Artificial Intelligence in Cybersecurity

Journal Homepage: sciencesforce.com/aics

Artificial Intell. Cyb. Vol. 1 (2024) 12–20

Paper Type: Original Article

A CNN-RF Hybrid Model for Intrusion Detection System: Analysis, Improvements, and Application

Ahmed Elmasry [1], **and Walid Abdullah** [1,*]

[1] Department of Computer Science, Faculty of Computers and Informatics, Zagazig University, Egypt; Emails: a.elmasry24@fci.zu.edu.eg; waleed@zu.edu.eg.

Received: 07 Sep 2023 **Revised**: 07 Dec 2023 **Accepted**: 29 Jan 2024 **Published**: 31 Jan 2024

Abstract

With the rapid development of technologies and the growing need for the internet in most aspects of life, the need for cyber security is also growing. There are various types of cyber intrusions attacks making detecting and identifying these attacks not an easy task. Conventional intrusion detection systems (IDS) lack accuracy which makes them unreliable and dependable. Recent applications of machine learning techniques have rapidly grown in the recent years made it a powerful tool that can be utilized for detecting cyber intrusion attack accurately. This paper proposed an enhanced convolution neural networks (CNNs)-based machine learning model for intrusion detection. This model makes use of the characteristics of CNN layers for extracting useful features and the Random Forest model for Robust intrusion attack detection. The model utilizes the NSL-KDD dataset, and it outperforms other deep learning (DL) techniques in the multi-class classification tasks, it can identify intrusion attacks with high precision and reach 99.3% accuracy rate leading for increasing the efficiency of intrusion detection and open new avenues for research.

Keywords: Intrusion Detection System, Convolution Neural Network, Random Forest, Features Extraction, Machine learning, Deep Learning, Cybersecurity.

1 | Introduction

The rabid development of new technologies like internet technologies and cloud computing was a reason for the rise in online data transmissions and storing which presents a challenge to intrusion detection systems (IDS) [1]. Malicious applications, or malware, present a significant problem to the design of intrusion detection systems (IDSs). The complexity of malicious attacks makes it difficult to identify hidden malware. There are two types of IDS: network-based (NIDS) and host-based (HIDS). SIDS can identify previous intrusions, but their detection rate is lower than expected. Open-source SIDS with default configurations is recommended for web assault defense [2].

Firewalls are crucial in preventing illegal access to networks, but conventional solutions like firewalls and even standard signature-based intrusion detection approaches are no longer viable and can be easily evaded by attackers [3]. IDS are essential in identifying unusual events, malicious activity, or policy violations. They can detect when an attacker has exploited a system flaw and monitor data transfers. The advancement of IDS is driven by the complexity of new networked systems, their vulnerability to security flaws, the inability to

Corresponding Author: waleed@zu.edu.eg

https://doi.org/10.61356/j.aics.2024.1212

Licensee **Artificial Intelligence in Cybersecurity**. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0).

achieve 100% protection with intrusion prevention technologies, the difficulty of detection by authorized users, and the development of new attack types that bypass prevention and detection methods.

In recent years, machine learning technologies have rapidly developed and have been utilized across many fields, due to this development, researchers have turned to using these techniques in cybersecurity. In [4], a dynamic framework with deep learning is recommended for improved security solutions. Other studies used various machine learning techniques like Naïve Bayes (NB) algorithm and support vector machines (SVM) for intrusion detection purposes [5, 6]. To increase the accuracy and get better performance of the models, researchers have used deep learning techniques like CNN and long short-term memory (LSTM) for deep analysis and to get better data understanding to increase the IDS system's accuracy in intrusion detection [7,8].

In this study, we introduce a hybrid convolution neural networks (CNNs)-based ML model for intrusion detection that utilizes the random forest (RF) model in the classification stage. This integration can take advantage of the CNN layers in extracting the useful features and the power of RF in in multi-class classification tasks for classifying and detecting intrusion attacks. This integration helps in eliminating the overfitting problem in data and increasing system performance. The proposed model is trained and evaluated on the NSL-KDD dataset.

The proposed hybrid model achieved superior results in terms of accuracy, precision, recall, and F1-Score by 0.993, 0.99, 0.99, 0.99, 0.99, and 0.99, respectively. The model was compared with other DL models such as the gated recurrent model (GRU) and LSTM deep learning model. As a result, this paper's primary contributions can be summarized as follows:

- Proposing a novel hybrid system that combines between CNNs and RF models.
- Utilizing CNN layers for Extracting significant features method.
- utilized RF classifier to eliminate the overfitting problem and provide more accuracy.
- The proposed model achieved superior results in terms of accuracy 0.993
- The proposed model was compared with other DL models such as GRU and LSTM.

