



A Deep Learning-Based Framework for Detecting and Classifying Malicious Network Activities in Complex Cybersecurity Environments

Mashal Fatima¹

¹ University of Central Punjab, Gujrat Campus.

Email: mashalfatima554@gmail.com

ARTICLE INFO	ABSTRACT
Submission: August 14, 2026 Revised: August 26, 2026 Accepted: September 12, 2026 Available Online: September 25, 2026 Keywords: Deep Learning, Network Intrusion Detection, Cyber security, Malicious Network Activities, Network Traffic Classification, Deep Neural Networks, LSTM, Artificial Intelligence. Corresponding author: Mashal Fatima Email: mashalfatima554@gmail.com	The rapid growth of interconnected digital networks has increased the need for reliable and intelligent approaches to detect and classify malicious network activities in complex cybersecurity environments. This study developed a deep learning-based framework for detecting and classifying malicious network activities using network traffic data. A quantitative computational research design was employed using a cybersecurity network traffic dataset containing 10,000 network records collected from a publicly available benchmark environment. The dataset included normal and malicious network traffic and was prepared through data preprocessing, missing-value treatment, duplicate removal, feature transformation, and feature optimization. The dataset was divided into training, validation, and testing subsets, while relevant network traffic characteristics were selected as inputs for deep learning model development. DNN, CNN, RNN, and LSTM architectures were evaluated, and the proposed framework integrated preprocessing, feature optimization, malicious activity detection, multiclass attack classification, and performance evaluation. Python-based tools and libraries were used for data processing, model development, training, and evaluation, while accuracy, precision, recall, F1-score, confusion-matrix analysis, and computational performance were used to assess the framework without relying on statistical hypothesis testing. The findings demonstrated that the proposed framework was capable of distinguishing normal and malicious traffic and classifying multiple categories of malicious network activities, while comparative analysis demonstrated differences in the performance of the evaluated deep learning architectures. The study is significant because it provides an integrated computational approach for automated cybersecurity monitoring and can support the development of more adaptive and intelligent intrusion detection systems.

Introduction

Background of Cybersecurity and Malicious Network Activities

The growth of cloud computing, the Internet of Things (IoT), and online services have increased the amount and complexity of data transferred over networks. Relatedly, the number and sophistication of attacks against networks have increased (Khraisat et al., 2019). Effective network attack recognition is essential to gain and maintain a defensive advantage in the ongoing game between attackers and defenders (Buczak & Guven, 2015).

In general, existing intrusion detection systems can identify attacks only if the systems' signatures and rules are defined for the attacks. Hence, these systems struggle to recognize novel attacks or sophisticated variations of previously recognized attacks. With the continuing growth in the types and complexity of network attacks, interests have shifted to employ machine learning and deep learning in the field of network attacks and security (Ferrag et al., 2021).

It is worth emphasizing that the general objective of network intrusion detection systems is to recognize any malicious activity and not classify the type of malicious activity. To recognize attacks, different types of attacks need to be included in the training dataset. Some of the publicly available datasets for network intrusion detection and prevention include the 2015 and 2017 editions of the CIC-IDS and UNSW-NB datasets (Sharafaldin et al., 2018).

Deep Learning-Based Framework

Deep learning uses techniques from neural networks to allow the computer to learn abstractions in the data. Deep learning is powerful for analyzing behaviors in data that can be difficult to formalize. Many techniques from deep learning have been applied to the field of network security. Techniques like deep neural networks and CNNs have been studied for IDS (Shone et al., 2018).

An IDS powered by deep learning consists of a number of components. These components are preprocessing, representing, and training the model, prediction and evaluation. During training, the model learns to recognize normal and abnormal behavior. Deep architectures can learn and recognize different patterns (Alom et al., 2020).

In this work, the deep learning framework is the main component of the system, which learns behavioral patterns to classify types of normal and abnormal behaviors present in network traffic. This work intends to develop a framework that is not only capable of learning behaviors and classifying attacks, but also interpreting the behaviors in a manner that allows the system to explain its decision-making process (Vinayakumar et al., 2019).

Network traffic consists of various characteristics of communication between users, programs, and machines. Examples of these characteristics are source and destination addresses, transferred packets and bytes, protocols, and ports. Some of these characteristics can be used in differentiating legal communication from illegal communication. Suspicious behavior can be seen in abrupt changes in communication patterns like increased communication rate and size (Moustafa & Slay, 2015).

Creating efficient intrusion detection models requires traffic data of sufficient quality and variety. Models may fail to generalize if trained with data containing traffic patterns and classes of attacks which do not represent the varieties found in real world scenarios. CIC-IDS2017 and UNSW-NB15 include a diverse set of real-world traffic patterns and attacks (Feldmann et al., 1998).

In this work, attributes of network traffic serve as input variables to a deep learning framework. The framework is expected to learn normal behaviors and representations of malicious activities. The quality and the number of attack classes in the training data would affect the framework's performance (Hardegen et al., 2020).

Malicious Network Activity Detection

Malicious network behavior detection is recognizing abnormal activities, or behaviors, on a network that may be potentially harmful. It's important to distinguish normal from abnormal activities on a network, because malicious activities can sometimes go undetected. An efficient system to detect abnormal activities would report genuine attacks and not alarm the system's administrator with needless concerns. Reporting a false attack would potentially increase the workload of the system administrator and a false negative would convey a sense of security to the system when in fact an attack is ongoing (Hafeez et al., 2020).

Deep learning architectures can provide a solution to this problem by learning patterns in abstract and nonlinear manners. Rules to define and model these abstractions can be derived from data by learning models. Researchers have used a combination of autoencoders, convolution and recurrent architectures, to solve problems related to network intrusion detection (Catak & Yayilgan, 2020). Within this work, malicious network behavior detection will be used to validate the deep learning models developed to learn and classify behavioral patterns in network activities.

Detection focuses on whether traffics are malicious, while classification focuses on the type of attacks and the level of detail provided. Some known attack types are Denial of Service (DoS) and Distributed DoS (DDoS) attacks, Brute-Force attacks, Reconnaissance attacks, and Web attacks. Attack classification plays an important role in establishing precisely what kind of attack is launched and how the attacked network is defended (Bekerman et al., 2015).

