Adaptive fuzzy model for anomaly detection in iot network traffic*

Nataliia Petliak[1,†], Yurii Klots[1,*,†], Dmytro Tymoshchuk[2,†], Mikolaj Karpinski[3,†] and Mariia Stadnyk[2,†]

[1] Khmelnytskyi National University, 11, Instytuts'ka str., Khmelnytskyi, 29016, Ukraine
[2] Ternopil Ivan Puluj National Technical University, 56, Ruska str., Ternopil, 46001, Ukraine
[3] University of the National Education Commission, 2 Podchorążych str, Krakow, 30084, Poland

Abstract

The paper proposes an adaptive fuzzy model for anomaly detection in the network traffic of the Internet of Things, focused on working in conditions of non-stationary data and limited computing resources. Unlike traditional signature and most deep approaches, the developed model combines automated formation of linguistic variables and a decision-making procedure within a single fuzzy mechanism. The formation of term sets and parameters of membership functions is carried out based on the Fuzzy C-Means algorithm, which allows to avoid manual setting of thresholds and reduce the subjective influence of expert assessments. The fuzzy rule base is automatically generated using the Wang–Mendel algorithm and supplemented by a formalized rule aging mechanism, which ensures adaptation of the model to the evolution of network traffic without full re-training. The experimental evaluation was carried out using open datasets MQTTset, IoTID20 and CICIoT2023, which differ in scale, structure and types of attacks. The obtained results demonstrate consistently high accuracy, completeness, and F1-measure (over 98%), confirming the effectiveness and generalizability of the proposed approach. The proposed model combines interpretability of solutions, computational efficiency, and suitability for practical application in real IoT environments.

Keywords

Internet of things, intrusion detection, network traffic anomalies, fuzzy logic, fuzzy c-means, Wang–Mendel

1. Introduction

The rapid growth of the number of connected devices within the Internet of Things (IoT) is significantly transforming modern information systems, creating the prerequisites for the widespread implementation of automated solutions in everyday life, industry, medicine and critical infrastructure. At the same time, this evolution is accompanied by a significant expansion of the attack surface, since typical IoT devices are characterized by limited computing resources, simplified authentication mechanisms and a long life cycle without regular security updates. As a result, the compromise of individual nodes often leads to large-scale network incidents, which increases the requirements for intrusion detection systems in such environments [1-2].

Traditional signature-based intrusion detection systems have limited effectiveness in the face of new or modified attacks, as they operate on predefined patterns. This has led to the active development of machine and deep learning methods that can automatically detect complex patterns in network traffic and distinguish between normal and abnormal behavior without explicitly specifying rules. Recent studies have shown that convolutional neural networks, recurrent architectures (RNN, LSTM, GRU), and their hybrid combinations are effective for analyzing the spatiotemporal characteristics of IoT traffic [3-4].

* IntelITSIS'26: The 7th International Workshop on Intelligent Information Technologies & Systems of Information Security, July 3, 2026, Khmelnytskyi, Ukraine
[1,*] Corresponding author.
[†] These authors contributed equally.
npetlyak@khmnu.edu.ua (N. Petliak); klots@khmnu.edu.ua (Y. Klots); dmytro.tymoshchuk@gmail.com (D. Tymoshchuk); mikolaj.karpinski@uken.krakow.pl (M. Karpinski); stadnyk_m@tntu.edu.ua (M. Stadnyk)
0000-0001-5971-4428 (N. Petliak); 0000-0002-3914-0989 (Y. Klots); 0000-0003-0246-2236 (D. Tymoshchuk); 0000-0002-8846-332X (M. Karpinski); 0000-0002-0287-2254 (M. Stadnyk)

Further development of this direction is associated with the use of attention mechanisms and multi-vector architectures, which allow to improve the quality of extracting informative features. In particular, CNN models with attention mechanisms are able to focus on the most significant fragments of network flows, which contributes to an increase in the accuracy of detecting attacks in complex IoT scenarios [1]. A number of works have proposed a combination of Inception-CNN with bidirectional recurrent networks, which provides better resistance to high-dimensional and unbalanced data [3].

In parallel, approaches focused on scalability and privacy preservation are actively being studied, in particular, federated learning methods, which allow training models in a distributed environment without centralized data collection from IoT devices [5]. Considerable attention is also paid to autoencoders and hybrid models that combine dimensionality reduction, anomaly detection, and subsequent classification of attacks, providing a compromise between accuracy and computational efficiency [6-7].

Despite the progress made, the application of deep models in real IoT environments is accompanied by a number of limitations, including high computational complexity, complexity of processing streaming data in real time, sensitivity to the imbalance of attack classes and dependence on computing infrastructure resources [2,8]. In this regard, the task of developing adaptive intrusion detection systems that combine high detection quality with computational efficiency, interpretability of solutions and suitability for practical use in heterogeneous IoT networks remains relevant.