The remainder of the paper is divided as follows. Section 2 provides the background needed for this study. Section 3 presents the materials and methods of this study. Section 4 presents the proposed model stages. Section 5 presents experimental results. Section 6 illustrates the conclusion and future directions of this proposal.

2 | Literature Review

For many years, academics have researched intrusion detection systems using publicly available datasets such as NSL-KDD as test subjects. 41 features and classification labels for both common access and various attack types are included in the dataset. For the past ten years, intrusion detection systems have used ML algorithms; nevertheless, DL technology is gaining greater prominence. Although it has potential in computer-based systems, the CNNs still need more investigation in IDS.

Stiawan et al. [9] used the CIC-IDS2017 dataset to train ML models on traffic anomaly detection, they selected significant features using Information Grain (IG) which was proposed by Nimbalkar and Kshirsagar [10], then trained the dataset using various ML classifiers such as RF, NB, Bayes Net (BN). And RF model provided the best accuracy compared to all other classifiers.

In [11], The authors proposed a hybrid methodology that integrates three techniques naïve base feature selection for features selection, optimized SVM for rejecting outliers, and prioritized k-nearest neighbors as a classifier for identifying and classifying the threats. the model was tested on three datasets including The Kyoto dataset. And the results in real-time demonstrated the effectiveness of the approach in tackling the problem of multi-class classification.

Hanmate et al. [12] introduced a deep convolutional neural network (DCNN) framework for intrusion detection, utilizing DL to extract meaningful features from network traffic data. The model, trained on large-scale datasets, effectively discriminates between normal and anomalous behavior. The performance of the model is evaluated using four publicly available IDS datasets, showing a 99.79% to 100% detection accuracy. This study provides valuable insights for network security and intrusion detection systems.

Another recent study presented AttackNet, a DL model for detecting and classifying botnet attacks in IIoT networks. The model, based on an adaptive CNN-GRU model, outperforms state-of-the-art techniques, and outperforms real-time anomaly detection systems in IIoT, achieving an accuracy of 99.75% across ten classes [13].

Sadia et al. proposed a NIDS for Wi-Fi-based Wireless Sensor Networks (WSNs) to protect against cyber threats like impersonation, flooding, and injection attacks. The system uses a meticulous feature selection process, focusing on relevant security indicators. The approach uses a CNN for optimal detection and prevention, reducing loss values and false alarm rates [14].

Another contribution proposed a new system for detecting intrusions in IoT networks in agriculture, utilizing the NSL KDD data set and evaluating its performance using CNN architectures like VGG16, Inception, and Xception, and comparing it with classical machine learning algorithms [15].

Authors in [16] used a feature selection technique based on the sandpiper optimization algorithm (SOA) to select only relevant features from the data with a minimum information loss and then applied transfer learning and used the AlexNet pre-trained model. And incorporates an extended equilibrium optimizer (EEO) for updating the network weights, The results indicate that the proposed approach outperformed other methodologies.

3 | Materials and Methods

In this work a hybrid ML model is proposed, it exploits the integration between CNN to extract important features from data and the RF ensemble classifier for the classification stage. The NSL-KDD dataset was utilized to train the proposed model.

3.1 | Utilize Dataset

The ISCX NSL-KDD data set addresses issues with the KDD'99 data set. Despite its limitations, it can serve as a benchmark for researchers comparing intrusion detection methods. The reasonable number of records in the NSL-KDD train and test sets ensures consistent and comparable evaluation results across different research works. The training set in NSL-KDD is called KDDTrain+ and the test set is called KDDTest+. Each record in the NSL-KDD data set has 42 attributes. 41 attributes represent the characteristic attributes of the data, and 1 attribute represents the type of attack [17].

3.2 | Convolution Neural Networks (CNN)

CNNs is one of the powerful DL models that was created especially for examining various datasets, including time series data and two-dimensional image input [18]. the most important of CNN is the Convolutional Layers. these layers use a filter called a kernel that moves between the Input Data to identify patterns and spatial relationships to discover the most important features in the Data. After extracting features, usually, A Pooling layer is used after Convolutional Layers to minimize the size of the input representation by choosing the maximum value within a certain pool size window that helps in highlighting the most significant features. The output from the convolutional layers is transmitted to the fully connected layers, which perform regression or classification tasks. It has demonstrated significant promise in time series data management, including stock price, solar irradiance, and wind speed predictions. The kernel functions as a filter in 1D convolution [19].