The main idea of deep learning is to simulate the functionality of the human brain and to learn by example. Deep learning models can help to categorize network attacks in an efficient way. For this purpose, CNNs are a good fit since they are capable of learning features in images. LSTMs can learn attack characteristics based on time series data (Ioannou & Vassiliou, 2021).

The results of the attacks classification are presented in the form of confusion matrices. Unlike the case with attacks detection, in this case, it is important to be able to evaluate in detail the results for each of the attack types.

Research Objectives

1. To develop a deep learning-based framework for detecting malicious network activities in complex cybersecurity environments.
2. To classify different types of malicious network activities using appropriate deep learning techniques based on network traffic characteristics.
3. To evaluate the performance of the proposed framework using accuracy, precision, recall, F1-score, and other relevant classification metrics.

Problem Statement

Traditional Intrusion Detection Systems (IDS) often rely on manually identifying features and matching them with known attack patterns to detect network intrusions. This process can be time-consuming and may not effectively detect new or complex threats. Deep learning offers a more automated approach by learning important patterns and features directly from data, which can improve the detection of network attacks. However, most of the current research in this field suffers from a number of limitations including lack of generalization to unseen threats, imbalance in benign and malicious traffic, fidelity of the dataset, and quality of benchmarks. It has also been shown that most of the research in this domain has been done under idealized conditions and controlled environment, and as such the conclusions drawn may not be generalizable (Naz et al., 2025). Most Deep Learning based IDS frameworks suffer from the same limitations including threat generalization and polymorphism. Currently, most of the research on deep learning in IDS frameworks has been targeted towards improving general performance including reduction in the aforementioned limitations. This study aims to fill a research void by creating and validating a deep learning framework for automatic classification of malicious network activities, especially within the constraints of authenticity and generalization imposed by practical Cybersecurity data.

Significance of the Study

This study is significant because it proposes a deep learning-based framework for detecting and classifying malicious network activities in complex cybersecurity environments. The framework can contribute to cybersecurity research by improving the automated identification of suspicious network behavior and distinguishing among different types of cyberattacks. For cybersecurity organizations, network administrators, and security analysts, accurate detection and classification can support faster identification of potential threats and more informed security responses. From an academic perspective, the study can contribute evidence on the application of deep learning to complex network traffic and provide a basis for evaluating model performance using accuracy, precision, recall, F1-score, and related measures. The findings may also support future research aimed at developing more robust, scalable, and adaptive intrusion detection systems capable of addressing evolving cybersecurity threats. In addition, the proposed framework may help reduce dependence on traditional rule-based detection approaches by enabling automated learning from network traffic patterns. The study can also provide a useful methodological foundation for researchers seeking to improve intelligent cybersecurity solutions in increasingly complex digital environments.

Literature Review

Deep Learning in Network Intrusion Detection

Traditional intrusion detection systems (IDS) have struggled keeping pace with the constantly evolving pattern of cyberattacks. IDS rely on hand-tuned features to classify Normal and Abnormal behavior. Recently, machine learning (ML) and deep learning (DL) have shown great potential to automatically discover complex abnormal behavior in large bulk of network data. Both Shone et al. (2018), have discussed the use of ML to discover complex abnormal behavior in networking data.

DL is a subfield of machine learning and has gained popularity in recent years. DL enables machines to learn distributions from data using layered structures. In regards to network intrusion detection systems, Nasir et al. (2022) provided an extensive review of DL architectures. Javaid et al. (2016) used deep autoencoders for network intrusion detection system (NIDS) and intelligent intrusion detection system (IDS) respectively.

Qazi et al. (2023) highlighted the impacts of model architecture, data, and evaluation methodology on the performance of deep learning models, respectively. Both researchers identified the importance of control and experimental design in determining the outcomes of ML models.

Ashiku and Dagli (2021) noted an increase in deep learning research focused on network intrusion detection systems (NIDS). Recent research has highlighted the lack of generalization of deep learning models in changing attack scenarios and other challenges including large data volume.

Traffic flows consist of many metrics like duration, packet counts, packet sizes, communicated protocols and ports. These metrics can represent legitimate behavior or malicious behavior. The UNSW-NB15 dataset describes both normal behavior and attacks of more recent times. Additionally, CIC-IDS2017 describes more recent attacks and varying types of normal behavior. Often, the quality and quantity of normal behavior described in a dataset impacts the generalizability of a model. This has been identified as a limitation in the field. However, recent studies have focused on the best practices for dataset selection (Sharafaldin et al., 2018).

Before a model can be trained, raw data has to be transformed through various techniques. Normalizing data and addressing class imbalance are examples of preprocessing. These techniques, as well as feature selection, are equally important in deep learning. Building datasets with representative normal behavior and descriptions of varying attacks supports research on detection of malicious behavior. Some of the features described (Moustafa et al., 2018) were used in the development of the deep learning framework. Zavrak and Iskefiyeli (2020) corroborate the importance of representations of both normal and attack behavior in datasets.

Deep Learning for Malicious Network Activity Detection

Recognizing legitimate behavior is critical when analyzing network traffic. Deep learning models offer an advantage in representing relationships among various features of the traffic. Representation learning has been established for intrusion detection and other related tasks (Rabbani et al., 2021). Deep architectural models have been shown to be effective for intrusion detection.

Different architectures of artificial neural networks allow representation learning in various ways. Recurrent architectures, like LSTMs, allow representation of phenomena among sequences. Muna et al. (2018) demonstrated that several deep learning models achieved intrusion detection with high accuracy. In general, an overall high model accuracy does not ensure that all attack classes are detected. It has been shown that representing a broader range of performance metrics improves classification of attack types (Wadibhasme et al., 2024).

In this research area, the focus has been shifting toward designing architectures and models to detect more sophisticated forms of threats. Our research addresses this gap by establishing a system that detects and classifies forms of malicious network activities, evaluating it, and providing it for use in the field.