The aim of this work is to develop an adaptive fuzzy model for anomaly detection in network IoT traffic, which combines automated formation of linguistic terms, generation of a rule base and online adaptation of parameters without full re-training.

2. Related work

The first intrusion detection systems for IoT networks were mostly based on classical machine learning algorithms and signature approaches. Although such methods provided acceptable performance for known types of attacks, their practical value decreased in the context of dynamic threat evolution, as rule and model updates were often delayed and adaptation to new attack scenarios was limited. This led to the transition to more sophisticated models capable of automatically analyzing nonlinear patterns in network traffic.

A significant area of modern research is related to the use of deep learning for the analysis of spatiotemporal characteristics of IoT traffic. In the work of Omarov et al. [9], a hybrid CNN–BiLSTM model is proposed, in which convolutional neural networks are used to extract local features, and bidirectional LSTMs are used to model temporal dependencies. This approach demonstrates a high ability to detect complex anomalies, but is accompanied by increased computational complexity and significant training time. The problem of the sensitivity of deep models to the amount of training data was analyzed in [10], where it is shown that under conditions of limited or unrepresentative sampling, the quality of deep architectures is significantly reduced compared to simpler machine learning methods.

Particular attention in modern research is paid to hybrid approaches that combine classical methods of network traffic analysis with fuzzy decision-making mechanisms. In particular, in [11], a step-by-step system for detecting anomalous IoT traffic was proposed, which integrates signature classification, traffic self-similarity analysis based on the Hurst coefficient, and fuzzy logic inference. This approach allows achieving high detection accuracy under limited computing resources, while maintaining a balance between the load on the processor and the network bandwidth. A separate class of studies is multi-level and hybrid IDS architectures, which combine several analysis methods. Alashkar et al. [12] proposed a two-level system that combines a cascaded neural network with backpropagation of the error and a CNN for analyzing pre-processed network data. A similar approach was implemented in [13], which combined unsupervised clustering IDBSCAN with a multi-core extreme learning machine HMKELM optimized by the

MTLBO algorithm. Although such solutions demonstrate high accuracy, they are sensitive to hyperparameter tuning and require significant computational resources, which makes their use in real IoT environments difficult.

An important direction is dimensionality reduction and feature selection to improve the efficiency of IDS. Xu et al. [14] proposed a system based on XGBoost with two-stage feature selection, combining bio-inspired optimization algorithms and recursive feature exclusion, supplemented by class balancing and Bayesian hyperparameter optimization. A similar approach is presented in [15], which combines a genetic algorithm for feature optimization with ensemble classification based on DT, RF, and XGBoost. Despite the performance improvement, such methods often add a separate processing stage, which reduces the adaptability of the system.

Autoencoders are considered as a universal tool for analyzing IoT traffic, combining dimensionality reduction and anomaly detection. In Alaghbari et al. [16] proposed an integrated model based on a deep autoencoder, which is used both for anomaly detection and for the formation of compact features. Comparison with the PCA and LDA methods showed comparable results, but the efficiency of autoencoders largely depends on the choice of the number of latent features and training parameters. A similar idea was used in [17], which combined smoothing and dimensionality reduction using Gaussian Pyramid with subsequent classification based on linear SVM, which requires additional transformations of numerical features.

A separate group is made up of context-oriented and applied IDS aimed at specific IoT usage scenarios. In [18], a CBCTL-IDS system for smart agriculture was proposed, which combines Extra Trees feature selection, network traffic transformation into images, and CNN ensemble transfer learning optimized by a bio-inspired algorithm. AlHayan et al. [19] developed a hybrid framework based on STL time series decomposition and deep neural networks to reduce false positives.

Ensemble and multiclassification approaches are presented in [20], which combines DT, RF, SVM, and CNN algorithms with GA and CFS-based feature selection, and in [21], which uses optimized XGBoost for binary classification and a sequential neural network for multiclass analysis. A separate direction is the integration of IDS with blockchain technologies, as shown in [22], where a deep neural network is used to detect anomalies and a blockchain to ensure data integrity and automated response to threats.

Authors in [23] introduced a behavior-based approach for detecting unknown metamorphic viruses that is resilient to code obfuscation techniques. Their method performs dynamic analysis by comparing the functional blocks of disassembled code before and after execution within a modified emulator. Unlike traditional signature-based solutions, the proposed technique identifies malware based on changes in program behavior, enabling the detection of previously unseen metamorphic malware variants and improving robustness against evasion techniques.

A promising direction for the development of IDS for IoT is the use of graph neural networks, which allow taking into account both the topological structure of the network and the dynamics of interaction between devices. In [24], the IoT network is formalized as a weighted directed graph, where nodes correspond to heterogeneous devices, and edges correspond to communication channels with telemetric characteristics. The use of Graph Attention Networks provides selective aggregation of information and increases the efficiency of detecting multi-vector attacks, while maintaining the interpretability of the results.

