Analysis algorithm in the first pipeline variant or are fed directly to the Machine Learning component for classification. It is important to note that for the training phase, the training set is subjected to a data-balancing procedure, achieving the 1:1 ratio of benign (majority) class to the total number of all attack class samples. This is done with the use of random subsampling on the majority class. The network's hyperparameters were deduced via the hyperband algorithm [17]. The best performing, optimized networks are pitted against each other in an effort to find the finest of the fine. The two processing pipelines are evaluated - both with and without the use of the PCA algorithm for dimensionality reduction. The achieved Accuracy, Balanced Accuracy and Matthews Correlation Coefficient are reported along with the achieved processing times.

The experiments used the recent netflow-based datasets, SIMARGL2021 [20] and the NetFlow Datasets [23], for training ML-based intrusion detectors to operate in real-time. This represents a realistic scenario where data for training and testing ML algorithms come directly from the infrastructure to be protected.

Evaluated network hyperparameters were as follows: The DNN used 3 layers with 772 and 128 neurons respectively, the Rectified Linear Unit (ReLU) activation function, and the adaptive momentum (ADAM) optimiser. The learning rate was 0.001, with 100 epochs, early stopping, and a batch size of 2.

The CNN employed a 1D Convolutional layer, max pooling, and dropout layers, followed by another set of similar layers, concluding with a flatten layer and a dense layer with 256 neurons. Activation functions were ReLU, the kernel was initialized uniformly, the optimizer was ADAM, batch size was 10, and there were 10 epochs.

The RNN used two sets of 16 LSTM unit layers with return sequences and dropout layers, followed by another LSTM layer and dropout set, and a dense layer of 15 neurons.

3. Experimental Setup, Experiments and Results

3.1. Datasets

This study uses meticulously curated benchmark datasets, the Netflow Dataset and SIMARGL2021, for reproducible results in real-time machine-learning-based network intrusion detection. NetFlow encapsulates realistic traffic and recent attacks, providing 43 flow-based features and 20 traffic classes from 4 different datasets. SIMARGL2021, captured in a real-life scenario, offers standard flow-based features for real-time network intrusion detection, demonstrating how an ML-based NIDS would function in an actual deployment.

The datasets utilised in this study are open, publicly-available benchmarks, available for

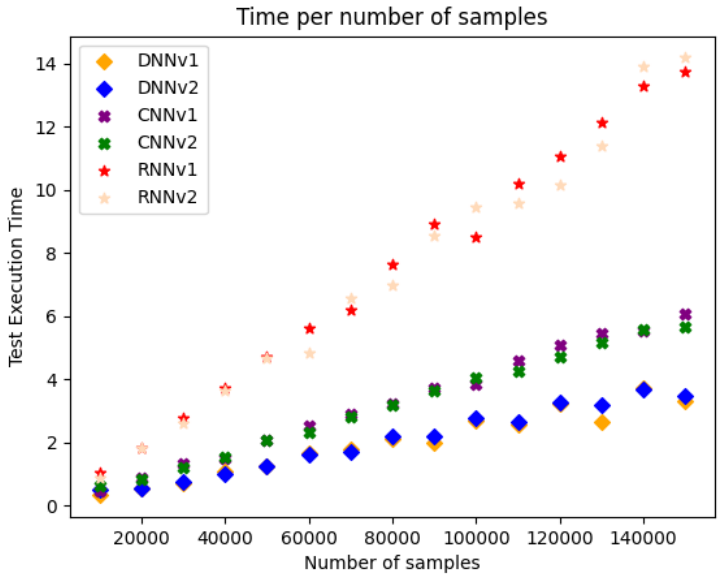

Fig. 2. Execution times of the evaluated models over the SIMARGL2021 dataset

download [1] [2].

3.2. Algorithms and Setup

The authors have sourced the ANN-based NIDS architectures from the state-of-the-art literature and tweaked them to work with the selected novel datasets. On top of that, the authors evaluated the notion of using PCA for dimensionality reduction and its influence on the performance metrics and computational times.

The results of the selected methods are showcased in Tab. 2 for all the six models over the SIMARGL2021 dataset, and in Tab.3, for all the six models over the NetFlow Dataset collection. The models featuring PCA are designated with 'v1'.

Many IDS works use datasets like KDD-Cup99 and NSL-KDD [24], unsuitable for real-time, real-world scenario models. In such a setting, most traffic is non-malicious, causing a data imbalance problem for ML algorithms [21]. Models trained with balanced data improve Recall but can increase false positives, affecting Precision, Matthews Correlation Coefficient (MCC), and False Positive Rate [21].