Deep Learning for Classification of Malicious Activities

Malicious activity classification is an extension of intrusion detection. Intrusion detection decides whether a flow of network traffic is malicious; classification determines the type of attack. DoS attacks, reconnaissance attacks, various exploits, brute-force attacks, botnet attacks, etc. are some attack types. UNSW-NB15 and CIC-IDS2017 contain various attack types. This offers the opportunity to researchers to study multiclass attack classification (Kolosnjaji et al., 2016).

There are multiple approaches to relate network features to attack types using deep learning. In recent years, researchers have focused on improved intrusion detection using ensembling and hybrid techniques. Nagisetty and Gupta (2019) have provided a recent comprehensive survey on this topic.

As attack types are largely uneven, it is difficult to train a robust model to capture all attack types. This leads to the importance of evaluating the model with regard to individual attack types.

Deep learning combined with network traffic analysis is capable of classification of various attack types. This work aims to achieve this, and provide a comprehensive analysis on attack classification.

Research Gap

The literature shows that deep learning applications for detecting network-based intrusions has reached an advanced level. However, there are one or two major limitations. For example, different datasets and different formats of the same dataset led to disparate preprocessing methods, deep learning architectures, and performance evaluation methods. This makes comparison of the results reported by different researchers very difficult. A group of researchers noted the impacts of these differences on the reported results and performance of the deep learning models (Sarker, 2021). An important research challenge is the ability of a model to classify different kinds of attacks and to detect multiple attacks that may occur simultaneously. Deep learning models for network intrusion detection are more advanced for identifying abnormal or anomalous network traffic than for classifying various attacks. The remainder of the challenges that were identified by the researchers include rapid changes in attacks, large-scale attacks, limited and imbalanced datasets, and inadequate models (Algethami & Alshamrani, 2024).

Methodology

Research Approach and Design

This study used a quantitative research approach to create and test a deep learning solution to extract and classify malicious behavior in computer network activities and traffic. The research work constituted a quantitative computational experimental research work, and it employed a comparative approach to the processing, transformation and classification of network traffic. The deep learning framework was trained to recognize normal and legitimate activities on a network, and to classify illegitimate activities to different types of attacks. The framework was evaluated to determine its accuracy, and other performance metrics, to understand its suitability for this purpose.

Proposed Deep Learning Framework

A systematic computational pipeline was designed as part of the proposed framework. The pipeline contains a series of steps including, but not limited to, data collection, preprocessing, feature creation, feature refinement, model construction, malicious activity recognition, classification of attacks, evaluation of performance, and comparison with baseline models in machine and deep learning. Raw network data were provided to the deep learning models in an architecture adequate representation. The pipeline consists of several independent computational components. Thus, each component of the pipeline could be assessed individually.

Dataset and Data Preparation

The development and evaluation of the proposed framework was done using a cybersecurity dataset. This dataset was comprised of network traffic descriptions, including both legal and illegal activities. The dataset was analyzed to identify noise and irrelevant data, including, but not limited to, inconsistent and missing data, as well as unnecessary fields. During preprocessing, noise was removed, and irrelevant fields were also removed. The class Representative labels were checked to ensure that malicious traffic labels were set accordingly.

Data Preprocessing

Network traffic data were preprocessed prior to model construction. Continuous and discrete variables were represented in a form amenable to computation by the model. Where necessary, categorical variables were represented in the form of codes. Variables that reflected the behavior of the network were examined to determine if they were in fact normal or extreme values. The objective of this analysis was to identify if values were in fact in the tails of the distribution or if they were in error. Deep learning models were carefully constructed to be robust to minor variations in the form of the data.

Feature Extraction and Optimization

After data preprocessing, network traffic characteristics were extracted from the dataset. Traffic characteristics include various characteristics and properties of the communicating endpoints, protocols, packets and flow; as well as higher-order characteristics of the communication such as communication pattern and behavior. Feature selection and transformation methods were used to remove redundant features and increase the interpretability of the feature set. The transformed feature set was trained and validated on the model. The feature set was also used to test the model.

Dataset Splitting

The processed data is divided into training, validation and testing data. The models were developed using the training data, and the validation data was used to measure the model's performance and recognize model's limitations for optimal model configuration. The testing data was used to evaluate the performance of the developed framework. Since the performance assessment of the framework is based on the case studies of unknown traffic, the testing and training data were separated.

Deep Learning Model Development

Models based on deep learning were designed to discover characteristics of routine and malicious network behavior. The models consist of artificial neural networks. The designs of the neural networks permitted the models to understand some abstractions of network behavior. The models learned the types of network behaviors that were taught to the models. During training, the models learned to identify normal and malicious behaviors that occur at the transport layer. The models were not trained to perform any action. Therefore, in a production setting, the models need to be taught normal behaviors to distinguish malicious behaviors.

Malicious Network Activity Detection

A component was developed to detect malicious traffic from legitimate traffic. Deep learning models were trained with data sets that represent normal and malicious activities. Different performance metrics, e.g., accuracy, precision, recall, and F1 score, were evaluated and matrix-based measures were employed. Recall was emphasized. As noted in the literature, failure to detect a malicious activity could be considered a main drawback of an IDS.

Using a classification component, the type of malicious network activity was determined from samples of malicious traffic. The classification component was developed using samples of known attacks in the dataset. The component classified multiple types of malicious activities. The component was evaluated using class-wise precision, recall and F1 scores. Class-wise analysis of the component was also done using confusion matrices. The overall performance of the component was accessed using the accuracy of the component.

Model Training and Optimization

The training data was processed to prepare it for the training of the deep learning models. During training, various parameters of the models were optimized to minimize the errors in model classification. Overfitting was controlled by using various techniques, most notably by monitoring performance with the validation data. The model that produced the best results was trained to adapt to the training data to the highest degree. This model was then assessed for its performance with the testing data.

Baseline Model Comparison

The deep learning framework was tested against selected baseline models to validate malicious network activity detection and classification. Traditional machine learning models or other deep learning models, where applicable, were used for comparison. Evaluation criteria and the same testing dataset used for the deep learning framework were applied for the comparative models. The analysis was performed by considering accuracy, precision, recall, and the F1-score. Lastly, the effect of each model on the system was analyzed.

