НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
сентябрь–октябрь 2025 Том 25 № 5 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
September–October 2025 Vol. 25 No 5 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

doi: 10.17586/2226-1494-2025-25-5-876-887

Anomaly detection for IIoT: analyzing Edge-IIoTset dataset with varied class distributions

Wafaa Ferhi[1]✉, Djilali Moussaoui[2], Mourad Hadjila[3], Al Baraa Bouidaine[4]

[1,2,3,4] University of Abu Bekr Belkaid, Tlemcen, 13000, Algeria

[1] wafaa.ferhi@univ-tlemcen.dz✉, https://orcid.org/0009-0005-7574-8368
[2] djilali.moussaoui@univ-tlemcen.dz, https://orcid.org/0000-0003-3478-263X
[3] mourad.hadjila@univ-tlemcen.dz https://orcid.org/0000-0002-6554-3925
[4] albaraa.bouidaine@univ-tlemcen.dz, https://orcid.org/0009-0005-2204-9117

Abstract

In the context of the Industrial Internet of Things (IIoT), cybersecurity refers to preventing unauthorized access, attacks, and vulnerabilities to interconnected devices, networks, and data. Given the inherent interconnectedness of IIoT devices, ensuring security is of paramount importance to mitigate potential disruptions, data breaches, and malicious activities. As IIoT systems continue to proliferate, the significance of robust security measures, effective intrusion detection, and intelligent detection techniques escalates to safeguard critical infrastructure and sensitive data from cyber threats. This work aims to contribute towards establishing a secure and resilient industrial environment through the utilization of a hybrid model: Convolutional Neural Network with Deep Neural Network, accommodating distinct class distributions. The recent "Edge IIoTset" dataset is harnessed to enhance the model efficacy. Throughout the evaluation process, diverse metrics are employed, encompassing Accuracy, Precision, Recall, and the F1-score. By applying thorough preprocessing and using various class distribution scenarios (2, 6, 9, 10, and 15 classes), the model achieved excellent classification results. Notably, the 9-class configuration reached an Accuracy of 99.13 %, while the 6-class and 10-class setups also delivered strong performance at 97.13 % and 96.11 %, respectively. Our architecture effectively combines feature extraction and deep classification layers, resulting in a robust solution adaptable to complex IIoT traffic.

Keywords

anomaly, convolutional neural network, deep neural network, Edge IIoTset dataset, Industrial Internet of Things, intelligent detection, metrics, security

For citation: Ferhi W., Moussaoui D., Hadjila M., Bouidaine A.B. Anomaly detection for IIoT: analyzing Edge-IIoTset dataset with varied class distributions. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2025, vol. 25, no. 5, pp. 876–887. doi: 10.17586/2226-1494-2025-25-5-876-887

УДК 004.056.5

Обнаружение аномалий для IIoT: анализ набора данных Edge-IIoTset с различными распределениями классов

Вафаа Ферхи[1]✉, Джилали Муссауи[2], Мурад Хаджила[3], Аль Бараа Буиден[4]

[1,2,3,4] Университет Абу Бекра Белкаида, Тлемсен, 13000, Алжир

[1] wafaa.ferhi@univ-tlemcen.dz✉, https://orcid.org/0009-0005-7574-8368
[2] djilali.moussaoui@univ-tlemcen.dz, https://orcid.org/0000-0003-3478-263X
[3] mourad.hadjila@univ-tlemcen.dz https://orcid.org/0000-0002-6554-3925
[4] albaraa.bouidaine@univ-tlemcen.dz, https://orcid.org/0009-0005-2204-9117

Аннотация

Кибербезопасность промышленного интернета вещей (Industrial Internet of Things, IIoT) означает предотвращение несанкционированного доступа, атак и уязвимостей взаимосвязанных устройств, сетей и данных. Учитывая внутреннюю взаимосвязь устройств IIoT, обеспечение безопасности имеет первостепенное значение для предотвращения потенциальных сбоев, утечек данных и вредоносных действий. По мере распространения

систем IIoT возрастает важность надежных мер безопасности, эффективного обнаружения вторжений и интеллектуальных методов обнаружения для защиты критически важной инфраструктуры и конфиденциальных данных от киберугроз. В данной работе исследованы вопросы создания безопасной и устойчивой промышленной среды посредством использования гибридной модели: сверточной нейронной сети и глубокой нейронной сети, учитывающей различные распределения классов. Для повышения эффективности модели применен набор данных Edge IIoTset. В процессе оценки использованы различные метрики, включая Accuracy, Precision, Recal и F1-меру. Благодаря тщательной предварительной обработке и использованию различных сценариев распределения классов (2, 6, 9, 10 и 15 классов) модель показала хорошие результаты классификации. Конфигурация с 9 классами достигла точности 99,13 %, в то время как конфигурации с 6 и 10 классами — 97,13 % и 96,11 % соответственно. Предложенная архитектура эффективно сочетает уровни извлечения признаков и глубокой классификации, что приводит к созданию надежного решения, адаптируемого к сложному трафику IIoT.

Ключевые слова

аномалия, сверточная нейронная сеть, глубокая нейронная сеть, набор данных Edge IIoTset, промышленный интернет вещей, интеллектуальное обнаружение, метрики, безопасность

Ссылка для цитирования: Ферхи В., Муссауи Д., Хаджила М., Буиден А.Б. Обнаружение аномалий для IIoT: анализ набора данных Edge-IIoTset с различными распределениями классов // Научно-технический вестник информационных технологий, механики и оптики. 2025. Т. 25, № 5. С. 876–887 (на англ. яз.). doi: 10.17586/2226-1494-2025-25-5-876-887

Introduction

The Internet of Things (IoT) is described as the interconnection of multiple devices that use unique identifiers to share data and other pertinent information across a network without the assistance of individuals [1]. Using sensing devices, any physical device can be simply operated, minimizing the need for human labor [2]. IoT applications have been deployed in virtually all fields, ranging from healthcare and agriculture to transportation and manufacturing. These applications have revolutionized and transformed industries by connecting devices, collecting data, and enabling intelligent decision-making processes [3]. Furthermore, as the industrial world progresses towards more advanced and complicated systems, the need for Industrial IoT (IIoT) has emerged. IIoT takes the principles of IoT and applies them specifically to industrial processes, enabling remote monitoring, intelligent analytics, and control of industrial operations. It introduces a higher level of automation, scalability, and efficiency, addressing the unique challenges and requirements of the manufacturing sector. With IIoT, industries can optimize production, improve resource utilization, and enhance overall operational performance [4]. IIoT, when integrated with Cyber-Physical Systems (CPS), brings a transformative shift to industrial operations. CPS is a system that integrates the physical and virtual worlds, fostering connectivity between them [5], which encompass a transformative realm where the physical and cyber worlds intricately interlace, imbuing the operational landscape with heightened intelligence and efficiency [6]. They use sensors and actuators to gather data from the physical world and software to analyze and act on that data, promoting seamless connectivity [7]. The integration of IIoT and CPS enhances connectivity among smart devices [8]. The rapid expansion of IIoT has led to a surge in connected devices, significantly increasing data generation [9]. This presents challenges in data security and anomaly detection, making the confidentiality, integrity, and availability of IIoT data crucial for protecting critical infrastructure [10]. Anomaly detection is essential in identifying security vulnerabilities or inefficiencies [11]. Artificial Intelligence and Deep Learning (DL) enable real-time anomaly detection in data traffic, device behavior, and system performance, allowing proactive threat mitigation [12]. These technologies strengthen cybersecurity defenses against malware, ransomware, and phishing, ensuring data integrity and system security. The main contributions of our research are outlined below:

— introduction of a novel combined DL model, integrating Convolutional Neural Networks (CNN) and Deep Neural Networks (DNN), which demonstrates enhanced performance;
— employing a contemporary dataset known as Edge-IIoTset to facilitate the training and evaluation of the proposed MC-CNN-DNN (Multiclassification CNN-DNN) model. Diverse multiclass distributions are introduced and analyzed;
— the evaluation of our model performance incorporates several metrics, including Accuracy and Precision.

