

Unified and evolved approach based on neural network and deep learning methods for intrusion detection

Alaeddine Boukhalfa¹, Anas El Attaoui², Sara Rhouas², Norelislam El Hami²

¹LASTI Laboratory, National School of Applied Sciences of Khouribga, Sultan Moulay Slimane University, Beni Mellal, Morocco

²Science and Engineering Laboratory, National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco

Article Info

Article history:

Received Oct 31, 2023

Revised Jan 24, 2024

Accepted Mar 21, 2024

Keywords:

Convolutional neural network

Deep learning

Feedforward neural network

Intrusion detection

Long short-term memory

Neural network

NSL KDD

ABSTRACT

Currently, network security has become a major concern for all entities around the world. Attackers employ various methods to disrupt services, which requires new methods to stop them all in one way. Moreover, these intrusions can evolve and overcome security measures and devices, which pushes to use new evolving methods able to accompany the evolution of these threats, to block them. In our paper, we propose a new approach for intrusion detection, founded on neural network (NN) and deep learning (DL) methods. This approach is planned to not only identify threats, but also to develop a long-term memory of them, in order to detect new ones resembling these memorized attacks, and simultaneously, to provide a single way to stop all kinds of intrusions. To test our model, we have chosen the most recently employed methods in literature, NN and DL algorithms: feedforward neural network (FNN), convolutional neural network (CNN), and long short-term memory (LSTM), then we have applied them on network security layer-knowledge discovery in databases (NSL KDD) intrusions dataset. The results of experiments were impressive for all the algorithms, with maximum performances noted by LSTM, which affirms the efficacy of our proposed method for intrusion detection.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Alaeddine Boukhalfa

LASTI Laboratory, National School of Applied Sciences of Khouribga, Sultan Moulay Slimane University
Beni Mellal, Morocco

Email: alaeddine.boukhalfa@gmail.com

1. INTRODUCTION

Currently, the world is undergoing a remarkable transformation within the domain of information technology. People are transferring all the time information through interconnected networks around the world. This evolution necessitates the development of new devices and strategies for intrusion detection, as well as the reinforcement of existing ones, for the purpose of enhancing overall security and protecting networks against potential attacks. The main role of security devices is to monitor carefully and identify traffic passing through the network, it relies on pre-installed rules and strategies to discern effectively between normal and doubtful network activity. Moreover, intruders are naturally interested in the large amount of information and data traversing the network, to exploit this valuable information and data, they are compelled to surmount the security barriers by inventing new attack strategies and reinforcing the current ones. Since the existing security devices and solutions often lack evolution and adaptability, as their algorithms do not evolve to detect automatically new threats, it is imperative to think about implementing new intelligent security systems and methods able to support the evolution of threats.

Additionally, attacks manifest in various forms, such as probe and remote to local (R2L). They can make a system unavailable and prevent users from using it, access to the system root by exploiting it is

vulnerabilities, and retrieve entire network information. This issue of diversity of type pushes us to find a solution to block them all in a one way.

Presently, neural network (NN) and deep learning (DL) methods have achieved significant success across multiple fields, it comprises a suite of techniques employed to identify forms, unveil concealed information within data, and perform predictive analytics [1]. To deal with problems mentioned, we suggest in this manuscript a new proposal for security devices, based on evolution and learning capacity of NN and DL algorithms. These methods will not only identify attacks but will also memorize them, for the purpose of enabling prevention of new attacks resembling to the memorized ones, and also it will stop all types of attacks through a unified way. To check the effectiveness of the proposed idea, we employed the most recent and used NN and DL classifiers [2], [3], such as convolutional neural network (CNN), feedforward neural networks (FNN), and long short-term memory (LSTM). These algorithms were applied on the attacks dataset network security layer knowledge discovery in databases (NSL KDD) [4], and their performances were compared to identify the best suited to our approach.

The manuscript is organized as follows. Section 2 provide a summary of related work. We present the proposed approach in the section 3. The section 4 exhibits adopted evaluation methods. Section 5 describes the evaluation dataset. Performance indicators are exposed in section 6. Section 7 is reserved for results and analysis. Finally, section 8 declares the conclusion and perspectives.