3.3 | Random Forest (RF)

Random Forest is one of the most effective ensemble models that is used for both classification and regression tasks, it was proposed by Breich in 2001. It ensembles a collection of decision trees known as a forest, A random selection of attributes is used to generate each decision tree at each node for separation. Finally, a process called aggregation occurs when the results of all decision trees combine to provide the outcome based on majority voting [20, 21].

4 | Proposed Work

The proposed work can be divided into four main stages data processing, data normalization, CNN feature extraction, and classification stage as shown in Figure 1.

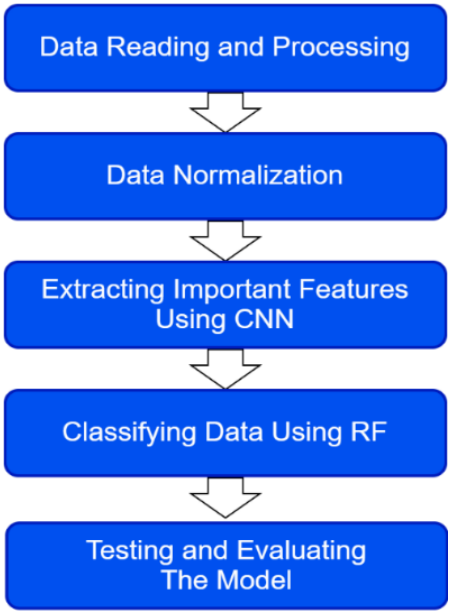

Figure 1. The Stages of the proposed work.

4.1 | Proposed Work Stages

4.1.1 Dataset Preprocessing

We re-classify the data into only two categories, the first category is normal. The second category is attack (Abnormal). Table 1 shows the dataset records number record of each category.

Table 1. Dataset records the number record of each category.

Total	Normal	attack
125,973	67343	58630

One hot encoding is a powerful technique used to convert categorical data to numerical Data. The features (protocol_type, service, Flag) are converted into numerical form so they can be input to training models. We obtained 122 features after one hot encoding process.

4.1.2 Data Normalization

Data normalization is the process of processing data by suggesting data values to close values, which results in better performance. A RobustScaler technique is utilized. This measure subtracts the median and scales data according to a quantitative range IQR defaults: interquartile range which is the difference between the 75th and 25th percentiles. It is mathematically represented as Eq. (1).

$$X_{new} = \frac{X - X_{median}}{IQR} \tag{1}$$

4.1.3 CNN Features Extraction

We propose a novel CNN model that consists of three 1D-convolution layers, followed by one flattened layer, then dense layers for producing the output features.

4.1.4 Classification Stage

An ML model is obtained to train on the important features extracted from the DL model. The extracted features from the last layer are inputs to the RF model. This can reduce the overfitting problem and increase performance.

4.2 | Proposed Model Architecture

The proposed model consists of two main parts: the first one is 3 convolution layers to extract important information from data, and then the output is reshaped using a flattened process to be entered into the dens layers that produce the output features of the first part, these extracted features is the input to the second part, which the random forest classifiers to perform classification task and produce the final prediction. More details for the proposed model architecture are shown in Figure 2.