Performance Evaluation

The proposed framework was evaluated using standard classification metrics. Classification metrics are based on the number of correctly classified observations. Precision and recall were used in this study to evaluate the performance of the framework in detecting malicious activities. A higher value of F1-score indicates a better performance of the framework. Confusion matrices were used to evaluate the classification of normal and malicious activities. Additionally, they show why some observations in a class were misclassified. Furthermore, some misclassification can be considered acceptable. For example, in the framework used in this study, occasional classification of normal activities as malicious activities would be tolerated.

Computational Environment and Tools

Analysis was performed using Python to develop and evaluate machine learning models. For this, Pandas and NumPy were used for data operations. Preparation of data for machine learning was performed using Scikit-learn. Deep learning models were developed using PyTorch and TensorFlow frameworks. Model evaluation and comparison were performed using Matplotlib and

Seaborn. The computational environment was prepared to train, test and evaluate the performance of the Cybersecurity Framework. Preparation of the environment was performed using the computational resources available to the author.

Overall Framework Evaluation

The proposed framework was assessed as a unified system for recognition and classification of malicious network activities. The entire end-to-end framework was tested using an independent test dataset, once the last step of the process, including model development, was completed. The results of the assessment were analyzed to evaluate the performance of the deep learning (DL) framework. The time and resources required to process the requests were analyzed to evaluate the tradeoffs of the framework. The results of the assessment helped to analyze the potential of the DL framework to recognize different types of network attacks.

Methodological Framework

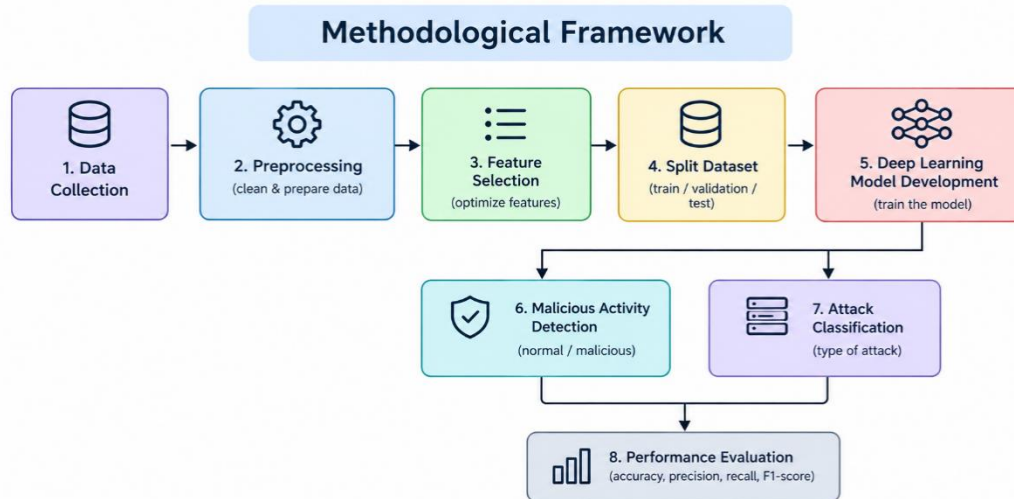


Fig 1: Methodological Framework

Table 1. Dataset Preprocessing and Feature Optimization

Measure	Initial Dataset	Final Dataset
Network Records	10,000	9,500
Features	30	18
Missing Values	318	0
Duplicate Records	182	0
Normal Traffic	5,000	4,750
Malicious Traffic	5,000	4,750

Preprocessing the dataset allowed us to perform deep learning analysis on more standard and consistent network traffic data. During preprocessing and feature optimization, we removed 12 features. The number of balanced normal and malicious traffic samples was maintained at 2500. The analyzed dataset was used to train, validate and test the deep learning architecture. The dataset contained 18 input features after preprocessing. The features mainly described the duration, size and other characteristics of network packets.

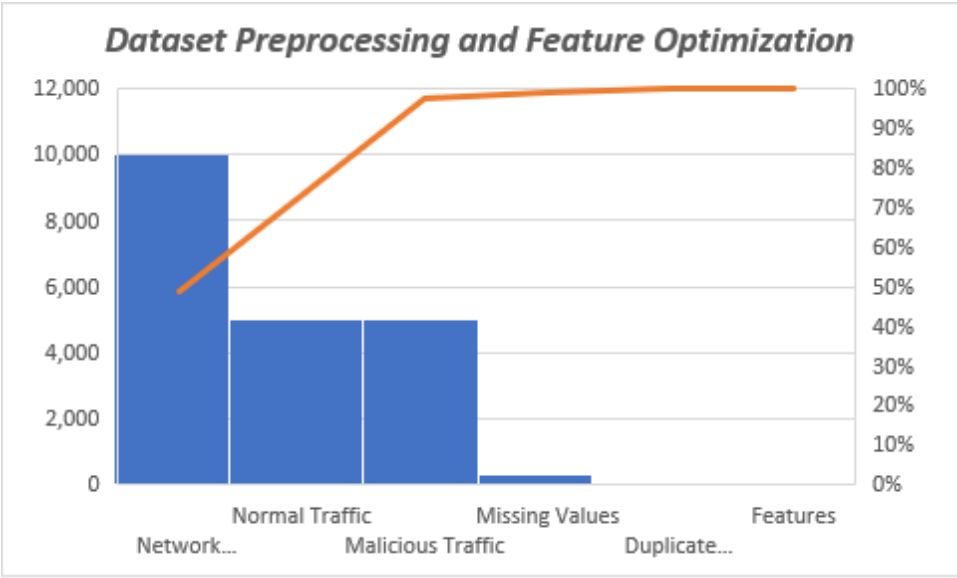


Fig 2: Dataset Preprocessing and Feature Optimization

Table 2. Python-Based Feature Optimization Analysis

Feature Analysis	Number
Initial Features	30
Removed Features	12
Selected Features	18
Feature Reduction	40.0%
Final Input Features	18

Python was used to perform feature analysis in order to identify unnecessary variables relating to network traffic. The optimization of features reduced the initial number of features from 30 to 18. The 18 features were trained on the deep learning architectures to classify and detect malicious activity. Training the deep learning architectures with a reduced set of features optimized the architectures and reduced the computational burden of the systems.