Related work

In recent studies, researchers have presented various approaches to addressing cybersecurity vulnerabilities and breaches in IIoT environments. In [13], authors present a DL-based intrusion detection model combining CNNs for spatial feature extraction and Long Short-Term Memory (LSTM) for temporal feature extraction (Network Intrusion Detection System (NIDS))-CNN-LSTM). Tested on datasets like KDD CUP99, NSL KDD, and UNSW NB15, the model showed robust Accuracy and performance in binary and multi-classification tasks. Similarly, in [14], another group of scientists propose a DL framework leveraging CNNs, Recurrent Neural Networks DNNs, and Generative Adversarial Networks for cyber threat detection in IoT-driven IIoT networks, achieving 95 %–97 % Accuracy on intrusion datasets. The study conducted by [15] examined seven Machine Learning (ML) classifiers on the CICIDS2017 dataset, with K-Nearest Neighbors outperforming others in Precision, Recall, Accuracy, and F1-score. In a related work [16], which uses the same dataset as [15], a combination of ML algorithms and Principal Component Analysis techniques for Distributed Denial of Service (DDoS) detection using the CICIDS2017 and CSE-CIC-IDS 2018 datasets, showing

superior results [17]. In this paper, a novel approach is presented in which the authors develop a DLmodel using DNN and Decision Trees to handle unbalanced ICS datasets, improving attack detection. Another study [18] introduces a Nonsymmetric Deep AutoEncoder for unsupervised feature learning in intrusion detection which is specifically designed for unsupervised feature learning. In [19] the researchers present a groundbreaking anomaly-based intrusion detection model that uses a CNN to build both binary and multi-class classification models [20, 21]. Refer to numerous interesting surveys that deal with ML and DL techniques for Intrusion Detection Systems (IDS). These surveys examine publicly available intrusion datasets used in recent IDS to reveal present-day challenges and future directions. The review published in [22] focuses on several advancements IDS datasets, specifically from CSE-CIC-IDS-2017 to CSE-CIC-IDS-2018. This update includes the addition of new attack categories. The review study discussed in [23] explores and analyses intrusion detection and prevention methods specifically aimed at mitigating DDoS attacks. The study delves into the classification of IDS and explores different anomaly detection approaches. Similarly, and in the same context, the researchers in [24] are using the Difficult Set Sampling Technique (DSSTE) algorithm. The purpose of DSSTE is to improve the learning of unbalanced network data in a classification model by increasing the number of minority samples to be learned. DSSTE aims to address the problem of unbalanced network traffic and improve the classification Accuracy for the minority class. In [25], the researchers will thoroughly analyze and provide solutions to the problems arising from dataset imbalance in both the training and inference phases.

Background Framework of the Study

DNN

DL, a subset of ML, utilizes artificial neural networks to learn complex patterns from data [26]. A neural network consists of an input layer, an output layer, and one or more hidden layers. The perceptron, the fundamental unit of neural networks, processes multiple inputs by applying weights, summing them with a bias term, and passing the result through an activation function [27]. Mathematically, this is expressed as:

$$z = w_1x_1 + w_2x_2 + \cdots + w_nx_n + b,$$

$$\begin{cases} f_1 = w_{11}x_1 + w_{12}x_2 + b_1 \\ f_2 = w_{21}x_1 + w_{22}x_2 + b_2 \\ f_3 = w_{31}x_1 + w_{32}x_2 + b_3 \end{cases},$$

where $x_1, x_2, \ldots x_n$, are inputs; $w_1, w_2, \ldots w_n$, are weights, and b is the bias term. Early DNNs were structured as multilayer perceptrons, where each perceptron computed outputs based on weighted inputs [28, 29]. In the case of three connected perceptrons, such as illustrated in Fig. 1, *a*, the first two perceptrons receive inputs w and x_2, perform calculations based on their respective parameters, and generate outputs y_1 and y_2. These outputs are then passed to the third perceptron, which further performs calculations to produce the final output y_3. Modern DNNs use advanced training techniques like backpropagation (Fig. 1, *b*) which optimizes learning by adjusting weights and biases efficiently.

CNN

In the evolution of neural networks, significant advancements were made with the introduction of multilayer perceptron variants and CNNs. In 1989, the concept of multilayer perceptron models emerged, marking a key milestone in neural network development. However, it was Yann LeCun who revolutionized the field by inventing the first CNNs [29]. LeCun's CNNs were inspired by the organization and functionality of the visual cortex in animals [30]. These networks were specifically designed to learn and process spatial hierarchies of features in an automated and adaptive manner. CNNs are a mathematical framework that typically consists of three fundamental layer types: convolutional layers, pooling layers, and fully connected layers [31]. Convolutional layers extract important features from input data using learnable filters. Pooling layers reduce the spatial dimensions of feature maps through down-sampling, improving computational efficiency and translation invariance. Fully connected layers analyze extracted features to make final predictions,

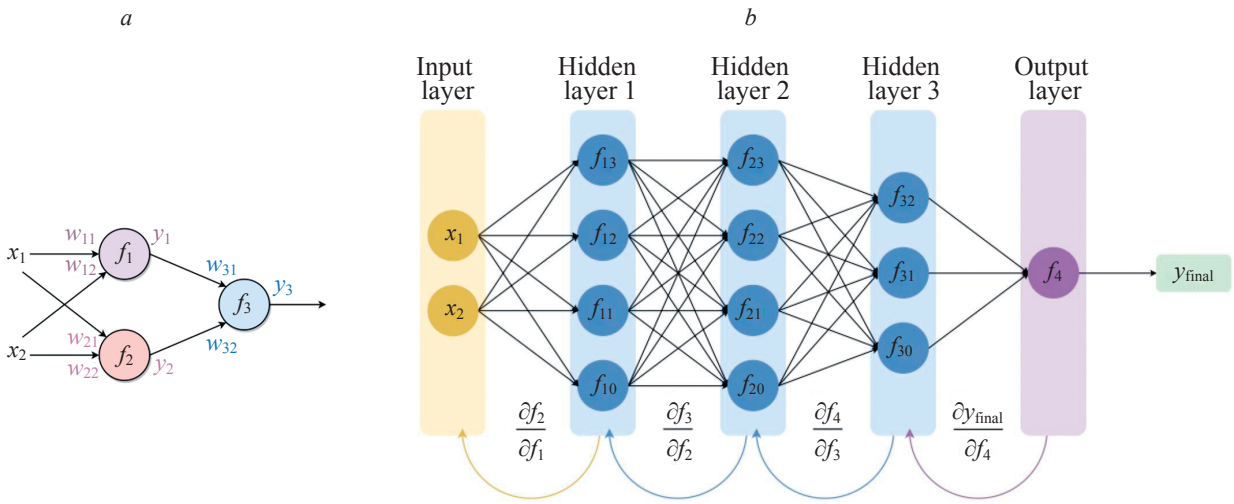

Fig. 1. DNN structure and learning mechanism: multilayer perceptron model (*a*); backpropagation process (*b*)

connecting all neurons from the previous layer to capture complex patterns. By combining these layers in a sequential manner and adjusting their parameters through processes like backpropagation and gradient descent, CNNs can learn complex patterns and make predictions on various tasks.

Evaluation Metrics

The evaluation of previous algorithms used for securing IIoT often involves employing various performance measures. These measures, including Accuracy, Precision, Recall, F1-score, true positive rate, false alarm rate, false positive rate, receiver operating characteristic curve, and area under the curve, are commonly utilized for assessing their effectiveness.

Model proposed

Dataset

The choice of dataset is critical for anomaly detection algorithms. This study makes use of the "Edge-IIoTset" dataset [32]. The dataset was created leveraging a purpose built IoT/IIoT testbed that includes a wide range of devices. The dataset contains data on 14 attacks related to IoT and IIoT connectivity protocols which are classified into five threat categories: DoS/DDoS attacks, information gathering, man-in-the-middle attacks, injection attacks, and malware assaults. It also includes features sourced from several sources, such as alarms, system resources, logs, and network traffic. The "Edge-IIoTset" dataset contains 61 features with two target variables: 'Attack label' for binary classification and 'Attack type' for multiclass classification. The 'Attack label' is explicitly designed for binary classification tasks, aiming to differentiate between two classes: "Attack" and "Normal". The target variable 'Attack label' assigns a binary label of 1 to instances representing attacks, and a label of 0 to instances representing normal traffic. On the other hand, the 'Attack type' target variable is intended for multiclass classification, enabling the categorization of instances into Different Attack (DA) types and normal traffic. Table 1 presents a summary of the instances of different IoT traffic types observed in the "Edge-IIoTset" dataset.