3.3. Results

Upon closer examination of the results contained in Tab. 2 and Tab. 3, it is observed that the particular algorithms vary dramatically across different ANN paradigms but revolve around similar values for similar algorithms when processing times are concerned. For both SIMARGL2021 and the NetFlow datasets, the measures for 160000 processed samples at the test time are in a similar range for both pipelines including and not including PCA. Upon closer examination of the results, it is found that the RNN model, which has obtained the highest metrics for the NetFlow collection, exhibited a significantly slower testing time compared to the CNN model and the DNN model.

[1] https://www.kaggle.com/datasets/h2020simargl/simargl2021-network-intrusion-detection-dataset
[2] https://staff.itee.uq.edu.au/marius/NIDS_datasets

Table 2. Classification results for 3 neural network paradigms over SIMARGL2021

SIMARGL2021	DNNv1	CNN v1	RNN v1	DNN v2	CNN v2	RNN v2
Accuracy	**0.9935**	0.9708	0.9921	**0.9935**	0.9708	0.9921
Balanced Acc	0.6232	0.6101	**0.8589**	0.6090	0.5612	0.6093
MCC	**0.9903**	0.9570	0.9883	0.9368	0.8384	0.9348
Test execution time /160k (s)	**3.063**	5.987	12.619	3.393	6.143	13.824

Table 3. Classification results for the three neural network paradigms over the NetFlow datasets

NetFlow Dataset	DNNv1	CNNv1	RNNv1	DNNv2	CNNv2	RNNv2
Accuracy	0.8460	0.6370	**0.8856**	0.8460	0.6370	**0.8856**
Balanced Acc	0.3592	0.0764	**0.5037**	0.4182	0.1657	0.4300
MCC	0.7843	0.4562	**0.8426**	0.8224	0.5914	0.8195
Test execution time /160k (s)	**3.423**	5.762	14.005	3.683	5.680	13.706

When considering the overall performance, the CNN model in all variants under-performed when compared to DNN and RNN. With the execution time just above 3s for 160 000 samples, the DNN is over 4.5 times faster than the RNN model and almost two times faster than the CNN model. This is a significant finding for the scalability of ML-based NIDS utilising ANNs as the detector.

Experiments on the SIMARGL2021 dataset are detailed in Tab.2, testing two pipelines: one using PCA (v1) and one without it (v2). Fig.2 demonstrates execution times for the tested ANN models. Results reveal O(n) run time with PCA slightly altering processing times for varying sample sizes. This effect is similarly observed on data from models run over the NetFlow datasets (Fig.5). In both datasets, DNN models showed the least computational effort (Fig.2, Fig.5). In terms of detection metrics (Tab.2), DNN models achieved the highest Accuracy and Matthews Correlation Coefficient while LSTM models had higher Balanced Accuracy but longer execution time. Tab.3 shows Accuracy, Balanced Accuracy, Matthews Correlation Coefficient, and processing times for models over the NetFlow datasets. LSTM models without PCA implemented had the highest detection metrics but longer computational time. Confusion matrices for the classifiers are displayed in Fig.4.

4. Discussion and Future Work

4.1. Discussion

This paper handles some important aspects of employing ANNs in a real-world NIDS; the experimental results point to DNNs for efficient and accurate handling of flow samples. The effect of dimensionality reduction with the use of PCA was highlighted. It is important to note that dataset balancing via random subsampling was employed to mitigate the imbalance problem. Another important feature of the study is that the networks with their hyperparameters setups were drawn from the literature study. The issue of decreasing computational time was evaluated and the results suggest that dimensionality reduction does not always provide enough reduction in the computational cost to justify the time spent at performing the procedure. The experiments also suggest that dimensionality reduction does not always reduce computational time equally for all the ANN variants.

The experiments performed on the SIMARGL2021 and the NetFlow datasets indicate that the chosen neural network type has a decisive influence over the execution time at the testing phase, regardless of the use of PCA.