2. RELATED WORK

Recently, various research papers have proposed new ideas to identify intrusions, within data exchange environments. Each study suggests its own steps to treat the subject and presents results. This section of article provides a critical analysis of these studies, in order to expose their methodologies, strengths and weaknesses.

A new idea of intrusion detection was exposed in the manuscript [5]. The authors proposed a new architecture of a passive defense system for monitoring and protecting the network against attacks, this system is based on steps for the choice and execution of methodologies for the training of machine learning (ML) and DL methods. The model was evaluated using both NSL KDD [4] and KDD Cup 1999 [6] datasets. The results reached high detection percentages, except that the authors did not mention the motivations for implementing this new architecture.

Another approach for detection of malicious activities in internet of things (IoT) environment was debated in the document [7]. The authors applied, directly, the deep neural network (DNN) method, which is a DL method, on KDD Cup 1999 [6], NSL KDD [4], and UNSW-NB15 datasets. The results were higher, but the authors did not explain the reasons of using the DNN method.

In the same IoT environment, a new article have proposed an idea for intrusion detection by exploiting DL methods capabilities [8]. The study has suggested the application of the CNN algorithm on two attack datasets. The evaluation has showed a high level of performance. Except that, the authors did not think about testing other DL algorithms, which can show higher levels of performance than CNN.

In a cloud computing environment, a new emergent model for anomaly detection, established on ML methods was proposed [9]. The authors have built a hybrid of clustering and classification methods, employing Gaussian mixture models (GMM), k-means clustering, and random forest (RF). Then, they have tested it is performance using the NSL KDD [4] and KDD cup 1999 [6] datasets. The results were promising. The provided effort was remarkable, except that, the approach was limited to cloud computing environment, and not dedicated to all networks.

Another hybrid model for intrusion detection was presented [10], which combines enhanced genetic algorithm and particle swarm optimization (EGA-PSO), and improved random forest (IRF) methods. Firstly, this combination aims to decrease the imbalance of instances by increasing the size of the minority part. Secondly, it removes the less significant attributes, add a list of decision trees across iterations, controls the performance of classifier, and avoids overfitting problems. The experiments were carried out using the NSL KDD [4] dataset, and the performance of the new model was compared with ML methods. The proposed approach showed a high level of detection, except that it is based on the change in data sampling and it is not dedicated to a raw data.

Another interesting study was realized for intrusion detection, within big data context [11]. The authors downloaded CICIDS2017 [12], which is a big dataset of attacks, and they subjected it to many operations, such as feature selection, deleting duplicate rows, reducing unbalancing of classes, and normalization and encoding of labels. Then, they applied DNN to this modified dataset. The proposal showed a high level of detection, the approach is remarkable since it aims a big data environment. However, the authors did not explain the choice of the employed DL model.

Our proposal is very different comparing it to others discussed. It will exploit the learning and evolution capacity of NN and DL methods, to be an evolved method for intrusion detection. In other words, it will memorize the existing attacks to identify the new ones. At the same time, it will be a unified approach for intrusion detection, since it is oriented to detect all intrusions in a unique way.

3. ADOPTED EVALUATION METHODS

This part is dedicated to present the adopted methods to evaluate our approach. We have chosen the most currently exploited and popular algorithms in literature, which are NN and DL methods: FNN, CNN, and LSTM. Therefore, we will give an overview of them, before test them and choose the best suited to our proposal.

3.1. Neural network

NNs called also artificial neural networks (ANNs), are a fundamental component of artificial intelligence (AI) and ML, they are the origin of DL algorithms [1]. Based on the human brain's functions and structure, NNs are designed to learn and model complex relationships within data. NNs have applications across a wide range of domains, including image recognition, natural language processing, cyber security, and reinforcement learning [13]. At their core, NNs consist of artificial neurons, organized into interconnected several layers, within the same layer, there are no interconnections: an input layer, one or more hidden layers, and an output layer, as exposed in Figure 1 [14], these neurons process data through forward propagation, where computations occur sequentially from input to output. Each neuron receives inputs, multiplies them by associated weights, adds a bias term, and applies an activation function. This process continues through the hidden layers, with each layer extracting and transforming features from the data [15].