Table 1. Edge-IIoTset dataset Type Instances 'Attack type'

Class	Traffic Type	Instances
Normal	NORMAL	1,615,643
Attack	DDoS UDP	121,568
	DDoS ICMP	116,436
	SQL injection	51,203
	Password	50,153
	Vulnerability scanner	50,110
	DDoS TCP	50,062
	DDoS HTTP	49,911
	Uploading	37,634
	Backdoor	24,862
	Port Scanning	22,564
	XSS	15,915
	Ransomware	10,925
	MITM	1,214
	Fingerprinting	1,001

Experimental Approaches

The proposed model in this work is a composite algorithm consisting of a CNNs followed by a complex DNN. The design of the hybrid CNN-DNN model was motivated by the complementary strengths of both architectures. CNN layers are well-suited for capturing spatial and temporal patterns in sequential feature representations, while DNN layers are effective in combining those features through deep nonlinear transformations for robust classification. Initial tests with DNN-only models showed a tendency toward overfitting and limited generalization. Conversely, CNN-only models struggled to differentiate between closely related attack classes. The hybrid configuration achieved a balance between rich feature extraction and accurate classification resulting in superior performance across multiple class distributions. These results validate the architectural synergy of the CNN-DNN combination and reflect the trade-offs considered during model development.

However, before implementing the model, a preprocessing step is performed on the dataset to enhance the performance of the created model. Preprocessing the dataset is an essential step in any ML or DL task. It consists of transforming and preparing the raw data in a way that makes it suitable for training the model. The steps involved in preprocessing utilized in this study are:

— **Load the dataset:** The code loads the dataset from a *csv* file.
— **Drop unnecessary columns:** Certain columns in the dataset are not needed for the ML model, so they are dropped using the drop method of the DataFrame.
— **Drop rows with missing values:** Rows containing any missing values are removed from the dataset using the *dropna* method.
— **Shuffle the dataframe:** The rows in the DataFrame are shuffled randomly using the shuffle function from the *sklearn.utils* module. This is done to ensure that the data is not biased in any particular order.
— **Encode categorical variables:** Some columns in the dataset are categorical, meaning they represent categories rather than numerical values. To convert these categorical variables into a numerical format suitable for the model, one-hot encoding is performed using the *pd.get* dummies method.
— **Normalize the features:** The numerical features in the dataset are normalized to achieve a mean of '0' and a standard deviation of '1'. This is done by leveraging the StandardScaler from the *sklearn.preprocessing* module.
— **Encode the target variable:** The target variable, which is the 'Attack type' column representing the attack class, is encoded leveraging label encoding. Label encoding maps use the different classes to integer values.
— **Split the data:** The preprocessed data is split into training and testing sets using the train test split function from *sklearn.model* selection. The training set is utilized for model training, and the testing set is employed to evaluate its performance.

Binary classification

We build a DNN model for binary classification leveraging the given dataset. The model consists of Dense layers with Rectified Linear Unit (ReLU) activation functions and a Sigmoid activation function for the output layer. We compile and train the model using the Adaptive Moment Estimation (Adam) optimizer, binary crossentropy loss function, and Accuracy as the evaluation metric. The algorithm is depicted in Algorithm 1.

Algorithm 1 DNN Model for Binary Classification

Require: Input *x* train scaled, *y* train, *x* test scaled, *y* test

1: Perform label encoding on *y* train and *y* test to convert class labels into numerical format. build DNN model

2: Create a Sequential model

3: Add a Dense layer with 256 neurons and activation function ReLU, with input dimension equal to the number of features in *x* train scaled.

4: Add another Dense layer with 164 neurons and activation function ReLU.

5: Add another Dense layer with 82 neurons and activation function ReLU.

6: Add another Dense layer with 32 neurons and activation function ReLU.

7: Add the output Dense layer with 1 neuron and activation function Sigmoid (binary classification).

8: Call build DNN model() to build the DNN model for binary classification.

9: Compile the model using Adam optimizer and binary crossentropy loss function, with Accuracy as the evaluation metric.

10: Train the model with 25 epochs and a batch size of 32. Validate the model using *x* test scaled and *y* test encoded.

Multiclass Classification

In a well-structured dataset with efficient pre-processing, it is possible to modify the number of classes in the target according to our objectives and the use of the model in our environment. In Edget IIoTset the 'attacks-types' target is generally used to perform a multiclass classification. Manipulating the number of classes in the target variable can be beneficial in various ways:

— **Remove non-essential classes:** To simplify the model and improve focus on critical attacks, rare or less relevant attack classes were removed. The study retained the nine most common attack classes, where the model demonstrated high Accuracy. Fig. 2, *b* illustrates the distribution of these selected classes.

— **Merging similar classes:** Classes with similar attack characteristics were combined to reduce complexity while maintaining data representativeness. After analysis, 15 similar attack classes were merged into six broader categories (Fig. 2, *c*) ensuring essential attack features were preserved while enhancing model efficiency.

— **Aggregate classes:** Some classes had low Accuracy or insufficient data points, making them difficult to distinguish. Instead of removing them, they were grouped into a single new class called DA (Fig. 2, *a*). This aggregation increased representativeness and improved predictive performance.

— **Duplicate classes:** In certain cases, classes were duplicated to represent specific attack subcategories, enhancing the model ability to differentiate between various attack scenarios and improving Accuracy.

Once the data was pre-processed and the classes defined, we proceeded to model design (Fig. 2). The proposed architecture, called MC-CNN-DNN, combines a CNN for feature extraction and a DNN for classification. The CNN part includes three 1D convolutional layers with 256, 128, and 64 filters, respectively, each followed by a max-pooling layer (pool size = 2). The extracted features are flattened and passed to a DNN consisting of four fully connected layers with 256, 164, 82, and 32 neurons, all using ReLU activation. L2 regularization ($\lambda = 0.00001$) is applied to all dense layers. The final output layer has 6 (or 9, 10, 15) neurons with Softmax activation for multiclass classification. After one-hot encoding and normalization, the input data contained 96 features per sample, reshaped to match the CNN input format of (96, 1) representing 96 features and one channel. This shape is optimal for Conv1D layers. The model was compiled with the Adam optimizer (learning rate = 0.0001) and categorical cross-entropy as the loss function. It was trained over 25 epochs with a batch size of 32, using 20 % of the training data for validation. The full structure and implementation of the model are detailed in Algorithm 2.

Algorithm 2 MC-CNN-DNN Model

Require: *x* train, *y* train, *x* test, *y* test.

1: Initialize the model as Sequential()

2: Add Conv1D Layer with filters=256, kernel size=3, activation= 'relu', input shape=(xtrain.shape[1], 1)

3: Add MaxPooling1D Layer with pool size=2

4: Add Conv1D Layer with filters=128, kernel size=3, activation='relu'

5: Add MaxPooling1D Layer with pool size=2

6: Add Conv1D Layer with filters=64, kernel size=3, activation='relu'

7: Add MaxPooling1D Layer with pool size=2

8: Add Flatten Layer

9: Add Dense Layer with units=256, activation='relu', kernel regularizer=l2(0.00001)

10: Add Dense Layer with units=164, activation='relu', kernel regularizer=l2(0.00001)

11: Add Dense Layer with units=82, activation='relu', kernel regularizer=l2(0.00001)

12: Add Dense Layer with units=32, activation='relu', kernel regularizer=l2(0.00001)

13: Add Dense Layer with units=classnum, activation='softmax'

14: Set the optimizer as Adam with learning rate 0.001

15: Set the loss function as categorical crossentropy

16: Compile the model with optimizer and loss function

17: Train the model

18: Fit the model on *x* train and *y* train for 20 epochs with batch size=512 and validation split=0.2

19: Save the training history in history

20: Evaluate the model on *x* test and *y* test, and save the results in score.