A separate problem of modern attack detection systems remains the limited interpretability of machine learning model solutions. In [25], an approach to detecting network attacks using Explainable Artificial Intelligence methods is proposed, which combines high-precision classification algorithms with local and global explanations of solutions. The use of XAI allows you to determine key traffic characteristics that affect decision-making, increasing confidence in IDS in critical and industrial environments.

Along with network traffic analysis methods, it is important to apply approaches to detect anomalies in information systems monitoring data. In [26], an intelligent monitoring system is considered that combines statistical time series methods with machine learning algorithms, in particular ARIMA and LSTM. This approach allows for effective detection of both point and

collective anomalies in the performance of servers and network resources, but requires prior training of models and is sensitive to changes in the nature of the data.

In general, modern intrusion detection systems for IoT are evolving from classical machine learning algorithms to complex hybrid and deep models focused on the analysis of high-dimensional and nonlinear characteristics of network traffic [27]. At the same time, most of the existing approaches are characterized by increased computational complexity, dependence on large and representative training samples, sensitivity to hyperparameter tuning, or the need to use external feature reduction methods. This emphasizes the relevance of developing consistent and computationally efficient models that can combine the formation of informative features and anomaly detection within a single approach and be suitable for practical use in resource-constrained IoT environments.

3. Adaptive fuzzy model for analyzing Internet of things traffic

The proposed model is aimed at detecting anomalous behavior in network traffic by analyzing deviations from the normal mode of operation of the information and communication system. Unlike approaches based on fixed threshold values or predefined signatures, the model implements an adaptive fuzzy mechanism, within which the formation of informative features and decision-making on the level of anomaly are integrated into a single process. The scientific novelty of the proposed approach lies in the automated formation of linguistic terms based on Fuzzy C-Means in combination with the generation of a fuzzy rule base without an expert task and a formalized rule aging mechanism, which ensures the adaptation of the model to the non-stationary nature of IoT traffic while maintaining the interpretability of solutions.

To implement the above approach, the model is formalized as a sequence of interconnected stages, including network traffic representation, linguistic variable formation, automated term set construction, fuzzy rule base generation, and adaptive fuzzy logical inference.

The input information for the analysis is network traffic, represented as a set of packets

$$P=\{p_k|k=1,\dots,K\} \quad (1)$$

where P is the set of packets of the outgoing network traffic of the ICS, p_k is the k-th packet of the outgoing stream, k is the packet index, K is the total number of packets in the flow under study.

From each packet, numerical parameters of network traffic are calculated, which are used as input features for further fuzzy analysis. These parameters are further interpreted through the linguistic variables of the model.

The assessment of the membership of input parameters to the corresponding terms of linguistic variables is carried out using membership functions, which quantitatively reflect the degree of correspondence of each input value to the specified linguistic terms.

The set of linguistic variables is given as

$$X=\{X_i, X_i+1,\dots,X_n\} \quad (2)$$

where X is a set of linguistic variables, X_i is the i-th linguistic variable characterizing the network traffic parameter, i is the index of the linguistic variable, n is the number of linguistic variables in the model. In the following, Xi denotes the linguistic variable, while xi is used to denote its current numerical value obtained from the network traffic.

The linguistic variables were constructed from normalized numerical traffic descriptors that characterize traffic intensity, packet size distribution, temporal behavior, transport-layer activity, and bidirectional flow structure. In particular, the selected feature groups included packet rate, byte rate, flow duration, inter-arrival time, average packet size, minimum and maximum packet length, standard deviation of packet length, protocol identifier, source and destination port characteristics, TCP flag statistics, and forward/backward packet counters. These features were selected because they are available or can be derived from the evaluated IoT traffic datasets, have low computational

cost, and are commonly informative for distinguishing normal IoT communication from flooding, scanning, brute-force, spoofing, and malformed-message attacks. During preprocessing, duplicate, non-informative, and highly correlated attributes were removed, while the features that preserved stable anomaly-discriminative behavior across MQTTset, IoTID20, and CICIoT2023 were retained.

Consider a linguistic variable that can take values from a term set, where l determines the number of terms. The formation of a set of linguistic variables used for network traffic analysis and corresponding to the components of the tuple was carried out on the basis of the results of the analysis of network activity obtained in the process of modeling typical attacks in a computer network.

The term set of a linguistic variable is given as

$$T_i = \{t_{ij}, t_{ij}+1, \ldots, t_{il}\} \quad (3)$$

where T_i is the term set of the i-th linguistic variable, t_{ij} is the j-th linguistic term of the variable X_i, j is the index of the linguistic term, l is the number of terms of the linguistic variable.