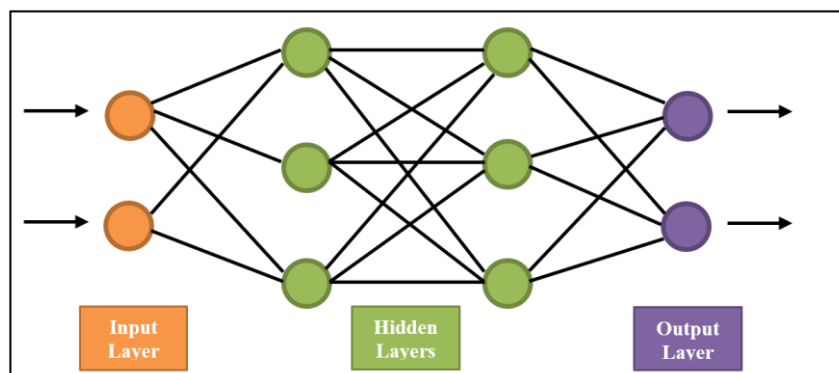


Figure 1. NN architecture

3.2. Feedforward neural network

A FNN is one of the recent NN models created in the domain of AI. It have the ability to realize several classification tasks, such as classification image in the domain of computer vision [16] and language identification [17]. FNN is characterized by the direction of information flow between its layers. Its flow is uni-directional, it means that the information in the model flows in only one direction (forward) from the input nodes, through the hidden nodes and to the output nodes, without any cycles or loops. To be classified, the input data passes, first, through the input layer, secondly, it reaches one or more hidden layers, where the classification is carried out, then it goes out the output layer, which is the classes under analysis. For example, if we have six different classes, six output neurons will be employed and just one positive output to only one specific neuron will constitute a classification match [18].

3.3. Convolutional neural network

A CNN is a type of DL model designed to process and analyze visual data, such as images and videos [19], [20]. It is specially designed to extract meaningful features from input images through the application of convolutional layers. The key characteristic of CNNs is their ability to automatically learn hierarchical representations of data, capturing low-level characteristics like edges and textures in early layers, and gradually detecting higher-level patterns and complex structures in deeper layers. CNNs have proven to

be highly effective in various computer vision tasks, such as image classification, object detection, and segmentation. CNNs contains multiple layers. As presented in Figure 2, the simple structure includes an input layer, connected to one or several convolutional layers, pooling layers, a fully connected layer, and finally an output layer. The convolutional layers extract characteristics from the input data through the employment of filters. The pooling layers decrease the spatial dimensions of the feature maps that reduce computational complexity. The fully connected layer links the extracted characteristics to the output layer, providing the network the possibility to predict or make classification founded on the extracted characteristics [21].

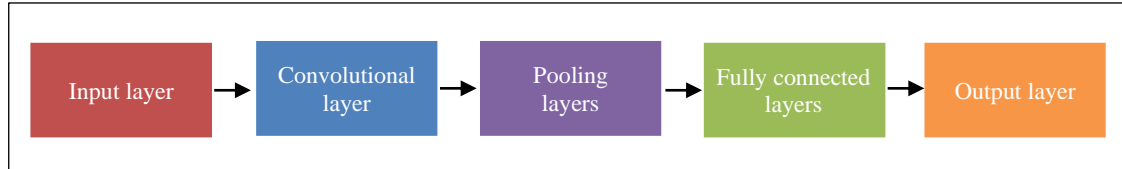


Figure 2. Simple CNN layers

3.4. Long short-term memory

LSTM networks are DL methods, specifically, they are a kind of recurrent neural network (RNN) architecture invented to overcome limitations of traditional RNNs. LSTMs are particularly effective at capturing and remembering information over extended sequences, making them ideal for tasks such as speech recognition, language modeling, and time series forecasting [22]. Figure 3 shows the design of LSTM structure, x and h represent the inputs of the network at time step t , σ means sigmoid function, and $Tanh$ means hyperbolic tangent function. LSTM regroups three gates to capture long-term dependencies. The input gate, output gate, and forget gate allow the LSTM to memorize or forget the new acquired information to the cell of memory [23].