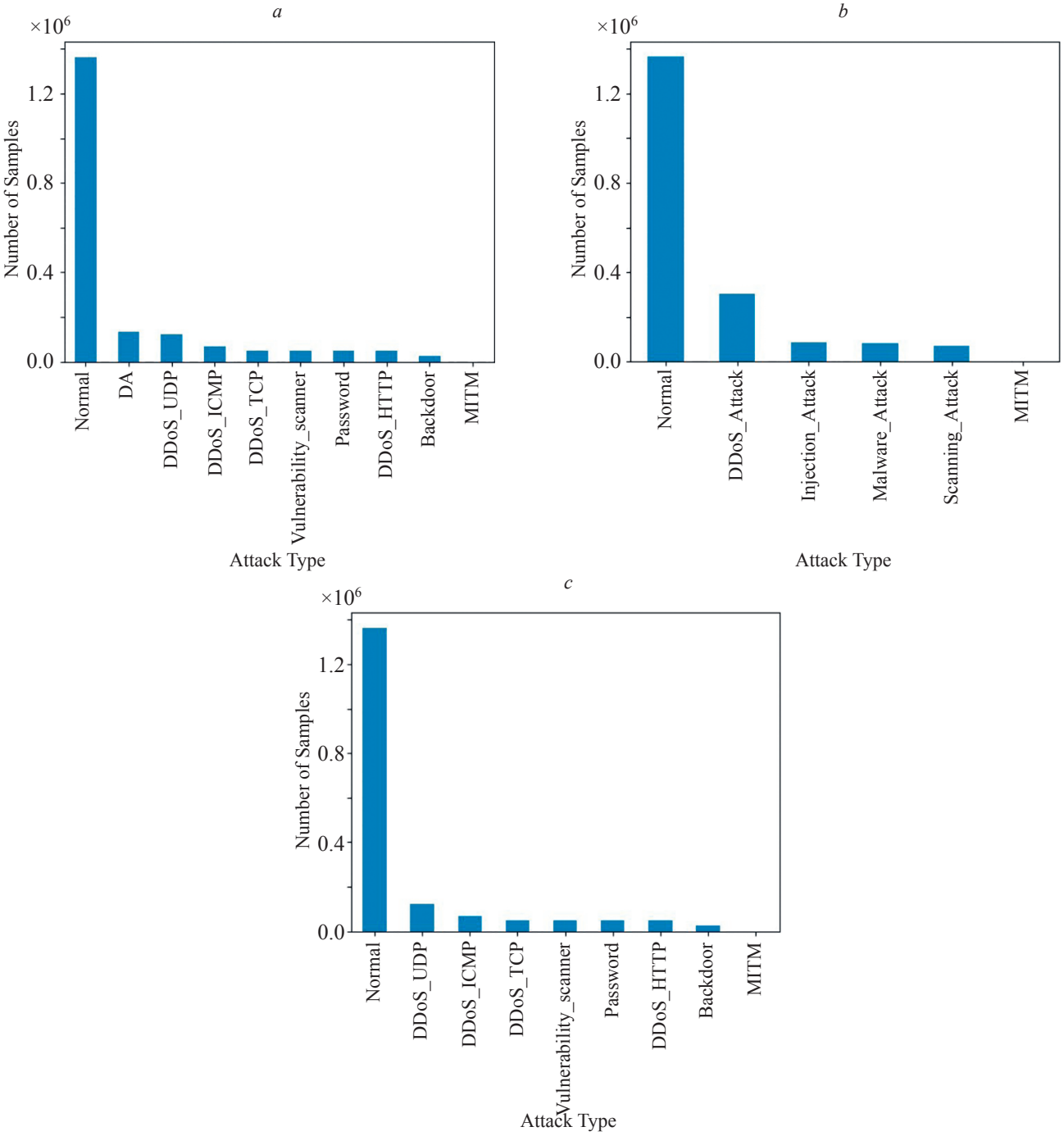

Fig. 2. Bar distribution across class settings: 10-class (*a*); 6-class (*b*); 9-class (*c*)

Results and Discussion

This paper proposes an innovative and efficient method for modern intrusion detection systems which are crucial for identifying unauthorized activity within computer networks. Despite the use of state-of-the-art algorithms to categorize a wide range of intrusion scenarios, their overall performance remains suboptimal. The experiment results show the model outstanding proficiency in distinguishing between the two classes, 'Normal' and 'Attack'. Achieving a perfect score (100 %) across all binary classification metrics — Accuracy, Precision, Recall, and F1-score, highlights its ability to classify instances with complete Accuracy while minimizing misclassifications. These results confirm the model exceptional suitability for binary classification tasks.

The Accuracy results across the testing, validation, and training sets using the "Edge IIoTset" dataset are illustrated in Fig. 4, with representing different class distribution scenarios.

Notably, our proposed method, the MC-CNN-DNN model, consistently demonstrates exceptional Accuracy across all approaches examined. Particularly, when assessing different class distributions, the 9-class distribution approach emerges as the standout performer, boasting an impressive Accuracy rate of 99.50 %. Similarly,