At the same time, only those linguistic variables that are informatively significant for describing traffic behavior without excessive detail were included in the consideration, which allowed to ensure correct consideration of the features of the functioning of various protocols of the OSI model layers.

For each linguistic variable, a term set is defined, consisting of five semantically ordered terms: “normal”, “moderately deviated”, “suspicious”, “anomalous” and “critical”. Such a term set structure allows to adequately describe both the standard modes of network operation and gradual transitions to dangerous states, which is characteristic of most network attacks and anomalies.

The number of linguistic terms was fixed at five for each input variable. This choice corresponds to the semantic interpretation of traffic states as “normal”, “moderately deviated”, “suspicious”, “anomalous”, and “critical”. Therefore, the number of fuzzy clusters in the Fuzzy C-Means procedure was also set to five. The main mechanism for forming the term set parameters and the corresponding membership functions is the Fuzzy C-Means algorithm, which is used as a method of automated selection of linguistic terms. The algorithm is fed a stream of numerical values of network traffic parameters collected in time windows of adaptive length. In the process of minimizing the objective function Fuzzy C-Means, observations are dynamically grouped into fuzzy subsets, each of which is interpreted as a separate term of the linguistic variable. The characteristic values of the terms determine the representative levels of anomaly, while the overlap areas between neighboring terms are used to form trapezoidal membership functions, which ensure a smooth transition between the values of the linguistic variable.

The general process of automated formation of linguistic terms based on the Fuzzy C-Means algorithm, including the clustering of numerical parameters of network traffic and the construction of the corresponding membership functions, is schematically presented in Fig. 1. The selected fuzzy clusters are interpreted as linguistic terms, and the areas of their overlap are used to form trapezoidal membership functions.

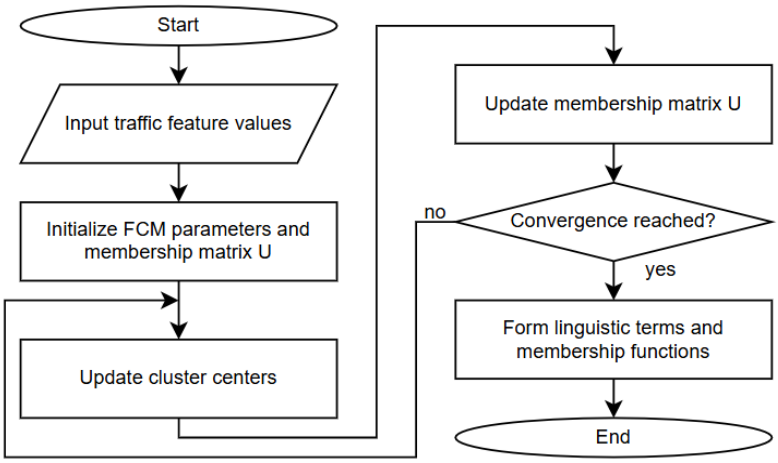

Figure 1: Formation of linguistic terms and membership functions based on the Fuzzy C-Means algorithm.

The membership function has the form:

$$\mu_{ij}(x_i): D_i \rightarrow [0,1] \tag{4}$$

where $\mu_{ij}(x_i)$ – the degree of membership of the value x_i to the term t_{ij}, x_i – the current numerical value of the parameter corresponding to the linguistic variable Xi, Di – the universal set of values of the variable Xi.

The shape of the membership functions for all terms is chosen to be trapezoidal, since it provides sufficient flexibility in modeling both stable and transient states of traffic. The parameters of the membership functions are determined directly based on the results of the Fuzzy C-Means algorithm, which minimizes subjectivity and increases the reproducibility of the results.

Since the number of linguistic terms is fixed, each fuzzy cluster formed by the Fuzzy C-Means algorithm is interpreted as a separate linguistic term of the corresponding variable.

Let the set of numerical observations of the network traffic parameter be given:

$$Z_i = \{z_{i1}, z_{i2}, \ldots, z_{iN}\} \tag{5}$$

The Fuzzy C-Means algorithm performs fuzzy clustering of this set into m clusters by minimizing the objective function:

$$J = \sum_{k=1}^{N} \sum_{j=1}^{m} u_{kj}^{q} * \|z_{ik} - c_{ij}\|^2 \tag{6}$$

where J is the value of the objective function of the Fuzzy C-Means algorithm, zik is the k-th observation of the parameter Xi, cij is the center of the jth fuzzy cluster, ukj is the degree of membership of the k-th observation to the j-th cluster, q is the algorithm's fuzziness index (q>1), N is the number of observations, m is the number of clusters.

In the experiments, the Fuzzy C-Means algorithm was configured with five clusters, corresponding to the five linguistic terms of each input variable. The fuzziness coefficient was set to q=2, the convergence threshold was set to $\varepsilon=10^{-5}$, and the maximum number of iterations was limited to 200. The membership matrix was initialized randomly, and the clustering procedure was repeated under different initial conditions to reduce sensitivity to initialization and verify the stability of the obtained cluster centers.