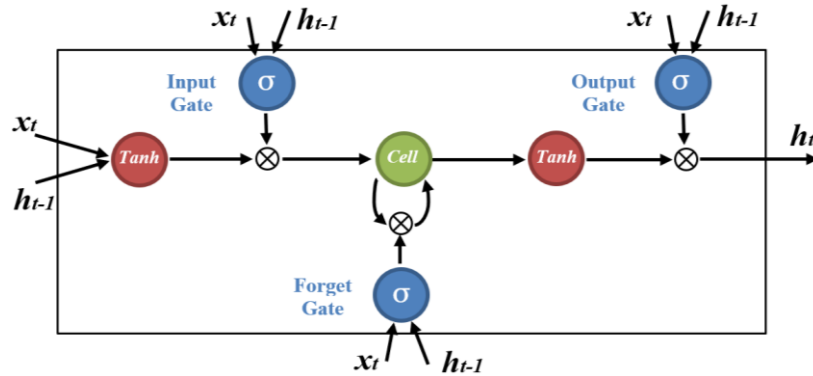


Figure 3. LSTM architecture

4. EVALUATION DATASET

To evaluate our approach, we used NSL KDD dataset [4]. It is an enhanced version of the original KDD Cup 1999 dataset [24]. It was proposed as an improvement over the original dataset to address certain limitations and challenges present in the KDD Cup 1999 dataset, specifically, the NSL KDD dataset aims to overcome the problems of unrealistic data distribution and the existence of duplicate and irrelevant samples [25]. The dataset presents a breakdown of network traffic samples into two main record classes: normal records and attack records as presented in the Table 1. Attack records category is further divided into subcategories, including denial of service (DoS), probe, remote-to-local (R2L), and user-to-root (U2R), the distribution of these subcategories is exposed in the Table 2. To assess the binary classification of our approach, the distribution into two classes is used (normal and attack). Likewise, to evaluate the multiple classification of our approach, the distribution into four classes is adopted (normal, DoS, probe, and U2R-R2L).

Table 1. Distribution of NSL KDD into two classes: normal and attack

Network traffic	Number of samples
Normal record	67343
Attack record	58630
Total	125973

Table 2. Distribution of NSL KDD into multiple classes: normal and attack subcategories

Network traffic	Number of samples
Normal record	67343
Attack record	DoS
	Probe
	U2R
	R2L
Total	125973

5. PERFORMANCE MEASURES

The performance metrics used for evaluation include accuracy, sensitivity, precision, recall and F-score:

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \quad (1)$$

$$Sensitivity = TP / (TP + FN) \quad (2)$$

$$Precision = TP / (TP + FP) \quad (3)$$

$$Recall = TP / (TP + FN) \quad (4)$$

$$F-Score = 2 * (Recall.Precision) / (Recall + Precision) \quad (5)$$

Where, accuracy is the fraction of true identification overall all samples. Sensitivity shows the capacity of the algorithm to identify without error. Precision is the fraction of pertinent samples between all suggested samples. Recall is the fraction of pertinent samples that have been detected over the entire pertinent samples. F-score, called also F-measure, indicates the harmonic average of recall and precision. TP, TN, FP, and FN signify respectively: true positive, true negative, false positive, and false negative, they are obtained from the confusion matrix.

6. RESULTS AND ANALYSIS

In this section, we present and analyze the achieved results. The evaluation of the approach involves two classification scenarios: binary and multiclassification. In the binary classification setup, the dataset is splitted into two distinct classes, one for normal records and the other for attack records. In the case of multiclassification, the occurrence rate of U2R attacks is relatively low, leading to less satisfactory classification results, to address this, we have grouped U2R attacks and R2L attacks into one class, so the dataset is splitted into four distinct classes: probe, normal, DoS, and U2R-R2L.

The results of the binary and multiple classification experiments are presented in Figures 4 to 6 and Tables 3 and 4. Figures 4 to 6 display respectively: accuracy, average of sensitivity, and average of precision for binary classification and multiclassification. While Tables 3 and 4 show precision, recall, and F-score for the classifications of two classes and multiple classes.

Figure 4 reveals the impressive Accuracy achieved for all adopted algorithms (LSTM, CNN, FNN, and NN). For binary classification, the maximum value is 99.98%, reached by LSTM. For multiple classification, the maximum value is 99.93%, reached also by LSTM. Which proves that all algorithms are able to classify normal and attack traffics, with a maximum accuracy reached by LSTM.