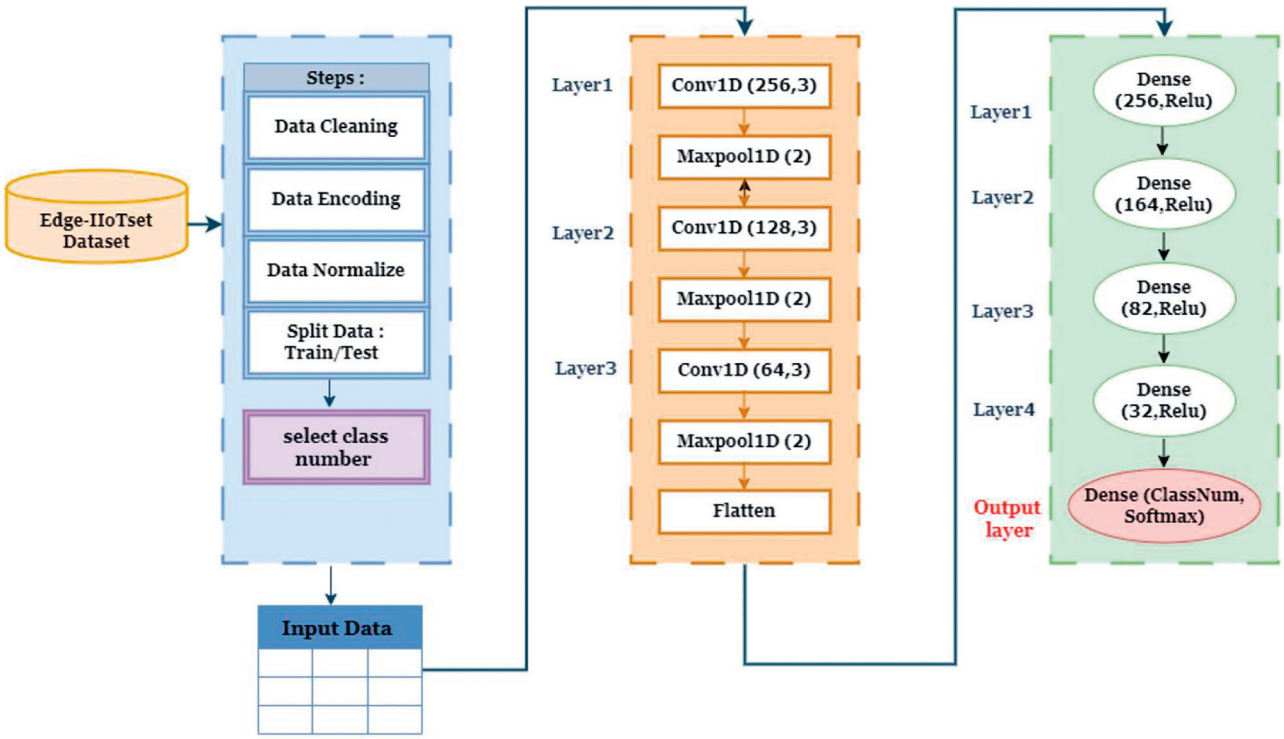

Fig. 3. Proposed methodology of the study

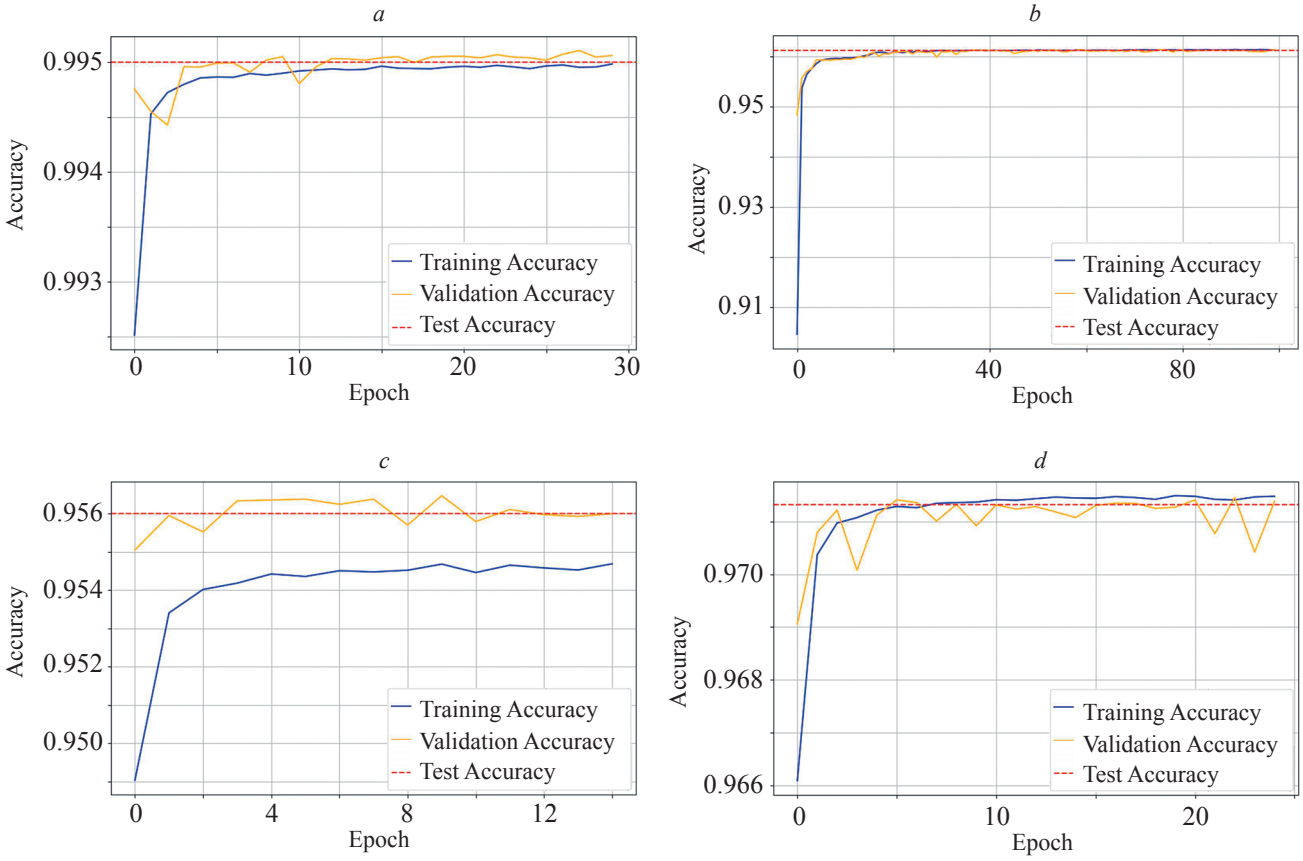

Fig. 4. Accuracy performance across various class distributions for the proposed MC-CNN-DNN model: 9-class (99.50 %) (*a*); 10-class (96.12 %) (*b*); 15-class (95.6 %) (*c*); and 6-class (97.14 %) (*d*)

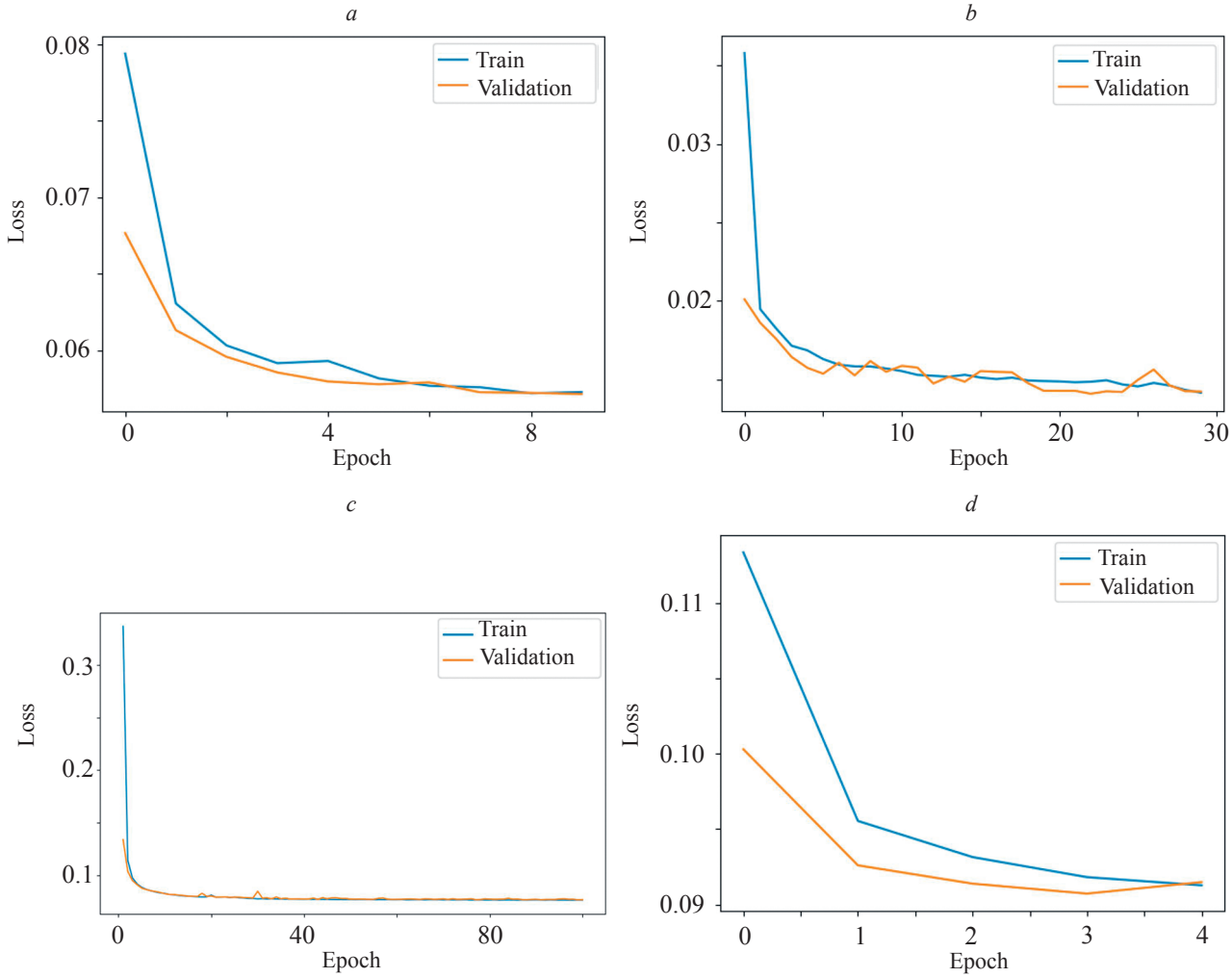

Fig. 5. Loss function across various class distributions: 6-class (*a*); 9-class (*b*); 10-class (*c*); 15-class (*d*)

the 6-class distribution approach exhibits a robust Accuracy level of 97.14 %. Meanwhile, the Accuracy for the 10-class distribution approach remains noteworthy at 96.12 %, followed closely by the 15-class distribution approach with an Accuracy of 95.6 %.

Fig. 5 subpictures reveal consistently low loss values across all scenarios, highlighting the model stability during training. Furthermore, the close alignment between training and validation loss curves indicates the absence of overfitting. These results underscore the efficacy of our proposed MC-CNN-DNN model in achieving high Accuracy across diverse class distribution scenarios, further affirming its potential for robust intrusion detection within the complex landscape of the "Edge IIoTset" dataset.

Table 2 shows the evaluation metrics in terms of Precision, Recall, and F1-score of a MC-CNN-DNN model on 15-class distribution, Classes like "Normal", "Backdoor", "DDoS HTTP", "DDoS ICMP", "DDoS TCP", "DDoS UDP", "Fingerprinting", "MITM", "Password", "Port Scanning", "Ransomware", "SQL injection", "Uploading", "Vulnerability scanner", and "XSS".