The adaptability of the proposed algorithm is implemented by periodically updating the parameters of term sets and the corresponding membership functions in real time. As new data on network activity is received, adaptive adjustment of the parameters of the membership functions and the corresponding characteristic values of the terms is performed without complete re-initialization of the algorithm. This allows the system to automatically adapt to changes in the

nature of traffic caused by the emergence of new services, changes in network configuration, or the evolution of attack scenarios.

After determining the linguistic variables and the corresponding membership functions, the next stage is the formation of a decision-making mechanism, which is implemented in the form of a fuzzy rule base. Based on the formed linguistic variables, the fuzzy rule base is automatically generated using the Wang–Mendel algorithm. The input data for this stage are the fuzzified feature vectors of the training sample and the corresponding values of the output linguistic variable, which is interpreted as the level of anomaly. For each training sample, an IF–THEN rule is formed, in which each variable is assigned the term for which the degree of membership is maximum.

The procedure for automatically generating a fuzzy rule base using the Wang–Mendel algorithm, including fuzzification of training samples, formation of IF–THEN rules, calculation and normalization of their weights, and elimination of conflicts between rules, is generally presented in Fig. 2. This approach allows you to form a compact and informative knowledge base without involving expert rule setting.

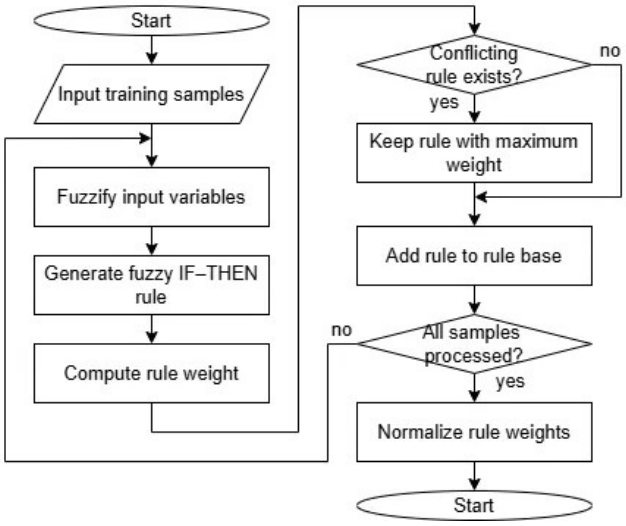

Figure 2: The process of automatic generation of a fuzzy rule base using the Wang–Mendel algorithm.

For each training sample, a fuzzy rule of the form is formed:

$$if\left(X_1 \in t_{1_{j_1}}\right) \wedge \ldots \wedge \left(X_n \in t_{n_{jn}}\right) then\, Y \in t_{yk} \tag{7}$$

where Y is the output linguistic variable “level of anomaly”.

The weight of a fuzzy rule is calculated as the product of the degrees of membership of the input and output variables, after which the weights of the fuzzy rules are normalized to ensure that the rules can be compared with each other. In case of conflicts, when the rules have the same conditions and different conclusions, only the rule with the maximum normalized weight is stored in the knowledge base:

$$w_r = \prod_{i=1}^{n} \mu_{ij}\left(x_i\right) \tag{8}$$

where w_r – weight of the r-th fuzzy rule, r – index of the fuzzy rule.

Normalization of weights ensures correct comparison of rules and stability of the conflict resolution mechanism:

$$\overline{w_r} = \frac{w_r}{\sum_{(k=1)}^{R} w_k} \tag{9}$$

where $\overline{w_r}$ is the normalized weight of the r-th fuzzy rule, R is the total number of rules.

Duplicate rules with identical antecedents and consequents are merged into a single rule. If several rules have identical antecedents but different consequents, they are treated as conflicting rules. Such conflicts are resolved by comparing the normalized rule weights: only the rule with the highest normalized weight is retained in the final knowledge base, while rules with lower confidence are discarded. As a result, the final rule base contains compact, non-contradictory, and weighted IF–THEN rules suitable for Sugeno-type inference.

The operational analysis of incoming network traffic is carried out using a fuzzy logical inference system of the Sugeno type, which provides high performance and the ability to directly calculate the numerical anomaly index. At the fuzzification stage, the current parameter values are converted into degrees of membership in the corresponding linguistic terms, then the rules are activated, and defuzzification is carried out by calculating the weighted average.

For a fuzzy logical inference system of the Sugeno type, the numerical anomaly index is defined as

$$A = \frac{\sum_{(k=1)}^{R} \overline{w_r} * y_r}{\sum_{(k=1)}^{R} \overline{w_r}} \tag{10}$$

where A is the numerical index of the network traffic anomaly level, y_r is the initial value of the r-th fuzzy rule.