Furthermore, Figure 5 displays the average sensitivity values. The values are very high for all proposed algorithms. The greatest values are of LSTM, which are 99.986% for binary recognition and 99.738% for multi-recognition. Indicating that our approach has a superior ability to differentiate between various traffic types, with more high sensitivity using LSTM model.

In addition, as presented in Figure 6, the average precision values are remarkably very high for all tested algorithms. The higher values are marked by LSTM, 99.98% for the classification of two classes, and 98.92% for the classification of multiple classes. Which means that our proposal is very precise for traffic detection, with maximum precision average achieved by LSTM classifier.

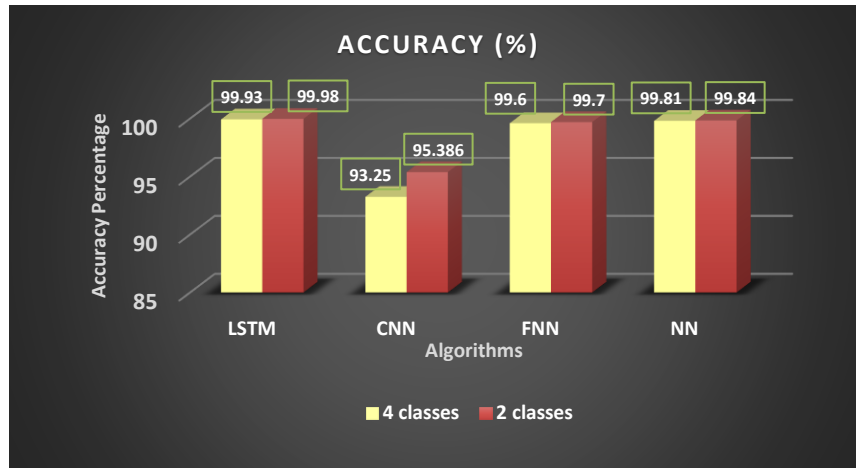


Figure 4. Accuracy for binary classification and multiclassification

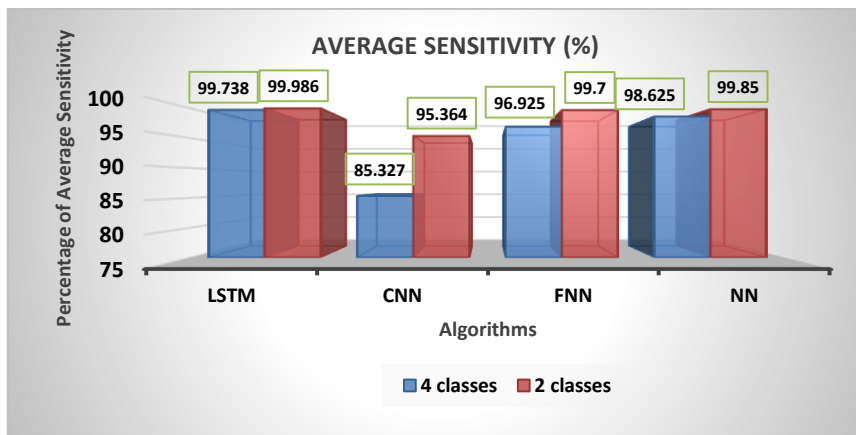


Figure 5. Average of Sensitivity for binary classification and multiclassification