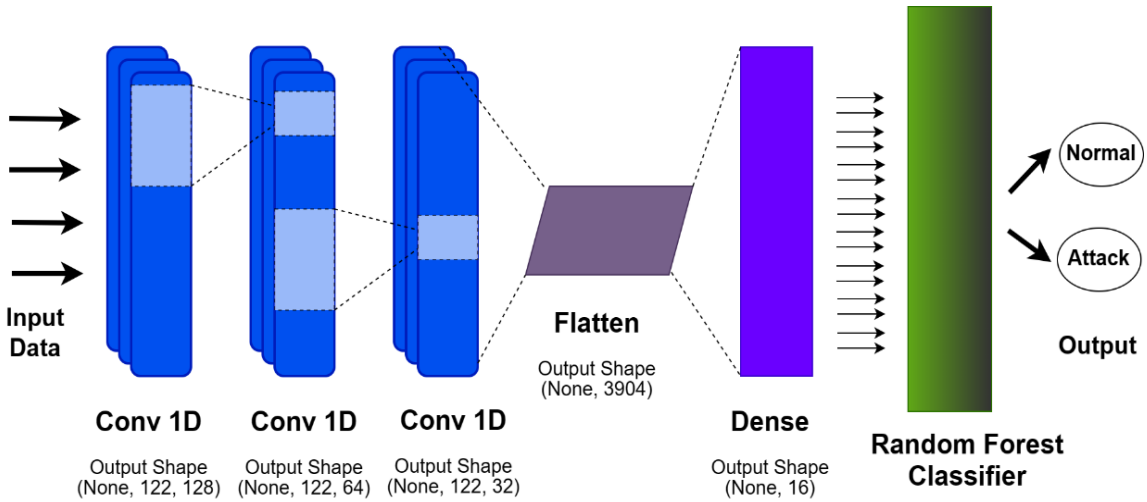

Figure 2. The proposed model architecture.

5 | Experiments, Results, and Discussion

In order to evaluate the proposed model and compare its performance against other models, four different deep learning models are implemented as follows:

1. The CNN-based model Consists of 2- Conv1d layer with Max-pooling and Dropout layers followed by an output layer.
2. MLP model which consists of 3 Dense layers with activation function ReLU and output layer.
3. LSTM model which involves three LSTM layers followed by a dropout layer and output layer.
4. The GRU model consists of three GRU layers followed by a dropout layer and an output layer.

All Models are trained on NSL-KDD data set using Adam optimizer with a learning rate of .0001, batch size of 1000, and number of 30 epochs [22]. The initial weights are optimized using the Categorical Cross Entropy (CCE) loss function to increase classification accuracy. The loss function is mathematically defined as presented in Eq. (2):

Minimize: $\mathrm{loss(CCE)} = -\sum_{i=1}^{M} y_i \cdot \log \check{y}_i$ (2)

Where y_i is true value $\breve{y}_i$ is shorthand for a vector that contains all of the outputs that were predicted based on the training samples.

5.1 | Experiments Setup

The experiments were conducted on the Kaggle platform with GPU Nvidia Tesla P100 With RAM of 16 GB, the proposed model was developed and trained using Python version 3.10.13, Keres version 3.5.0 [23], and TensorFlow version 2.15.5 [24].

5.2 | Evaluation Metrics

In order to evaluate the proposed model and compare it against other state-of-art a set of metrics are used such as Accuracy, precision, recall, and F1-score.

- Accuracy – Measures the ratio of the number of correct predictions for all categories to the total number of predictions. It is mathematically represented in Eq. (3).
  $$\text{Accuracy} = \frac{(TP+TN)}{(TP+FP+TN+FN)} \quad (3)$$
- Precision – The ratio of the number of correct predictions for a category to the total number of predictions in the same category. It is mathematically represented in Eq. (4).
  $$\text{Precision} = \frac{TP}{(TP+FP)} \quad (4)$$
- Recall – Measures the proportion of correctly identified predictions for a category to the total number of identified predictions in the same category. it is mathematically represented in Eq. (5).
  $$\text{Recall} = \frac{TP}{(TP+FN)} \quad (5)$$
- F1 Score – is the harmonic mean of precision and recall. it is mathematically represented in Eq. (6).
  $$\text{F1 Score} = 2 \times \frac{\text{recall} \times \text{precision}}{\text{recall} + \text{Precision}} \quad (6)$$

5.3 | Experimental Results

In this section, the performance of the proposed model was measured and compared against other implemented models in terms of utilized evaluation metrics accuracy, precision, recall, and F1-score, As shown in Table 2, The proposed model outperformed all other models and achieved the highest accuracy with .0.993. Figure 3 shows the rank of each model with different metrics. The proposed model achieves the highest rank, followed by the GRU model. Figure 4 shows the Confusion Matrix used to provide the performance details of a Proposed model for each category.

Table 2. Performance of proposed model.