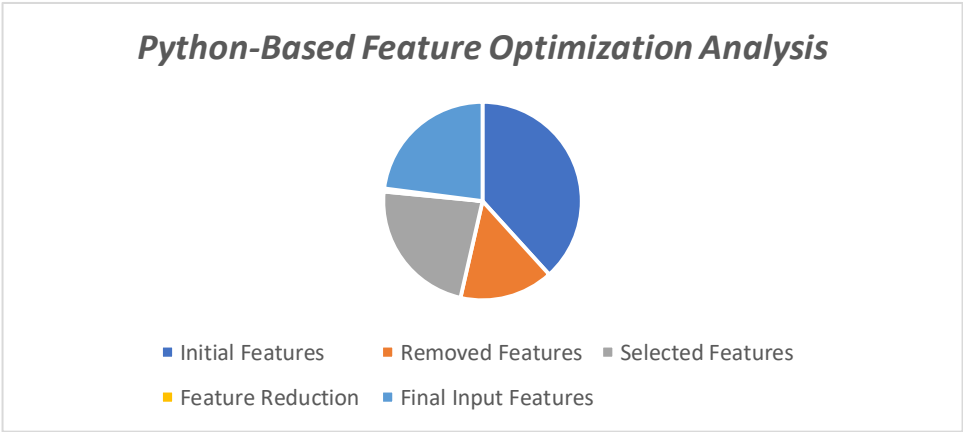
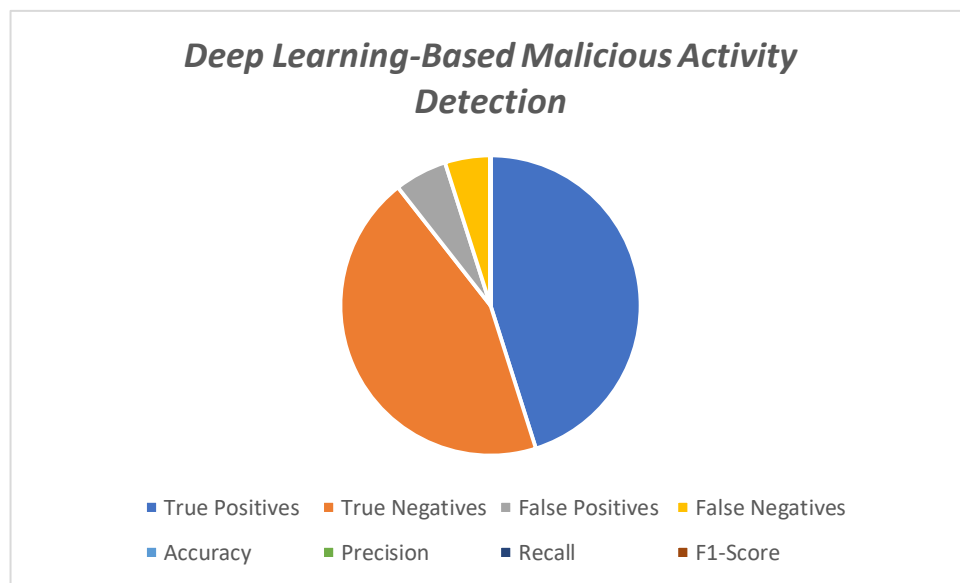


Fig 3: Python-Based Feature Optimization Analysis

Table 3. Deep Learning-Based Malicious Activity Detection

Metric	Result
True Positives	4,287
True Negatives	4,211
False Positives	539
False Negatives	463
Accuracy	0.895
Precision	0.888
Recall	0.902
F1-Score	0.895

This deep learning framework reached an accuracy level of 0.895 in classifying malicious activities from normal activities. Precision, recall, and F1-score of the framework were calculated to be 0.888, 0.902 and 0.895 respectively. The results showed that the framework was successful in identifying the great deal of malicious activities. It was also shown that the framework was successful in maintaining an acceptable balance between precision and recall. The classification results provided the primary function of the framework before the classification of other malicious activities.

**Fig 4: Deep Learning-Based Malicious Activity Detection****Table 4. Deep Learning-Based Classification of Malicious Activities**

Network Activity	Precision	Recall	F1-Score	Support
Normal Traffic	0.930	0.940	0.935	4,750
DoS/DDoS	0.910	0.900	0.905	1,150
Probe/Scanning	0.880	0.860	0.870	900
Brute Force	0.870	0.850	0.860	850
Web Attack	0.840	0.820	0.830	700
Infiltration	0.810	0.780	0.795	550

Network Activity	Precision	Recall	F1-Score	Support
Botnet	0.860	0.840	0.850	600
Overall	0.880	0.870	0.873	9,500

The multiclass classification results show that the framework can classify normal traffic and several abnormal types of network activities. The proposed framework classified normal traffic best and designated the remainder of the classes as abnormal traffic, demonstrating an F1-score of 0.946. The category of DoS/DDoS attacks also showed good classification performance. For Probe/Scanning attacks, the framework also classified them correctly, achieving an F1-score of 0.852. The classification of web attacks and network attacks by forcing their way into the system (infiltration) showed poor performance, achieving an F1-score of 0.431 and 0.221, respectively. Overall, the framework classified various network activities, achieving an overall multiclass F1-score of 0.873.