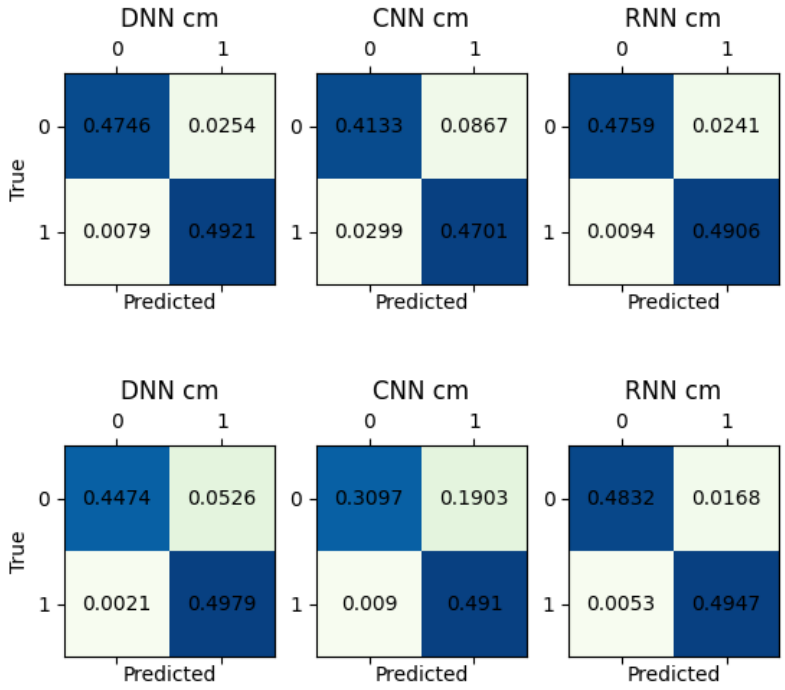

Fig. 4. Binary Confusion Matrices for the three optimised (top) and not-optimised (bottom) models

Future directions: The study aims to advance in several ways: Exploring new methods for data grouping and summarising to provide improved features for ML-based network intrusion detection, ensuring the collected data quality is apt for real-world ML-NIDS, and considering techniques like curriculum learning for effective ML model training. The researchers also aim to incorporate active, online, and lifelong learning techniques to maintain ML-based NIDS's relevancy, introducing a concept drift detector for necessary updates. Additionally, domain adaptation could allow ML-NIDS to utilize knowledge from data collected across different networks and times. Finally, efforts will be dedicated to developing better classification techniques.

5. Conclusions

In the current landscape of interconnected devices, cybersecurity is a crucial aspect influencing the technology proving successful or not. Malicious users are ever on the lookout for opportunities and vulnerabilities. The machine-learning-based network intrusion detection helps provide a measure of protection for the Internet of Things. This paper disclosed a set of experiments evaluating the utilisation of different ANNs in real-time NIDS. The experiments used realistic datasets from multiple sources. The performance metrics and execution times were disclosed and compared. The key contribution of this paper is the benchmarking of processing pipelines for the use of state-of-the-art ANNs in NIDS, aiming to improve the accuracy and efficiency of NIDS.

Acknowledgements

This work is funded under the ELEGANT project, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 957286.