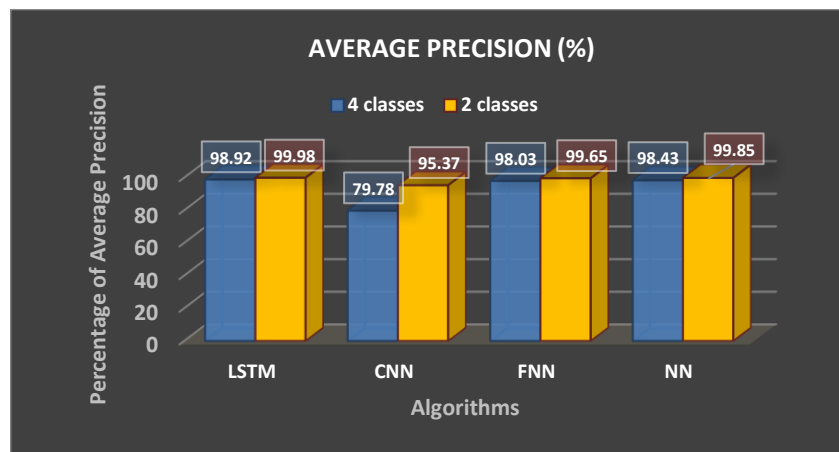


Figure 6. Average of precision for binary classification and multiclassification

Moreover, the values of precision are supreme for all suggested classifiers, as depicted in Tables 3 and 4. Concerning the classification of two classes, precisions reach up to 99.999% for normal traffic, and 99.969% for attack traffic, noted by LSTM. Concerning the classification of multiple classes, the

precisions reach up to 100% for normal traffic and 99.924% for DoS attack, achieved by LSTM also. Which justifies that the proposed idea is efficient, with a remarkable precision of LSTM method.

Additionally, as shown in Tables 3 and 4, the values of recall are all higher. In binary detection context, the maximum recall values are 99.977% for normal traffic, and 99.998% for attack traffic, mentioned by LSTM. In multiple detection context, the maximum recall values are 99.938% for normal traffic, and 99.906% for DoS attack traffic, marked by LSTM too. Which proves that our new idea has a great ability to detect instances, with more exactitude noted by LSTM algorithm.

As displayed in Tables 3 and 4, the values of F-score reach a very high level for all employed classifiers. In the case of binary classification, the value of F-score reaches up to 99.986% for normal traffic and 99.983% for attack traffic, mentioned by LSTM method. In the case of multiple classification, the value of F-score reaches up to 99.969% for normal traffic and 99.915% for DoS attack traffic. Which explains that our suggested proposition is very accurate, with a significant precision using LSTM model.

All the experiment results have proved that our approach is very efficient and accurate, for intrusion detection. All the classifiers (NN, FNN, CNN, and LSTM) reach very high values concerning all performance indicators, with maximum performance indicators marked by LSTM algorithm. Which confirms the great ability of the proposal, to differentiate between real and doubtful traffic, with more precision using LSTM algorithm.

Table 3. Recall, Precision and F-Score of 2 classes

Classifier	Class	Precision (%)	Recall (%)	F-Score (%)
LSTM	Normal	99.999	99.977	99.986
	Attack	99.969	99.998	99.983
CNN	Normal	95.664	95.705	95.684
	Attack	95.067	95.023	95.045
FNN	Normal	99.600	99.700	99.650
	Attack	99.700	99.700	99.700
NN	Normal	99.900	99.900	99.900
	Attack	99.800	99.800	99.800

Table 4. Recall, Precision and F-Score of 4 classes

Classifier	Class	Precision (%)	Recall (%)	F-Score (%)
LSTM	Normal	100	99.938	99.969
	DoS	99.924	99.906	99.915
	U2R, R2L	95.896	99.106	97.475
	Probe	99.863	100	99.931
CNN	Normal	96.665	95.186	95.920
	Dos	93.690	93.198	93.443
	U2R, R2L	53.394	70.158	60.639
	Probe	75.360	82.765	78.889
FNN	Normal	96.600	99.800	99.700
	Dos	99.900	99.900	99.900
	U2R, R2L	93.500	89.500	91.456
	Probe	99.100	98.500	98.799
NN	Normal	99.900	99.800	99.850
	Dos	99.900	99.900	99.900
	U2R, R2L	94.500	95.200	94.849
	Probe	99.400	99.600	99.500

7. CONCLUSION

In this manuscript, we have proposed a new approach based on NN and DL methods for intrusion detection. This approach aims to memorize existing attacks, in order to stop other new ones that are similar to them, and at the same time, it will be a unique way to block all types of menaces. To validate our idea, we have selected the most recent and popular NN and DL methods: FNN, CNN, and LSTM, and we have evaluated their detection using NSL KDD intrusions dataset. The detection results were very interesting for all methods, with maximum performances marked by LSTM. which justifies the validity of our suggestion for intrusion detection, with maximum performances using LSTM model. In future, we will test our proposal within a real network.