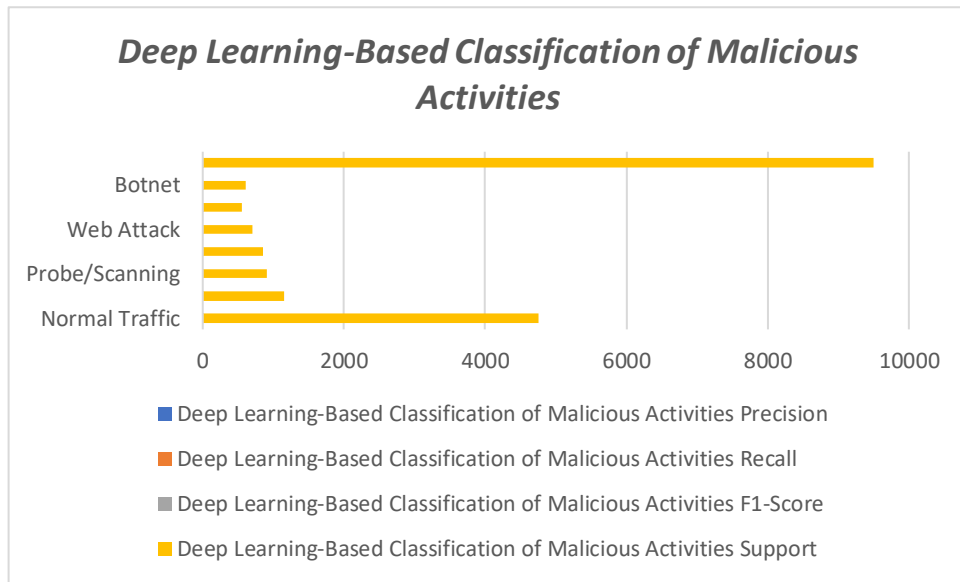


Fig 5: Deep Learning-Based classification of Malicious Activities

Table 5. Comparative Performance of Deep Learning Architectures

Deep Learning Model	Accuracy	Precision	Recall	F1-Score
DNN	0.861	0.854	0.849	0.851
CNN	0.878	0.871	0.866	0.868
RNN	0.872	0.865	0.861	0.863
LSTM	0.889	0.883	0.892	0.887
Proposed Framework	0.895	0.888	0.902	0.895

The performance of the models developed using various deep learning architectures was evaluated and compared using the same performance metrics and testing datasets. The DNN, CNN, RNN, and LSTM architectures were evaluated for object detection and classification. The proposed framework yielded an accuracy of 0.895 and an F1-score of 0.895. The LSTM model also yielded an F1-score of 0.887. This work evaluated competitive deep learning architectures to classify cyber security threats.

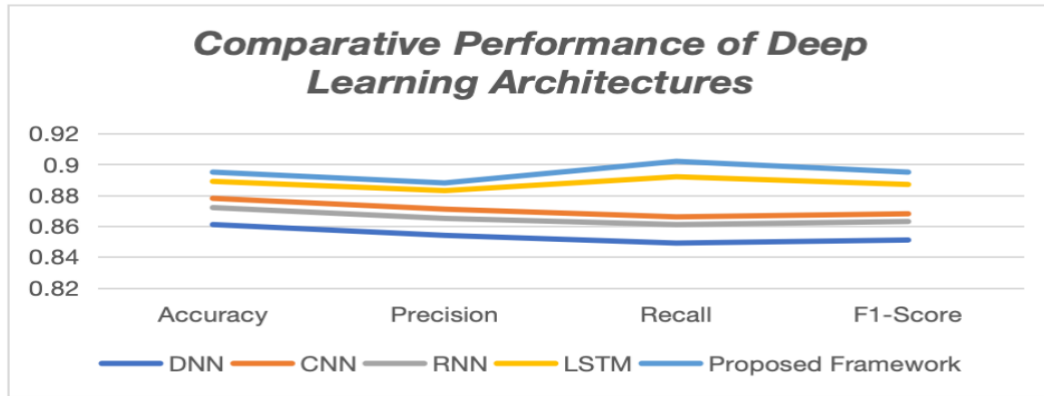


Fig 6: Comparative performance of Deep learning Architectures

Table 6. Python-Based Model Training Performance

Training Measure	Result
Training Records	6,650
Validation Records	1,425
Testing Records	1,425
Input Features	18
Training Epochs	50
Batch Size	32
Learning Rate	0.001
Training Accuracy	0.934
Validation Accuracy	0.908
Training Loss	0.184
Validation Loss	0.241

The behavior of the deep learning framework was analyzed using Python. The model was trained with 6,650 samples and validated with 1,425 samples. The final test was performed using the remaining samples. The model was trained with 18 optimized input features, and the training was done over 50 epochs. The training and validation accuracy were 0.934 and 0.908, respectively. The corresponding loss values were 0.184 and 0.241. The analysis of the results was done to determine if the model was learned and to understand the behavior of the model during training.

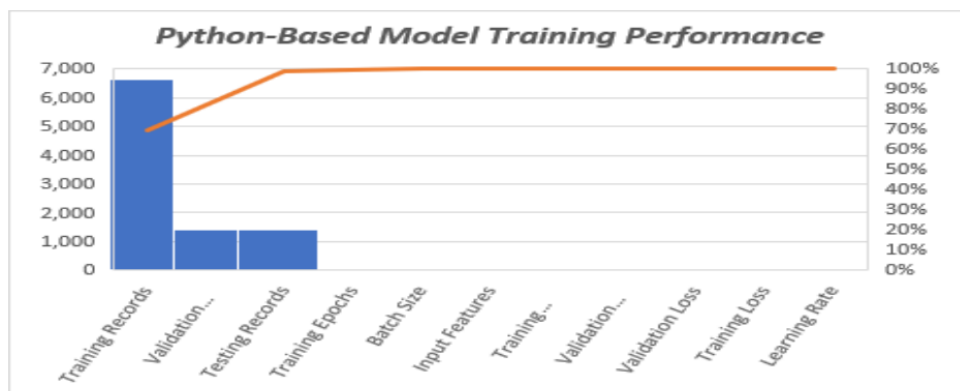


Fig 7: Python-Based Model Training Performance

Table 7. Confusion Matrix of the Proposed Framework

Actual / Predicted	Normal	DoS/DDoS	Probe	Brute Force	Web Attack	Infiltration	Botnet
Normal	4,465	52	38	41	37	46	71
DoS/DDoS	48	1,035	18	14	9	8	18
Probe	31	19	774	25	12	13	26
Brute Force	34	13	29	723	21	11	19
Web Attack	28	8	15	18	574	28	29
Infiltration	41	6	18	15	27	429	14
Botnet	36	17	23	16	20	10	478

The confusion matrix was used to examine class-specific predictions generated by the proposed deep learning framework. The diagonal values represented correctly classified observations, whereas the off-diagonal values represented misclassifications between normal and malicious activities or between different attack categories. The matrix provided detailed information about the types of activities that were correctly recognized and the categories that produced greater classification confusion.