Model	Accuracy	Precision	Recall	F1 Score
CNN	.955	0.96	0.95	0.95
LSTM	.986	0.99	0.99	0.99
GRU	.987	0.99	0.99	0.99
MLP	.983	0.98	0.98	0.98
Proposed Model	**0.993**	**0.99**	**0.99**	**0.99**

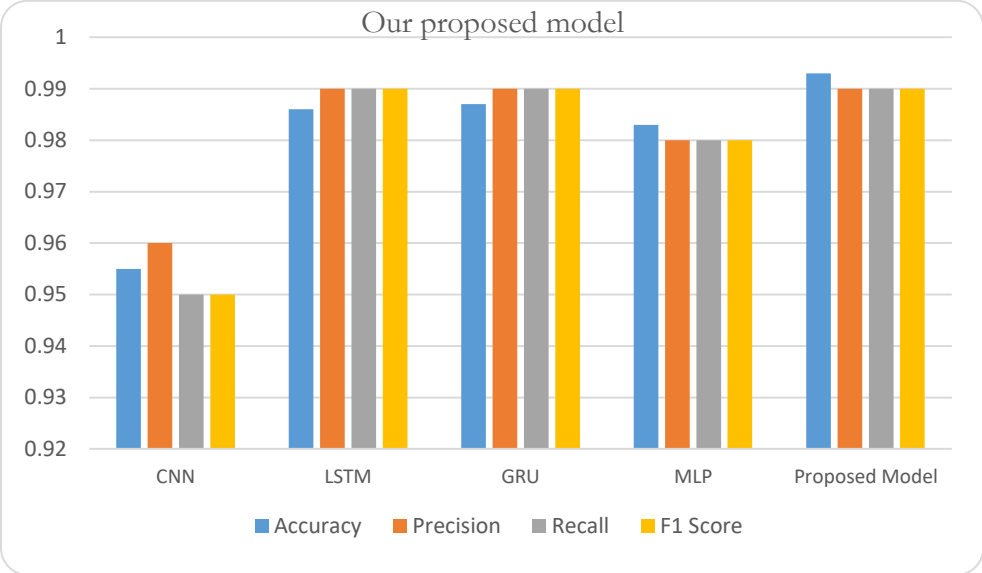

Figure 3. The proposed model performance.

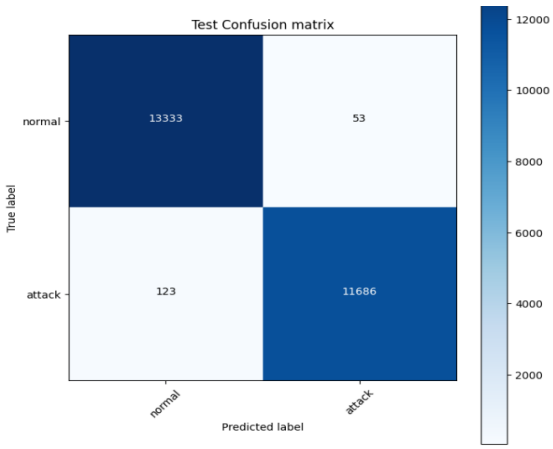

Figure 4. Confusion matrix of proposed model.

6 | Conclusion and Future Work

The increasing requirement for cyber security has led to a focus on detecting cyber intrusions. Conventional intrusion detection systems (IDS) are not very accurate or reliable. In this work, we present an adapted version of a machine learning (ML) model with a CNN model to detect network intrusions. The Random Forest (RF) classifier is utilized to eliminate the overfitting problem and provide accuracy. The proposed model was compared with other DL models such as GRU and LSTM. The proposed model achieved superior results in terms of accuracy, precision, recall, and F1-Score by 0.993, 0.99, 0.99, 0.99, 0.99, and 0.99, respectively. Future directions include working on designing a new feature selection mechanism and integrating it with different ML and DL models to achieve high intrusion detection accuracies.

Acknowledgments

The author is grateful to the editorial and reviewers, as well as the correspondent author, who offered assistance in the form of advice, assessment, and checking during the study period.

Author Contribution

All authors contributed equally to this work.

Funding

This research has no funding source.

Data Availability

In this study, publicly available datasets were analyzed. These data can be found here: NSL-KDD (kaggle.com).

Conflicts of Interest

The authors declare that there is no conflict of interest in the research.

Ethical Approval

This article does not contain any studies with human participants or animals performed by any of the authors.

References

[1] Bakro, M., et al. Performance analysis of cloud computing encryption algorithms. in Advances in Intelligent Computing and Communication: Proceedings of ICAC 2020. 2021. Springer.

[2] Silivery, A.K., et al., A model for multi-attack classification to improve intrusion detection performance using deep learning approaches. Measurement: Sensors, 2023. 30: p. 100924.