Table 3 shows the performance of a MC-CNN-DNN model on 9-class distribution. Classes like "Normal", "DDoS UDP", "DDoS ICMP", and "MITM" show perfect

Table 2. Evaluation Metrics for 15-class Distribution, %

Class	Precision	Recall	F1-score
Normal	100	100	100
Backdoor	94	97	96
DDoS HTTP	74	96	84
DDoS ICMP	100	100	100
DDoS TCP	84	100	91
DDoS UDP	100	100	100
Fingerprinting	35	46	40
MITM	100	100	100
Password	91	19	32
Port Scanning	85	57	69
Ransomware	100	75	86
SQL injection	46	91	61
Uploading	67	48	56
Vulnerability scanner	100	83	90
XSS	62	35	44

Table 3. Evaluation Metrics for 9-class Distribution, %

Class	Precision	Recall	F1-score
Normal	100	100	100
DDoS UDP	100	100	100
DDoS ICMP	100	100	100
DDoS TCP	99	100	100
Vulnerability scanner	100	100	100
Password	98	85	91
DDoS HTTP	87	98	92
Backdoor	100	98	99
MITM	100	100	100

Precision, Recall, and F1-score, indicating that the model performs exceptionally well on these classes. The "DDoS TCP" class has also high Precision 99 %, suggesting that there might be a few false positives. However, the Recall and F1-score are still high. "Vulnerability scanner", "Password", and "Backdoor" classes also show good performance, although "Password" has relatively lower Recall, impacting its F1-score. "DDoS HTTP" class has a lower Precision 87 % but a high Recall 98 %, resulting in a good F1-score.

In Table 4, the model demonstrates excellent performance in classifying various 10-class of attack subtypes. For "DDoS UDP" and "DDoS ICMP" classes, it achieves perfect Precision and Recall. In the "DDoS TCP" class, the model achieves a Precision of 82 % and a Recall of 100 %, resulting in an F1-score of 92 %. In "DA" class, the model performance is reasonable, achieving a Precision of 71 % and a Recall of 85 %, leading to an F1-score of 77 %. The model performs well on the "Vulnerability scanner" class with a Precision of 91 % and a Recall of 81 %. However, for the "Password" class, Precision is perfect at 100 %, and Recall is 84 %. In the "Backdoor" class, the model performs admirably with high Precision of 99 % and Recall of 95 %, resulting in an F1-score of 97 %.

In Table 5, for 6-class distribution the model performance remains strong. In "DDoS attack" it achieves a Precision of 68 % and a high Recall of 99 %, resulting in an F1-score of 81 %. For "Injection attack", "Scanning attack", and "MITM", the model excels with perfect Precision, Recall, and F1-score for these classes. However, in "Malware attack", the model performance is moderate, attaining a Precision of 95 % but a lower Recall of 51 %, which leads to an F1-score of 66 %. Table 6 summarizes the results obtained in terms of both Accuracy and loss function.

Table 7 offers a concise comparison of model performances within the domain of intrusion detection leveraging the "Edge IIoTset" dataset. Our MC-CNN-DNN hybrid model stands out with the highest Accuracy, indicating its robustness and potential for enhanced security measures in industrial IoT environments. This comparison sheds light on the advancements made in intrusion detection techniques, further contributing to the development of effective solutions for safeguarding IIoT systems.

Table 4. Evaluation Metrics for 10-class Distribution, %

Class	Precision	Recall	F1-score
Normal	100	100	100
DA	71	85	77
DDoS UDP	100	100	100
DDoS ICMP	100	99	100
DDoS TCP	82	100	92
Vulnerability scanner	91	81	92
Password	100	84	91
DDoS HTTP	75	94	84
Backdoor	99	95	97
MITM	100	100	100

Table 5. Evaluation Metrics for 6-class Distribution, %

Class	Precision	Recall	F1-score
Normal	95	100	97
DDoS Attack	68	99	81
Injection attack	100	100	100
Malware attack	95	51	66
Scanning attack	100	100	100
MITM	98	73	84

Table 6. Summary of results

Class Num	Accuracy, %	Loss Function
2-class	100	$5.52 \cdot 10^{-6}$
6-class	97	0.062
9-class	99	0.014
10-class	96	0.070
15-class	95	0.080

Table 7. Comparison of the results with previous studies using the 'Edge IIoTset' dataset

Authors	Model	Accuracy, %
[32]	DNN	96.0
[33]	CNN-LSTM	98.7
[34]	Inception Time	94.9
Our work	CNN-DNN	99.5

Limitations and Future Work

While our proposed Multiclassification CNN-DNN model achieved outstanding results on the Edge-IIoTset dataset, certain considerations remain for future exploration. As with most DL models, performance can vary with dataset size and class balance, suggesting that larger or more diverse datasets may further enhance generalization. The hybrid architecture, though highly effective, introduces a moderate computational cost that could be optimized

for edge deployments. Moreover, extending validation to other IIoT datasets would further confirm the model adaptability across varying industrial environments. Future work will focus on improving efficiency and portability, while exploring integration with other learning strategies such as autoencoders, Reinforcement Learning, or Graph Neural Networks.

Conclusion

This study presented a hybrid Convolutional Neural Network with Deep Neural Network model for intrusion detection, trained and tested on the Edge-IIoTset dataset. By applying thorough preprocessing and using various class distribution scenarios (2, 6, 9, 10, and 15 classes), the model achieved excellent classification results. Notably, the 9-class configuration reached an Accuracy of 99.13 %, while the 6-class and 10-class setups also delivered strong performance at 97.13 % and 96.11 %, respectively. Our architecture effectively combines feature extraction and deep classification layers, resulting in a robust solution adaptable to complex Industrial Internet of Things traffic. Future work will focus on integrating other models like Reinforcement Learning, autoencoders, and Graph Neural Networks, along with evaluating the system on new datasets and in real-time industrial environments.

References

1. Jaidka H., Sharma N., Singh R. Evolution of IoT to IIoT: applications & challenges. *Proc. of the International Conference on Innovative Computing & Communications (ICICC)*, 2020, pp. 1–6. https://doi.org/10.2139/ssrn.3603739
2. Farhan L., Kharel R., Kaiwartya O., Quiroz-Castellanos M., Alissa A., Abdulsalam M. A concise review on internet of things (IoT)-problems, challenges and opportunities. *Proc. of the 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP)*, 2018, pp. 1–6. https://doi.org/10.1109/CSNDSP.2018.8471762
3. Chalishazar T. *Peerbits exploring the applications of IoT in different industries*, 2023. Available at: https://www.peerbits.com/blog/iot-applications-in-different-industries.html (accessed: 24.06.2023)
4. Qiu T., Chi J., Zhou X., Ning Z., Atiquzzaman M., Wu D.O. Edge computing in Industrial Internet of Things: architecture, advances and challenges. *IEEE Communications Surveys & Tutorials*, 2020, vol. 22, no. 4, pp. 2462–2488. https://doi.org/10.1109/COMST.2020.3009103
5. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues. *Computers in Industry*, 2018, vol. 100, no. 1, pp. 212–223.
6. Mohamed N., Al-Jaroodi J., Jawhar I. Cyber–physical systems forensics: today and tomorrow. *Journal of Sensor and Actuator Networks*, 2020, vol. 9, no. 3, pp. 37. https://doi.org/10.3390/jsan9030037
7. Javaid M., Haleem A., Singh R.P., Suman R., Gonzalez E.S. Understanding the adoption of industry 4.0 technologies in improving environmental sustainability. *Sustainable Operations and Computers*, 2022, vol. 3, pp. 203–217. https://doi.org/10.1016/j.susoc.2022.01.008
8. Mirani A.A., Velasco-Hernandez G., Awasthi A., Walsh J. Key challenges and emerging technologies in industrial iot architectures: A review. *Sensors*, 2022, vol. 22, no. 15, pp. 5836. https://doi.org/10.3390/s22155836
9. Younan M., Houssein E.H., Elhoseny M., Ali A.A. Challenges and recommended technologies for the industrial internet of things: A comprehensive review. *Measurement*, 2020, vol. 151, pp. 107198. https://doi.org/10.1016/j.measurement.2019.107198
10. Gebremichael T., Ledwaba L.P., Eldefrawy M.H., Hancke G.P., Pereira N., Gidlund M., Akerberg J. Security and privacy in the industrial internet of things: current standards and future challenges. *IEEE Access*, 2020, vol. 8, pp. 152351–152366. https://doi.org/10.1109/ACCESS.2020.3016937
11. Madhuri G.S., Rani M.U. Anomaly detection techniques. *Proc. of the IADS International Conference on Computing, Communications & Data Engineering (CCODE)*, 2018, pp. 1–6.
12. Munir M., Chattha M.A., Dengel A., Ahmed S. A comparative analysis of traditional and deep learning-based anomaly detection methods for streaming data. *Proc. of the 18th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 2019, pp. 561–566. https://doi.org/10.1109/icmla.2019.00105
13. Du J., Yang K., Hu Y., Jiang L. NIDS-CNNLSTM: Network intrusion detection classification model based on deep learning. *IEEE Access*, 2023, vol. 11, pp. 24808–24821. https://doi.org/10.1109/ACCESS.2023.3254915
14. Kandhro I.A., Alanazi S.M., Ali F., Kehar A., Fatima K., Uddin M. Detection of real-time malicious intrusions and attacks in IoT