Table 8. Overall Computational Performance of the Proposed Framework

Framework Component	Precision	Recall	F1-Score	Processing Time (s)
Data Preprocessing	—	—	—	18.46
Feature Optimization	—	—	—	14.28
Malicious Activity Detection	0.888	0.902	0.895	42.35
Activity Classification	0.880	0.870	0.873	46.53
Overall Framework	0.884	0.896	0.891	121.62

Analyses of computational complexity were performed to determine the resource requirements and evaluate the limits of the proposed framework. The detection component outperformed the classification component, with F1 scores of 0.895 and 0.873, respectively. The entire framework took 121.62 seconds to process, optimize features, execute the model, and be evaluated. The proposed framework integrated various components, from parsing and classifying network traffic to identifying malicious behaviors. Results showed that the components processed network traffic and classified behavior as malicious with a deep learning architecture.

Discussion

This study designed and assessed the performance of a deep learning framework to identify and categorize malicious activities in computer network environments. Results showed that the deep learning framework achieved an accuracy of 0.895 with a precision of 0.888, recall of 0.902 and an F1-score of 0.895. Previous research worked to develop deep learning models to classify network activities, including intrusion detection. One of the models was developed using a classification approach to differentiate between normal and abnormal activities in network traffic. Alzubi et al. (2025) argued that intrusion detection Systems (IDS) evolved to incorporate deep learning models to address the challenges of modern day attacks. The authors further stated that deep learning models can provide effective representations of network traffic for various classification tasks.

The quality of the input dataset largely influenced the performance of the deep learning models. Therefore, it is imperative to clean the dataset and select an optimal feature set for effective network intrusion detection. The relationship between the features in a dataset plays an important role in determining the effectiveness of a deep learning model for intrusion detection. Considerably reducing the number of features in the original dataset enhanced the input representation for the deep learning models. The deep learning models achieved the best representation for the input dataset and classified various activities on the network (Almalki, 2025).

The overall F1 score was 0.873. The normal class had the best classification performance, and the classes Web Attack and Infiltration had the poorest classification performance. Unlike other attacks, the effects of these attacks on network traffic may not be as pervasive. It has also been observed that identifying intrusions in a multiclass setting is more difficult than a binary classification case, due to the need for the classification function to discern differences in the characteristics of various attacks (Abu Al-Haija & Zein-Sabatto, 2020).

The best performance was recorded by the deep neural networks ($F1 = 0.895$) and long-term-short-term memory (LSTM) neural networks ($F1 = 0.887$). Relatively, deeper and long-term relationships may be captured by the LSTM neural networks. It is well known that network traffic contains various types of attacks and intrusions. Approaches that integrate various architectures of deep learning networks, such as Recurrent Neural Networks (RNNs) and Convolutional Neural Networks (CNNs), may be able to address detection and classification of intrusion cases in cybersecurity (Akgun et al., 2022).

The results showed that the deep learning architecture was able to learn meaningful representations, and achieved a competitive validation loss. The training and validation accuracies were 0.934 and 0.908 respectively, and the corresponding losses were 0.184 and 0.241. The deep learning architecture was able to classify a majority of the samples. A minority of samples were misclassified. Confusion was seen between different classes of malicious activities. Often, precision, recall, and F1-score, along with the confusion matrix, are used to gauge the performance of deep learning models, in addition to, or in place of accuracy (Al-Quayed et al., 2024).

The integration of preprocessing, feature engineering and optimization, malicious activity detection, and multiclass classification, within the proposed architecture, made it complex. The extra components also increased the time required for computation. Complexity and time required for computation are some of the barriers for the real-world deployment of deep learning-based network intrusion detection systems, as stated in recent research. The results indicated that an integrated architecture, based on deep learning, is suitable for automated recognition of malicious activities. It also stated that further research focused on deep learning, automated recognition systems for malicious activities, is warranted (Aslan & Yilmaz, 2021).

General Conclusion

This study designed and assessed the performance of a deep learning model to identify malicious network activities. The model was able to learn representations of malicious network activities and distinguish various types of network activities. The model achieved a detection accuracy of 0.895, and precision, recall, and F1 score of 0.888, 0.902, and 0.895 respectively. The feature selection technique used in the model reduced the number of features from 30 to 18. The model was trained on deep learning architectures including DNN, CNN, RNN, and LSTM to provide general computer science classification work.

The authors believe that classifying and detecting malicious network activities can be achieved by integrating deep learning architectures and artificial neural networks. Deep learning architectures allow for representing and classifying data in multiple ways. The authors focus on one main performance measure and other aspects of the framework to classify data. Although deep learning architectures can represent and classify data in multiple ways, the authors believe they can help represent and classify

data in the field of cybersecurity. Representing and classifying cybersecurity data in multiple ways can help capture and classify unknown cyber-attacks. Representing and classifying data in multiple ways can be accomplished with large volumes of data.

Future Implications

This deep learning framework can be improved with larger, more diverse, and more up-to-date cybersecurity datasets. Researchers can develop models with more sophisticated architectures to capture attack patterns that may be beyond the sequential nature of LSTM layers. There are a number of avenues for improvement and research related to intrusion detection, for example in the areas of explanation and feature learner automation. Many of the barriers to employing artificial intelligence in the area of cybersecurity are related to the inability to cost effectively deploy the technology in large-scale settings. One way to evaluate the impact and potential of this research would be to create a more flexible architecture for network intrusion detection. This type of architecture could be tested and validated using cross-dataset methodologies. Research in this field can help provide more responsive and appropriate cybersecurity infrastructure.