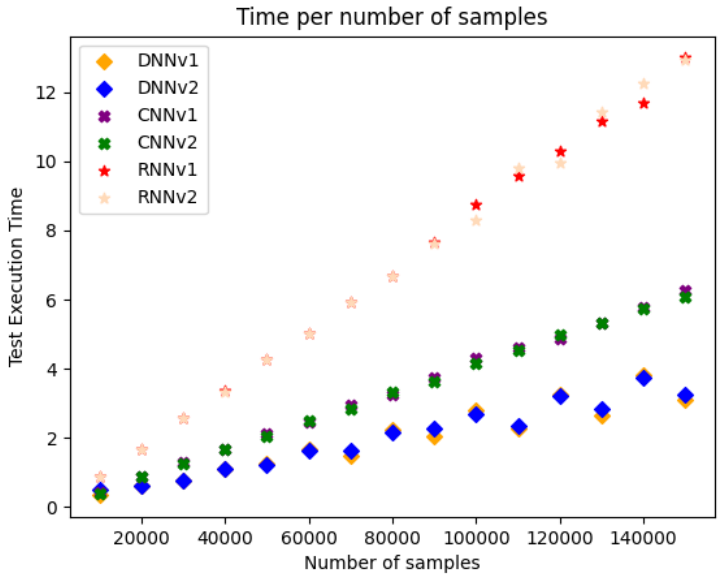

Fig. 5. Execution times of the evaluated models over the NetFlow datasets

References

1. Ahmad, R. and Alsmadi, I. (2021). Machine learning approaches to iot security: A systematic literature review. *Internet of Things*, 14:100365.
2. Aldweesh, A., Derhab, A., and Emam, A. Z. (2020). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues. *Knowledge-Based Systems*, 189:105124.
3. Aminanto, E. and Kim, K. (2016). Deep learning in intrusion detection system: An overview. In *2016 International Research Conference on Engineering and Technology (2016 IRCET)*. Higher Education Forum.
4. Drewek-Ossowicka, A., Pietrołaj, M., and Rumiński, J. (2021). A survey of neural networks usage for intrusion detection systems. *Journal of Ambient Intelligence and Humanized Computing*, 12(1):497–514.
5. Eshghi, B. (2022). IoT Cybersecurity in 2022: Vulnerabilities & Countermeasures. *AI Multiple*. (Accessed on 03/11/2022).
6. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., and Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50:102419.
7. Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., and Atkinson, R. (2017). Shallow and deep networks intrusion detection system: A taxonomy and survey. *arXiv preprint arXiv:1701.02145*.
8. Huang, D.-S. (1999). Radial basis probabilistic neural networks: Model and application. *International Journal of Pattern Recognition and Artificial Intelligence*, 13(07):1083–1101.
9. Huang, D.-S. and Du, J.-X. (2008). A constructive hybrid structure optimization methodology for radial basis probabilistic neural networks. *IEEE Transactions on neural networks*, 19(12):2099–2115.
10. Huang, D.-S. and Zhao, W.-B. (2005). Determining the centers of radial basis probabilistic neural networks by recursive orthogonal least square algorithms. *Applied Mathematics and Computation*, 162(1):461–473.

11. Kim, K. and Aminanto, M. E. (2017). Deep learning in intrusion detection perspective: Overview and further challenges. In *2017 International Workshop on Big Data and Information Security (IWBIS)*, pages 5–10. IEEE.
12. Komisarek, M., Pawlicki, M., Kowalski, M., Marzecki, A., Kozik, R., and Choraś, M. (2021a). Network intrusion detection in the wild-the orange use case in the simargl project. In *The 16th International Conference on Availability, Reliability and Security*, pages 1–7.
13. Komisarek, M., Pawlicki, M., Kozik, R., and Choras, M. (2021b). Machine learning based approach to anomaly and cyberattack detection in streamed network traffic data. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.*, 12(1):3–19.
14. Kozik, R., Pawlicki, M., and Choraś, M. (2018). Cost-sensitive distributed machine learning for netflow-based botnet activity detection. *Security and Communication Networks*, 2018.
15. Krawczyk, B. and Cyganek, B. (2017). Selecting locally specialised classifiers for one-class classification ensembles. *Pattern Analysis and Applications*, 20(2):427–439.
16. Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., and Kim, K. J. (2019). A survey of deep learning-based network anomaly detection. *Cluster Computing*, 22(1):949–961.
17. Li, L., Jamieson, K., DeSalvo, G., Rostamizadeh, A., and Talwalkar, A. (2017). Hyperband: A novel bandit-based approach to hyperparameter optimization. *The Journal of Machine Learning Research*, 18(1):6765–6816.
18. Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., and Gan, D. (2017). Cloud-based cyber-physical intrusion detection for vehicles using deep learning. *Ieee Access*, 6:3491–3508.
19. Margolis, J., Oh, T. T., Jadhav, S., Kim, Y. H., and Kim, J. N. (2017). An in-depth analysis of the mirai botnet. In *2017 International Conference on Software Security and Assurance (ICSSA)*, pages 6–12. IEEE.
20. Mihailescu, M.-E., Mihai, D., Carabas, M., Komisarek, M., Pawlicki, M., Hołubowicz, W., and Kozik, R. (2021). The proposition and evaluation of the roedunet-simargl2021 network intrusion detection dataset. *Sensors*, 21(13):4319.
21. Pawlicki, M., Choraś, M., Kozik, R., and Hołubowicz, W. (2020). On the impact of network data balancing in cybersecurity applications. In *Computational Science–ICCS 2020: 20th International Conference, Amsterdam, The Netherlands, June 3–5, 2020, Proceedings, Part IV 20*, pages 196–210. Springer.
22. Pawlicki, M., Kozik, R., and Choraś, M. (2022). A survey on neural networks for (cyber-) security and (cyber-) security of neural networks. *Neurocomputing*.
23. Sarhan, M., Layeghy, S., Moustafa, N., and Portmann, M. (2020). Netflow datasets for machine learning-based network intrusion detection systems. In *Big Data Technologies and Applications*, pages 117–135. Springer.
24. Thomas, R. and Pavithran, D. (2018). A survey of intrusion detection models based on nsl-kdd data set. *2018 Fifth HCT Information Technology Trends (ITT)*, pages 286–291.
25. U.S. Department of Health and Human Services Office for Civil Rights (2022). Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. (Accessed on 03/11/2022).
26. Vigneswaran, R., Vinayakumar, R., Soman, K. P., and Poornachandran, P. (2018). Evaluating shallow and deep neural networks for network intrusion detection systems in cyber security. *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–6.
27. Xiao, Y., Xing, C., Zhang, T., and Zhao, Z. (2019). An intrusion detection model based on feature reduction and convolutional neural networks. *IEEE Access*, 7:42210–42219.