To maintain the relevance of the knowledge base over time, a formalized rule aging mechanism is introduced, according to which the rule is removed in case of its prolonged inactivation or a decrease in the average weight below a given threshold value. This ensures the adaptability and stability of the hybrid network traffic analysis system in the context of the evolution of network behavior and cyber threats.

The rule aging condition is defined as

$$t_{now} - t_r^{last} > T_{age} \vee \overline{w_r} < w_{min} \tag{11}$$

where t_{now} is the current time, t^r_{last} is the time of the last rule activation, T_{age} is the limit time of rule inactivity, w_{min} is the minimum allowable value of the rule weight.

To ensure the reproducibility of the proposed model and a clear formalization of the sequence of operations, the general workflow of the fuzzy intrusion detection system is summarized in Algorithm 1.

Algorithm 1. Training, testing and online operation of the fuzzy IDS for IoT traffic

Input: dataset *D*, number of linguistic terms *l=5*, training ratio *p=0.7*, window size *W*, decision threshold θ, adaptation interval *K*.

Output: fuzzy rule base *R*, predicted labels $\hat{y}$, evaluation metrics

1. Load dataset *D* and perform data cleaning, categorical feature encoding, and normalization.
2. Split dataset *D* into training and testing subsets using stratified sampling $D \to D_{train}(p), D_{test}(1-p)$
3. Apply Fuzzy C-Means clustering to D_{train} and construct linguistic term sets for each feature.
4. Fuzzify the training data and generate the fuzzy rule base *R* using the Wang–Mendel method.
5. Configure the Sugeno-type fuzzy inference system and determine the decision threshold θ.
6. Apply the trained model to D_{test} and obtain predicted labels $\hat{y}$.
7. Compute the confusion matrix and evaluation metrics (Accuracy, Precision, Recall, F1-score).
8. Initialize a sliding window buffer of size *W* for online traffic processing.
9. While network traffic is being received do:
   9.1. Extract feature vectors and aggregate them into windows of size *W*.

9.2. Perform fuzzification and fuzzy inference to obtain the anomaly score.
9.3. Classify traffic as normal or attack using threshold θ.
9.4. Update rule activity statistics and remove inactive rules.
9.5. Every K windows, update linguistic terms and the rule base using recent data.
10. End while.

The algorithm integrates offline training and testing stages with an online traffic analysis phase, reflecting the full life cycle of the proposed model in practical IoT environments. The offline stage is used exclusively for the initial initialization of linguistic variables and the rule base, while all subsequent adaptation processes are performed online without repeated access to the training dataset. To clearly present the structure of the proposed system and the relationship between the offline training and online detection stages, a generalized block diagram of an adaptive fuzzy IoT traffic analysis system is shown in Fig. 3.

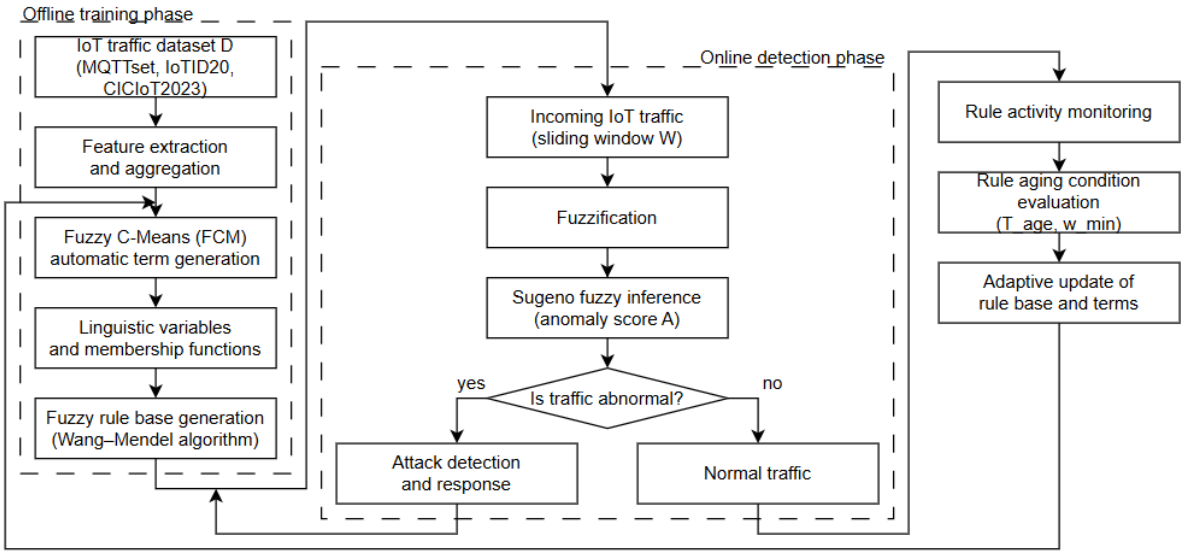

Figure 3: Structural diagram of an adaptive fuzzy intrusion detection system for IoT traffic with separation of offline training and online detection and adaptation stages.