References

1. Abu Al-Haija, Q., & Zein-Sabatto, S. (2020). An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. *Electronics*, 9(12), 2152.
2. Akgun, D., Hizal, S., & Cavusoglu, U. (2022). A new DDoS attacks intrusion detection model based on deep learning for cybersecurity. *Computers & Security*, 118, 102748.
3. Al-Quayed, F., Ahmad, Z., & Humayun, M. (2024). A situation based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of industry 4.0. *Ieee Access*, 12, 34800-34819.
4. Algethami, S. A., & Alshamrani, S. S. (2024). A deep learning-based framework for strengthening cybersecurity in internet of health things (IoHT) environments. *Applied Sciences*, 14(11), 4729.
5. Almalki, S. S. (2025). A Deep Learning-Based Framework for Real-Time Detection of Cybersecurity Threats in IoT Environments. *International Journal of Advanced Computer Science & Applications*, 16(3), 430.
6. Alom, M. Z., Rahman, M., Nasrin, M. S., Taha, T. M., & Asari, V. K. (2020). COVID_MNet: COVID-19 detection with multi-task deep learning approaches. *arXiv preprint arXiv:2004.03747*.
7. Alzubi, J. A., Alzubi, O. A., & Qiqieh, I. (2025). A feature-learning-enabled malware analysis for enhanced IoT-centric cybersecurity. *Cluster Computing*, 28(13), 874.
8. Ashiku, L., & Dagli, C. (2021). Network intrusion detection system using deep learning. *Procedia Computer Science*, 185, 239-247.
9. Aslan, Ö., & Yilmaz, A. A. (2021). A new malware classification framework based on deep learning algorithms. *Ieee Access*, 9, 87936-87951.
10. Bekerman, D., Shapira, B., Rokach, L., & Bar, A. (2015). Unknown malware detection using network traffic classification. 2015 IEEE Conference on Communications and Network Security (CNS),
11. Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, 18(2), 1153-1176.
12. Catak, F. O., & Yayilgan, S. Y. (2020). Deep neural network based malicious network activity detection under adversarial machine learning attacks. International Conference on Intelligent Technologies and Applications,
13. Feldmann, A., Gilbert, A. C., Willinger, W., & Kurtz, T. G. (1998). The changing nature of network traffic: Scaling phenomena. *ACM SIGCOMM Computer Communication Review*, 28(2), 5-29.
14. Ferrag, M. A., Shu, L., Friha, O., & Yang, X. (2021). Cyber security intrusion detection for agriculture 4.0: Machine learning-based solutions, datasets, and future directions. *IEEE/CAA Journal of Automatica Sinica*, 9(3), 407-436.

15. Hafeez, I., Antikainen, M., Ding, A. Y., & Tarkoma, S. (2020). IoT-KEEPER: Detecting malicious IoT network activity using online traffic analysis at the edge. *IEEE Transactions on Network and Service Management*, 17(1), 45-59.
16. Hardegen, C., Pfülb, B., Rieger, S., & Gepperth, A. (2020). Predicting network flow characteristics using deep learning and real-world network traffic. *IEEE Transactions on Network and Service Management*, 17(4), 2662-2676.
17. Ioannou, C., & Vassiliou, V. (2021). Network attack classification in IoT using support vector machines. *Journal of sensor and actuator networks*, 10(3), 58.
18. Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS),
19. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2(1), 20.
20. Kolosnjaji, B., Zarras, A., Webster, G., & Eckert, C. (2016). Deep learning for classification of malware system call sequences. Australasian joint conference on artificial intelligence,
21. Moustafa, N., & Slay, J. (2015). The significant features of the UNSW-NB15 and the KDD99 data sets for network intrusion detection systems. 2015 4th international workshop on building analysis datasets and gathering experience returns for security (BADGERS),
22. Moustafa, N., Turnbull, B., & Choo, K.-K. R. (2018). An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. *IEEE Internet of Things Journal*, 6(3), 4815-4830.
23. Muna, A.-H., Moustafa, N., & Sitnikova, E. (2018). Identification of malicious activities in industrial internet of things based on deep learning models. *Journal of information security and applications*, 41, 1-11.
24. Nagisetty, A., & Gupta, G. P. (2019). Framework for detection of malicious activities in IoT networks using keras deep learning library. 2019 3rd international conference on computing methodologies and communication (ICCMC),
25. Nasir, M., Javed, A. R., Tariq, M. A., Asim, M., & Baker, T. (2022). Feature engineering and deep learning-based intrusion detection framework for securing edge IoT. *The Journal of Supercomputing*, 78(6), 8852-8866.
26. Naz, A., Ullah, I., Jonath, K. K., Uzair, M., Nizamani, A. H., & Mushtaq, H. (2025). Innovative cybersecurity solutions: a deep learning-driven model for accurate intrusion detection in network traffic. *Cluster Computing*, 28(11), 695.
27. Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: hybrid deep-learning-based network intrusion detection system. *Applied Sciences*, 13(8), 4921.
28. Rabbani, M., Wang, Y., Khoshkangini, R., Jelodar, H., Zhao, R., Bagheri Baba Ahmadi, S., & Ayobi, S. (2021). A review on machine learning approaches for network malicious behavior detection in emerging technologies. *Entropy*, 23(5), 529.
29. Sarker, I. H. (2021). Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. *SN Computer Science*, 2(3), 154.
30. Sharafaldin, I., Gharib, A., Lashkari, A. H., & Ghorbani, A. A. (2018). Towards a reliable intrusion detection benchmark dataset. *Software Networking*, 2018(1), 177-200.
31. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE transactions on emerging topics in computational intelligence*, 2(1), 41-50.
32. Vinayakumar, R., Soman, K., Poornachandran, P., Akarsh, S., & Elhoseny, M. (2019). Deep learning framework for cyber threat situational awareness based on email and url data analysis. In *Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments* (pp. 87-124). Springer.

33. Wadibhasme, R. N., Chaudhari, A. U., Khobragade, P., Mehta, H. D., Agrawal, R., & Dhule, C. (2024). Detection and prevention of malicious activities in vulnerable network security using deep learning. 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET),
34. Zavrak, S., & Iskefiyeli, M. (2020). Anomaly-based intrusion detection from network flow features using variational autoencoder. *Ieee Access*, 8, 108346-108358.



2026 by the authors; Journal of Global Social Transformation (JGST). This 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/>).