REFERENCES

- [1] I. H. Sarker, "Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions," *SN Computer Science*, vol. 2, no. 6, 2021, doi: 10.1007/s42979-021-00815-1.




- [2] J. Ahmad, H. Farman, and Z. Jan, "Deep learning methods and applications," in *Deep Learning: Convergence to Big Data Analytics*, pp. 31–42, 2019, Singapore: Springer, doi: 10.1007/978-981-13-3459-7_3.
- [3] A. Mosavi, S. Ardabili, and A. R. V. -Kóczy, "List of deep learning models," *International Conference on Global Research and Education*, vol. 101, pp. 202–214, 2020, doi: 10.1007/978-3-030-36841-8_20.
- [4] M. Eroğlu, "NSL-KDD network intrusion detection," *GitHub*, 2023, [Online]. Available: https://github.com/Mamcose/NSL-KDD-Network-Intrusion-Detection/blob/master/NSL_KDD_Train.csv.
- [5] B. M. Serinelli, A. Collen, and N. A. Nijdam, "Training guidance with KDD Cup 1999 and NSL-KDD data sets of ANIDINR: anomaly-based network intrusion detection system," *Procedia Computer Science*, vol. 175, pp. 560–565, 2020, doi: 10.1016/j.procs.2020.07.080.
- [6] "SIGKDD: KDD Cup 1999: computer network intrusion detection," *SIGKDD*, 2023, [Online]. Available: <https://www.kdd.org/kdd-cup/view/kdd-cup-1999/Data>.
- [7] S. Choudhary and N. Kesswani, "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT," *Procedia Computer Science*, vol. 167, pp. 1561–1573, 2020, doi: 10.1016/j.procs.2020.03.367.
- [8] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for IoT networks through deep learning model," *Computers and Electrical Engineering*, vol. 99, 2022, doi: 10.1016/j.compeleceng.2022.107810.
- [9] K. Samunnisa, G. S. V. Kumar, and K. Madhavi, "Intrusion detection system in distributed cloud computing: Hybrid clustering and classification methods," *Measurement: Sensors*, vol. 25, pp. 1–12, 2023, doi: 10.1016/j.measen.2022.100612.
- [10] A. K. Balyan *et al.*, "A hybrid intrusion detection model using EGA-PSO and improved random forest method," *Sensors*, vol. 22, no. 16, pp. 1–20, 2022, doi: 10.3390/s22165986.
- [11] K. Farhana, M. Rahman, and M. T. Ahmed, "An intrusion detection system for packet and flow based networks using deep neural network approach," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 5, pp. 5514–5525, 2020, doi: 10.11591/IJECE.V10I5.PP5514-5525.
- [12] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Intrusion detection evaluation dataset (CIC-IDS2017)," *Canadian Institute for Cybersecurity*, 2018, [Online]. Available: <https://www.unb.ca/cic/datasets/ids-2017.html>.
- [13] O. I. Abiodun, A. Jantan, A. E. Omolara, K. V. Dada, N. A. E. Mohamed, and H. Arshad, "State-of-the-art in artificial neural network applications: a survey," *Heliyon*, vol. 4, no. 11, pp. 1–41, 2018, doi: 10.1016/j.heliyon.2018.e00938.
- [14] Y. Wang, Z. Cui, and R. Ke, "Fully connected neural networks," *Machine Learning for Transportation Research and Applications*, pp. 41–55, 2023, doi: 10.1016/b978-0-32-396126-4.00009-6.
- [15] S. Bashir and B. Arora, "Prediction of need for cyber training for university students using artificial neural networks," *Procedia Computer Science*, vol. 218, pp. 1414–1423, 2022, doi: 10.1016/j.procs.2023.01.120.
- [16] X. Zhou, H. Liu, C. Shi, and J. Liu, "The basics of deep learning," *Deep Learning on Edge Computing Devices*, pp. 19–36, 2022, doi: 10.1016/b978-0-32-385783-3.00009-0.
- [17] I. L. -Moreno, J. G. -Dominguez, D. Martinez, O. Plchot, J. G. -Rodriguez, and P. J. Moreno, "On the use of deep feedforward neural networks for automatic language identification," *Computer Speech and Language*, vol. 40, pp. 46–59, 2016, doi: 10.1016/j.csl.2016.03.001.
- [18] J. A. L. Marques, F. N. B. Gois, J. P. do V. Madeiro, T. Li, and S. J. Fong, "Artificial neural network-based approaches for computer-aided disease diagnosis and treatment," *Cognitive and Soft Computing Techniques for the Analysis of Healthcare Data*, pp. 79–99, 2022, doi: 10.1016/B978-0-323-85751-2.00008-6.
- [19] S. Indolia, A. K. Goswami, S. P. Mishra, and P. Asopa, "Conceptual understanding of convolutional neural network-a deep learning approach," *Procedia Computer Science*, vol. 132, pp. 679–688, 2018, doi: 10.1016/j.procs.2018.05.069.
- [20] S. Xie, R. Girshick, P. Dollár, Z. Tu, and K. He, "Aggregated residual transformations for deep neural networks," *Proceedings-30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017*, vol. 2017, pp. 5987–5995, 2017, doi: 10.1109/CVPR.2017.634.
- [21] M. T. Ahad, Y. Li, B. Song, and T. Bhuiyan, "Comparison of CNN-based deep learning architectures for rice diseases classification," *Artificial Intelligence in Agriculture*, vol. 9, pp. 22–35, 2023, doi: 10.1016/j.aiaa.2023.07.001.
- [22] K. Smagulova and A. P. James, "A survey on LSTM memristive neural network architectures and applications," *European Physical Journal: Special Topics*, vol. 228, no. 10, pp. 2313–2324, 2019, doi: 10.1140/epjst/e2019-900046-x.
- [23] S. Oh, K. Jang, J. Kim, and I. Moon, "Online state of charge estimation of lithium-ion battery using surrogate model based on electrochemical model," *Computer Aided Chemical Engineering*, vol. 51, pp. 1447–1452, 2022, doi: 10.1016/B978-0-323-95879-0.50242-3.
- [24] R. R. Nuiaa, S. Manickam, A. H. Alsaedi, and E. S. Alomari, "A new proactive feature selection model based on the enhanced optimization algorithms to detect DRDoS attacks," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 2, pp. 1869–1880, 2022, doi: 10.11591/ijece.v12i2.pp1869-1880.
- [25] A. Divekar, M. Parekh, V. Savla, R. Mishra, and M. Shirole, "Benchmarking datasets for anomaly-based network intrusion detection: KDD CUP 99 alternatives," *2018 IEEE 3rd International Conference on Computing, Communication and Security, ICCCS 2018*, pp. 1–8, 2018, doi: 10.1109/CCCS.2018.8586840.