As can be seen from Fig. 3, the offline stage is used exclusively to initialize linguistic variables, membership functions, and the fuzzy rule base based on the training data. Further work of the system is carried out in the online mode, where traffic analysis, decision-making, and adaptation of model parameters occur without repeated access to the initial data set. This approach ensures the system's suitability for operation in non-stationary IoT environments and reduces computational costs compared to methods that require periodic retraining.

4. Experimental evaluation and discussion of results

To experimentally verify the effectiveness of the proposed approach, an isolated test environment was formed that simulates a typical multi-tiered IoT infrastructure. The architecture of the environment includes the IoT device layer, the traffic collection gateway layer, and the analytical layer, where data preprocessing, feature formation, and model training and testing procedures are performed.

The IoT device layer is modeled by a set of logical nodes corresponding to sensors, surveillance cameras, smart home devices, and industrial controllers. To ensure traffic diversity, both TCP/UDP protocols and application IoT protocols, including MQTT, are used. Network packets are collected at the gateway layer using traffic mirroring and subsequent storage in a format compatible with the data sets used in the study.

The analytical layer is implemented as a separate computing node with the Python programming environment and libraries for data analysis and machine learning installed. It is at this level that the procedures for normalizing features, forming linguistic variables, training a fuzzy model, and evaluating its quality are performed. To make the experimental procedure more reproducible, the same general configuration of the adaptive fuzzy model was used for all datasets. The anomaly score produced by the Sugeno-type fuzzy inference system was normalized to the interval [0,1], and the decision threshold was set to $\theta=0.6$. Values below this threshold were interpreted as normal or weakly deviated traffic behavior, whereas values equal to or greater than the threshold were classified as anomalous. This threshold was selected because it corresponds to the transition from suspicious to anomalous traffic states in the adopted five-term linguistic scale and provided a stable balance between Precision and Recall during preliminary evaluation on the training subsets.

To ensure the representativeness of the experiments and verify the generalization ability of the model, several open IoT traffic datasets (Table 1) were used, which differ in structure, attack types, and application scenarios. The MQTTset set was used to study the specifics of attacks on the MQTT protocol, which is widely used in IoT systems with a publication messaging model. This set is appropriate for testing the effectiveness of the proposed linguistic variables in environments with a high frequency of short messages. The IOTID20 set was used for multi-class classification of attacks in heterogeneous IoT networks. It includes both network and application attacks, which allows assessing the adaptability of the model to various types of threats. For additional verification of scalability and resilience to modern attack scenarios, CICIoT2023 was used, which is characterized by a large number of features and modern types of malicious activity. The use of this set allows us to evaluate the behavior of the model in conditions of high-dimensional and unbalanced data.

Table 1
Characteristics of the used data sets and distribution of records by network traffic categories and attack types

Dataset	Category/type of attack	Number of records
MQTTset	DoS via Flooding	130 223
	MQTT Publish Flood	613
	SlowITe	9 202
	Malformed MQTT data	10 924
	Brute Force	14 501
IoTID20	Benign	40 073
	Mirai	415 677
	Scan	75 265
	DoS	59 391
	MITM (ARP Spoofing)	35 377
CICIoT2023	DDoS	33 984 560
	DoS	8 090 738
	Mirai	2 634 124
	Benign	1 098 195
	Spoofing	486 504
	Recon	354 565
	Web attacks	24 829
	Brute Force	13 064

For online traffic aggregation, a fixed sliding window of $W=100$ traffic records was used. The adaptation of linguistic terms and the fuzzy rule base was performed every $K=50$ windows using the most recent traffic observations. The rule aging mechanism was configured with the inactivity limit $T_{age}=500$ windows and the minimum allowable normalized rule weight $w_{min}=10^{-3}$. A rule was

removed from the knowledge base if it had not been activated for longer than the specified inactivity interval or if its normalized weight decreased below the minimum threshold. These settings were applied uniformly to MQTTset, IoTID20, and CICIoT2023 in order to ensure comparable experimental conditions across datasets. At the first stage, all data sets were brought to a unified format. Categorical features were converted into a numerical representation, and numerical parameters were normalized to a single range of values. To reduce the impact of noise, packet aggregation was used in fixed-length time windows, which corresponds to the streaming nature of IoT traffic.

Based on the selected network traffic parameters, linguistic variables were formed, for which term sets and trapezoidal membership function parameters were automatically determined using the Fuzzy C-Means algorithm. This approach made it possible to avoid manual threshold setting and reduce the subjective influence of expert assessments.