[3] Bakro, M., et al., Hybrid blockchain-enabled security in cloud storage infrastructure using ECC and AES algorithms, in Blockchain based Internet of Things. 2022, Springer. p. 139-170.

[4] Saranya, T., et al., Performance analysis of machine learning algorithms in intrusion detection system: A review. Procedia Computer Science, 2020. 171: p. 1251-1260.

[5] Alkhatib, N., H. Ghauch, and J.-L. Danger. SOME/IP intrusion detection using deep learning-based sequential models in automotive ethernet networks. in 2021 IEEE 12th annual information technology, electronics and mobile communication conference (IEMCON). 2021. IEEE.

[6] Tao, P., Z. Sun, and Z. Sun, An Improved Intrusion Detection Algorithm Based on GA and SVM. IEEE Access, 2018. 6: p. 13624-13631.

[7] Gadze, J.D., et al., An Investigation into the Application of Deep Learning in the Detection and Mitigation of DDOS Attack on SDN Controllers. Technologies, 2021. 9(1): p. 14.

[8] Tang, C., N. Luktarhan, and Y. Zhao, SAAE-DNN: Deep Learning Method on Intrusion Detection. Symmetry, 2020. 12(10): p. 1695.

[9] Stiawan, D., et al., CICIDS-2017 dataset feature analysis with information gain for anomaly detection. IEEE Access, 2020. 8: p. 132911-132921.

[10] Nimbalkar, P. and D. Kshirsagar, Feature selection for intrusion detection system in Internet-of-Things (IoT). ICT Express, 2021. 7(2): p. 177-181.

[11] Saleh, A.I., F.M. Talaat, and L.M. Labib, A hybrid intrusion detection system (HIDS) based on prioritized k-nearest neighbors and optimized SVM classifiers. Artificial Intelligence Review, 2019. 51: p. 403-443.

[12] Hnamte, V. and J. Hussain, Dependable intrusion detection system using deep convolutional neural network: A Novel framework and performance evaluation approach. Telematics and Informatics Reports, 2023. 11: p. 100077.

[13] Nandanwar, H. and R. Katarya, Deep learning enabled intrusion detection system for Industrial IOT environment. Expert Systems with Applications, 2024. 249: p. 123808.

[14] Sadia, H., et al., Intrusion Detection System for Wireless Sensor Networks: A Machine Learning based Approach. IEEE Access, 2024: p. 1-1.

[15] El-Ghamry, A., A. Darwish, and A.E. Hassanien, An optimized CNN-based intrusion detection system for reducing risks in smart farming. Internet of Things, 2023. 22: p. 100709.

[16] Sreelatha, G., A.V. Babu, and D. Midhunchakkaravarthy, Improved security in cloud using sandpiper and extended equilibrium deep transfer learning based intrusion detection. Cluster computing, 2022. 25(5): p. 3129-3144.

[17] Tavallaee, M., et al. A detailed analysis of the NSL KDD CUP 99 data set. in 2009 IEEE symposium on computational intelligence for security and defense applications. 2009. Ieee.

[18] Krizhevsky, A., I. Sutskever, and G.E. Hinton, ImageNet classification with deep convolutional neural networks. Communications of the ACM, 2017. 60(6): p. 84-90.
[19] Maheri, M., et al., Machine learning to assess CO2 adsorption by biomass waste. Journal of CO2 Utilization, 2023. 76: p. 102590.
[20] Belavagi, M.C. and B. Muniyal, Performance evaluation of supervised machine learning algorithms for intrusion detection. Procedia Computer Science, 2016. 89: p. 117-123.
[21] Han, J., J. Pei, and H. Tong, Data mining: concepts and techniques. 2022: Morgan kaufmann.
[22] Kingma, D.P. and J. Ba, Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980, 2014.
[23] Abadi, M., et al. {TensorFlow}: a system for {Large-Scale} machine learning. in 12th USENIX symposium on operating systems design and implementation (OSDI 16). 2016.
[24] Chollet, F., Deep learning mit python und keras: das praxis-handbuch vom entwickler der keras-bibliothek. 2018: MITP-Verlags GmbH & Co. KG.

Disclaimer/Publisher's Note: The perspectives, opinions, and data shared in all publications are the sole responsibility of the individual authors and contributors, and do not necessarily reflect the views of Sciences Force or the editorial team. Sciences Force and the editorial team disclaim any liability for potential harm to individuals or property resulting from the ideas, methods, instructions, or products referenced in the content.