Литература

1. Jaidka H., Sharma N., Singh R. Evolution of IoT to IIoT: applications & challenges // Proc. of the International Conference on Innovative Computing & Communications (ICICC). 2020. P. 1–6. https://doi.org/10.2139/ssrn.3603739
2. Farhan L., Kharel R., Kaiwartya O., Quiroz-Castellanos M., Alissa A., Abdulsalam M. A concise review on internet of things (IoT)-problems, challenges and opportunities // Proc. of the 11th International Symposium on Communication Systems, Networks & Digital Signal Processing (CSNDSP). 2018. P. 1–6. https://doi.org/10.1109/CSNDSP.2018.8471762
3. Chalishazar T. Peerbits exploring the applications of IoT in different industries. 2023. URL: https://www.peerbits.com/blog/iot-applications-in-different-industries.html (accessed: 24.06.2023)
4. Qiu T., Chi J., Zhou X., Ning Z., Atiquzzaman M., Wu D.O. Edge computing in Industrial Internet of Things: architecture, advances and challenges // IEEE Communications Surveys & Tutorials. 2020. V. 22. N 4. P. 2462–2488. https://doi.org/10.1109/COMST.2020.3009103
5. Alguliyev R., Imamverdiyev Y., Sukhostat L. Cyber-physical systems and their security issues // Computers in Industry. 2018. V. 100. N 1. P. 212–223.
6. Mohamed N., Al-Jaroodi J., Jawhar I. Cyber–physical systems forensics: today and tomorrow // Journal of Sensor and Actuator Networks. 2020. V. 9. N 3. P. 37. https://doi.org/10.3390/jsan9030037
7. Javaid M., Haleem A., Singh R.P., Suman R., Gonzalez E.S. Understanding the adoption of industry 4.0 technologies in improving environmental sustainability // Sustainable Operations and Computers. 2022. V. 3. P. 203–217. https://doi.org/10.1016/j.susoc.2022.01.008
8. Mirani A.A., Velasco-Hernandez G., Awasthi A., Walsh J. Key challenges and emerging technologies in industrial iot architectures: A review // Sensors. 2022. V. 22. N 15. P. 5836. https://doi.org/10.3390/s22155836
9. Younan M., Houssein E.H., Elhoseny M., Ali A.A. Challenges and recommended technologies for the industrial internet of things: A comprehensive review // Measurement. 2020. V. 151. P. 107198. https://doi.org/10.1016/j.measurement.2019.107198
10. Gebremichael T., Ledwaba L.P., Eldefrawy M.H., Hancke G.P., Pereira N., Gidlund M., Akerberg J. Security and privacy in the industrial internet of things: current standards and future challenges // IEEE Access. 2020. V. 8. P. 152351–152366. https://doi.org/10.1109/ACCESS.2020.3016937
11. Madhuri G.S., Rani M.U. Anomaly detection techniques // Proc. of the IADS International Conference on Computing, Communications & Data Engineering (CCODE). 2018. P. 1–6.
12. Munir M., Chattha M.A., Dengel A., Ahmed S. A comparative analysis of traditional and deep learning-based anomaly detection methods for streaming data // Proc. of the 18th IEEE International Conference on Machine Learning and Applications (ICMLA). 2019. P. 561–566. https://doi.org/10.1109/icmla.2019.00105
13. Du J., Yang K., Hu Y., Jiang L. NIDS-CNNLSTM: Network intrusion detection classification model based on deep learning // IEEE Access. 2023. V. 11. P. 24808–24821. https://doi.org/10.1109/ACCESS.2023.3254915
14. Kandhro I.A., Alanazi S.M., Ali F., Kehar A., Fatima K., Uddin M. Detection of real-time malicious intrusions and attacks in IoT

empowered cybersecurity infrastructures. *IEEE Access*, 2023, vol. 11, pp. 9136– 9148. https://doi.org/10.1109/ACCESS.2023.3238664
15. Alrowaily M., Alenezi F., Lu Z. Effectiveness of machine learning based intrusion detection systems. *Lecture Notes in Computer Science*, 2019, vol. 11611, pp. 277–288. https://doi.org/10.1007/978-3-030-24907-6_21
16. Cam N.T., Trung N.G. An intelligent approach to improving the performance of threat detection in IoT. *IEEE Access*, 2023, vol. 11, pp. 44319–44334. https://doi.org/10.1109/ACCESS.2023.3273160
17. Al-Abassi A., Karimipour H., Dehghantanha A., Pariz R.M. An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access*, 2020, vol. 8, pp. 83965– 83973. https://doi.org/10.1109/ACCESS.2020.2992249
18. Shone N., Ngoc T.N., Phai V.D., Shi Q. A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2018, vol. 2, no. 1, pp. 41–50. https://doi.org/10.1109/TETCI.2017.2772792
19. Ullah I., Mahmoud Q.H. Design and development of a deep learning-based model for anomaly detection in IoT networks. *IEEE Access*, 2021, vol. 9, pp. 103906–103926. https://doi.org/10.1109/ACCESS.2021.3094024
20. Gümüşbaş D., Yıldırım T., Genovese A., Scotti F. A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. *IEEE Systems Journal*, 2020, vol. 15, no. 2, pp. 1717–1731. https://doi.org/10.1109/JSYST.2020.2992966
21. Ashraf E., Areed N.F., Salem H., Salem H., Abdelhady E., Farouk A. IoT based intrusion detection systems from the perspective of machine and deep learning: a survey and comparative study. *Delta University Scientific Journal*, 2022, vol. 5, no. 2, pp. 367–386. https://doi.org/10.21608/dusj.2022.275552
22. Thakkar A., Lohiya R. A review of the advancement in intrusion detection datasets. *Procedia Computer Science*, 2020, vol. 167, pp. 636–645. https://doi.org/10.1016/j.procs.2020.03.330
23. Mishra N., Pandya S. Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*, 2021, vol. 9, pp. 59353–59377. https://doi.org/10.1109/ACCESS.2021.3073408
24. Liu L., Wang P., Lin J., Liu L. Intrusion detection of imbalanced network traffic based on machine learning and deep learning. *IEEE Access*, 2020, vol. 9, pp. 7550–7563. https://doi.org/10.1109/ACCESS.2020.3048198
25. Ito A., Saito K., Ueno R., Homma N. Imbalanced data problems in deep learning-based side-channel attacks: Analysis and solution. *IEEE Transactions on Information Forensics and Security*, 2021, vol. 16, pp. 3790–3802. https://doi.org/10.1109/TIFS.2021.3092050
26. Goyal P., Pandey S., Jain K. *Deep Learning for Natural Language Processing: Creating Neural Networks with Python*. Apress, 2018, 294 p.
27. Chinnathambi R.A., Plathottam S.J., Hossen T., Nair A.S., Ranganathan P. Deep neural networks (DNN) for day-ahead electricity price markets. *Proc. of the IEEE electrical power and energy conference (EPEC)*, 2018, pp. 1–6. https://doi.org/10.1109/EPEC.2018.8598327
28. Rosenblatt F. The perceptron: a probabilistic model for information storage and organization in the brain. *Psychological Review*, 1958, vol. 65, no. 6, pp. 386–408. https://doi.org/10.1037/h0042519
29. LeCun Y., Boser B., Denker J.S., Henderson D., Howard R.E., Hubbard W., Jackel L.D. Backpropagation applied to handwritten zip code recognition. *Neural Computation*, 1989, vol. 1, no. 4, pp. 541–551. https://doi.org/10.1162/neco.1989.1.4.541
30. Hubel D.H., Wiesel T.N. Receptive fields and functional architecture of monkey striate cortex. *The Journal of Physiology*, 1968, vol. 195, no. 1, pp. 215–243. https://doi.org/10.1113/jphysiol.1968.sp008455
31. Yamashita R., Nishio M., Do R.K.G., Togashi K. Convolutional neural networks: an overview and application in radiology. *Insights into Imaging*, 2018, vol. 9, pp. 611–629. https://doi.org/10.1007/s13244-018-0639-9
32. Ferrag M.A., Friha O., Hamouda D., Maglaras L., Janicke H. Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. *IEEE Access*, 2022, vol. 10, pp. 40281–40306. https://doi.org/10.1109/access.2022.3165809
33. Khacha A., Saadouni R., Harbi Y., Aliouat Z. Hybrid deep learning-based intrusion detection system for industrial Internet of Things. *Proc. of the 5th International Symposium on Informatics and its*