BIOGRAPHIES OF AUTHORS






Alaeddine Boukhalfa    is a professor of computer science at National School of Applied Sciences (NSAS) in Khouribga, Morocco. He received an engineer degree in Computer Science from (NSAS) in Tetouan, Morocco. He got his Ph.D. degree in computer sciences at (NSAS) in Kenitra, Morocco. His researches is interested in big data and AI. He has published many conference/journals papers. He can be contacted at email: alaeddine.boukhalfa@gmail.com.






Anas El Attaoui    is a Ph.D. Student in computer science from (NSAS) in Kenitra, Morocco. He received an engineer degree from (NSAS) in Kenitra, Morocco. His research interests reside in the fields of big data and business intelligence. He has published a conference/journal paper. He can be contacted at email: anaselatt045@gmail.com.



Sara Rhoulas    is a Ph.D. student in computer science from (NSAS) in Kenitra, Morocco. She received an engineer degree from (NSAS) in Kenitra, Morocco. Her research interests reside in the fields of big data, interoperability, and artificial intelligence. She has published a conference/journal paper. She can be contacted at email: rhoulas.sara@gmail.com.



Norelislam El Hami    is a professor of computer science at (NSAS) in Kenitra, Morocco. He obtained a Diploma of State Engineer from Polytechnic Faculty of MONS in Belgium. He earned a Ph.D. in Computer Science from the National Institute of Applied Sciences of Rouen in France, and Ph.D. in Applied Mathematics and Computer Science from M V-Agdal University, EMI, Rabat, Morocco. He has published many conference/journals papers. He can be contacted at email: norelislam@outlook.com.