empowered cybersecurity infrastructures // IEEE Access. 2023. V. 11. P. 9136– 9148. https://doi.org/10.1109/ACCESS.2023.3238664
15. Alrowaily M., Alenezi F., Lu Z. Effectiveness of machine learning based intrusion detection systems // Lecture Notes in Computer Science. 2019. V. 11611. P. 277–288. https://doi.org/10.1007/978-3-030-24907-6_21
16. Cam N.T., Trung N.G. An intelligent approach to improving the performance of threat detection in IoT // IEEE Access. 2023. V. 11. P. 44319–44334. https://doi.org/10.1109/ACCESS.2023.3273160
17. Al-Abassi A., Karimipour H., Dehghantanha A., Pariz R.M. An ensemble deep learning-based cyber-attack detection in industrial control system // IEEE Access. 2020. V. 8. P. 83965– 83973. https://doi.org/10.1109/ACCESS.2020.2992249
18. Shone N., Ngoc T.N., Phai V.D., Shi Q. A deep learning approach to network intrusion detection // IEEE Transactions on Emerging Topics in Computational Intelligence. 2018. V. 2. N 1. P. 41–50. https://doi.org/10.1109/TETCI.2017.2772792
19. Ullah I., Mahmoud Q.H. Design and development of a deep learning-based model for anomaly detection in IoT networks // IEEE Access. 2021. V. 9. P. 103906–103926. https://doi.org/10.1109/ACCESS.2021.3094024
20. Gümüşbaş D., Yıldırım T., Genovese A., Scotti F. A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems // IEEE Systems Journal. 2020. V. 15. N 2. P. 1717–1731. https://doi.org/10.1109/JSYST.2020.2992966
21. Ashraf E., Areed N.F., Salem H., Salem H., Abdelhady E., Farouk A. IoT based intrusion detection systems from the perspective of machine and deep learning: a survey and comparative study // Delta University Scientific Journal. 2022. V. 5. N 2. P. 367–386. https://doi.org/10.21608/dusj.2022.275552
22. Thakkar A., Lohiya R. A review of the advancement in intrusion detection datasets // Procedia Computer Science. 2020. V. 167. P. 636–645. https://doi.org/10.1016/j.procs.2020.03.330
23. Mishra N., Pandya S. Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review // IEEE Access. 2021. V. 9. P. 59353–59377. https://doi.org/10.1109/ACCESS.2021.3073408
24. Liu L., Wang P., Lin J., Liu L. Intrusion detection of imbalanced network traffic based on machine learning and deep learning // IEEE Access. 2020. V. 9. P. 7550–7563. https://doi.org/10.1109/ACCESS.2020.3048198
25. Ito A., Saito K., Ueno R., Homma N. Imbalanced data problems in deep learning-based side-channel attacks: Analysis and solution // IEEE Transactions on Information Forensics and Security. 2021. V. 16. P. 3790–3802. https://doi.org/10.1109/TIFS.2021.3092050
26. Goyal P., Pandey S., Jain K. Deep Learning for Natural Language Processing: Creating Neural Networks with Python. Apress, 2018. 294 p.
27. Chinnathambi R.A., Plathottam S.J., Hossen T., Nair A.S., Ranganathan P. Deep neural networks (DNN) for day-ahead electricity price markets // Proc. of the IEEE electrical power and energy conference (EPEC). 2018. P. 1–6. https://doi.org/10.1109/EPEC.2018.8598327
28. Rosenblatt F. The perceptron: a probabilistic model for information storage and organization in the brain // Psychological Review. 1958. V. 65. N 6. P. 386–408. https://doi.org/10.1037/h0042519
29. LeCun Y., Boser B., Denker J.S., Henderson D., Howard R.E., Hubbard W., Jackel L.D. Backpropagation applied to handwritten zip code recognition // Neural Computation. 1989. V. 1. N 4. P. 541–551. https://doi.org/10.1162/neco.1989.1.4.541
30. Hubel D.H., Wiesel T.N. Receptive fields and functional architecture of monkey striate cortex // The Journal of Physiology. 1968. V. 195. N 1. P. 215–243. https://doi.org/10.1113/jphysiol.1968.sp008455
31. Yamashita R., Nishio M., Do R.K.G., Togashi K. Convolutional neural networks: an overview and application in radiology // Insights into Imaging. 2018. V. 9. P. 611–629. https://doi.org/10.1007/s13244-018-0639-9
32. Ferrag M.A., Friha O., Hamouda D., Maglaras L., Janicke H. Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning // IEEE Access. 2022. V. 10. P. 40281–40306. https://doi.org/10.1109/access.2022.3165809
33. Khacha A., Saadouni R., Harbi Y., Aliouat Z. Hybrid deep learning-based intrusion detection system for industrial Internet of Things // Proc. of the 5th International Symposium on Informatics and its

Applications (ISIA), 2022, pp. 1–6. https://doi.org/10.1109/ISIA55826.2022.9993487
34. Tareq I., Elbagoury B.M., El-Regaily S., El-Horbaty E.S.M. Analysis of ToN-IoT, UNW-NB15, and edge-IIoT datasets using dl in cybersecurity for IoT. *Applied Sciences*, 2022, vol. 12, no. 19, pp. 9572. https://doi.org/10.3390/app12199572

Applications (ISIA). 2022. P. 1–6. https://doi.org/10.1109/ISIA55826.2022.9993487
34. Tareq I., Elbagoury B.M., El-Regaily S., El-Horbaty E.S.M. Analysis of ToN-IoT, UNW-NB15, and edge-IIoT datasets using dl in cybersecurity for IoT // Applied Sciences. 2022. V. 12. N 19. P. 9572. https://doi.org/10.3390/app12199572

Authors

Wafaa Ferhi — PhD Student, Assistant, University of Abu Bekr Belkaid, Tlemcen, 13000, Algeria, sc 58480659800, https://orcid.org/0009-0005-7574-8368, wafaa.ferhi@univ-tlemcen.dz
Djilali Moussaoui — Lecturer, University of Abu Bekr Belkaid, Tlemcen, 13000, Algeria, sc 56360232600, https://orcid.org/0000-0003-3478-263X, djilali.moussaoui@univ-tlemcen.dz
Mourad Hadjila — Lecturer, University of Abu Bekr Belkaid, Tlemcen, 13000, Algeria, sc 56440246000, https://orcid.org/0000-0002-6554-3925, mourad.hadjila@univ-tlemcen.dz
Al Baraa Bouidaine — PhD Student, Assistant, University of Abu Bekr Belkaid, Tlemcen, 13000, Algeria, sc 58482050500, https://orcid.org/0009-0005-2204-9117, albaraa.bouidaine@univ-tlemcen.dz

Авторы

Ферхи Вафаа — аспирант, ассистент, Университет Абу Бекра Белкаида, Тлемсен, 13000, Алжир, sc 58480659800, https://orcid.org/0009-0005-7574-8368, wafaa.ferhi@univ-tlemcen.dz
Муссауи Джилали — преподаватель, Университет Абу Бекра Белкаида, Тлемсен, 13000, Алжир, sc 56360232600, https://orcid.org/0000-0003-3478-263X, djilali.moussaoui@univ-tlemcen.dz
Хаджила Мурад — преподаватель, Университет Абу Бекра Белкаида, Тлемсен, 13000, Алжир, sc 56440246000, https://orcid.org/0000-0002-6554-3925, mourad.hadjila@univ-tlemcen.dz
Буиден Аль Бараа — аспирант, ассистент, Университет Абу Бекра Белкаида, Тлемсен, 13000, Алжир, sc 58482050500, https://orcid.org/0009-0005-2204-9117, albaraa.bouidaine@univ-tlemcen.dz

Received 11.02.2025
Approved after reviewing 27.08.2025
Accepted 25.09.2025

Статья поступила в редакцию 11.02.2025
Одобрена после рецензирования 27.08.2025
Принята к печати 25.09.2025