Training and testing of the proposed model were performed separately for each dataset, following a single experimental procedure and the same parameter settings for all three datasets. At the first stage, a stratified sample division was performed for all data sets in the ratio of 70% for training and 30% for testing, which ensured the preservation of the initial class proportions and minimized the impact of data imbalance on the experimental results. For the MQTTset set, the training set was formed from 70% of the traffic of each attack type, including 91,156 Denial of Service (DoS) attack packets, 429 MQTT Publish Flood packets, 6,441 SlowITe packets, 7,647 malformed MQTT message packets, and 10,151 brute force authentication attack packets. The remaining 30% of the corresponding data was used as a test set to evaluate the model's ability to detect protocol-oriented anomalies. For the IoTID20 set, training was performed on a multi-class sample containing 28,051 normal traffic records, as well as 290,974 Mirai attack records, 52,686 Scan records, 41,574 DoS records, and 24,764 MITM (ARP Spoofing) records, which corresponds to 70% of the total number of records in each class. The test set was formed from the remaining 30% of the data and was used to independently assess the quality of the classification. In the case of the CICIoT2023 set, 70% of the records of each generalized attack category were used for training, including 23,789,192 records of DDoS attacks, 5,663,517 records of DoS attacks, 1,843,887 records related to the Mirai botnet, 768,737 records of legitimate traffic, as well as 340,553 records of Spoofing attacks, 248,196 records of Recon, 17,380 records of Web-based attacks, and 9,145 records of brute force attacks. The remaining 30% of the data of each category was used to test the model under conditions of high dimensionality and variety of attacks.

Directly during the training process, the adaptation of the term set parameters and the adjustment of the fuzzy inference rules were performed in accordance with the statistical characteristics of the network traffic. To assess the stability of the obtained results, the experiments were repeated with different initial clustering conditions, which allowed us to check the convergence of the algorithm and reduce the influence of random factors.

The model was tested on delayed samples for each of the data sets. The main performance indicators were accuracy, completeness, F1-measure and the level of false positives, and for multi-class scenarios, the discrepancy matrix was additionally analyzed in order to identify the most problematic attack classes.

Table 2 displays the results of the first stage of testing the model on samples for each of the used data sets in the form of an error matrix. For the MQTTset set, the largest number of true positive and true negative responses is observed with a minimum number of false positive and false negative decisions, which indicates the high ability of the model to correctly distinguish between normal and anomalous MQTT traffic. This is due to the protocol-oriented nature of the data set and the relatively limited variety of attack scenarios. For the IoTID20 set, the number of false positives increases slightly, which is explained by the presence of several types of attacks with similar behavioral characteristics, but the ratio of TP and TN to FP and FN remains quite high.

In the case of CICIoT2023, the largest absolute values of FP and FN were recorded, which is expected given the significant volume of data, large number of classes and high dimensionality of

features. At the same time, the predominance of true responses confirms the ability of the model to scale to large and complex data sets without significant loss of accuracy.

Table 2
Test results (Test 1)

Dataset	TP	TN	FP	FN
MQTTset	152840	89214	2146	1993
IoTID20	552310	97845	6284	5231
CICIoT2023	42318905	8764120	412486	398772

Table 3 shows the results of the retest of the model performed under different initial conditions of clustering and initialization of parameters. Comparison of the values of TP, TN, FP and FN with the results of the first test shows insignificant fluctuations of the indicators for all data sets, which indicates the stability and convergence of the proposed approach. For the MQTTset set, the model maintains a high level of true activations with minimal changes in the number of errors, which confirms its reliability for protocol-oriented IoT scenarios.

A similar trend is observed for the IoTID20 set, where variations in the indicators do not affect the overall quality of the classification. For CICIoT2023, insignificant changes in the absolute values of FP and FN are a consequence of the large amount of data, however, the ratio between true and false solutions remains practically unchanged, which confirms the reproducibility of the experimental results.

Table 3
Test results (Test 2)

Dataset	TP	TN	FP	FN
MQTTset	152615	89347	2011	2220
IoTID20	549982	100126	6037	5525
CICIoT2023	42107694	8982431	389275	414883

The summarized table displays the averaged values of the error matrices obtained from several independent runs of experiments. This approach allows to reduce the influence of random factors and provide a more objective assessment of the model's effectiveness.

The best generalized results were recorded for the MQTTset set, which confirms the effectiveness of the proposed approach for analyzing protocol-oriented IoT traffic. For the IoTID20 and CICIoT2023 sets, the model demonstrates slightly lower, but stable indicators, which is due to a greater variety of attacks, the presence of similar classes and high dimensionality of features.

Table 4
Generalized test results

Dataset	TP	TN	FP	FN
MQTTset	152728	89281	2079	2107
IoTID20	551146	98986	6161	5378
CICIoT2023	42213300	8873276	400881	406828

The results obtained indicate that the proposed model provides consistently high attack detection rates on all used data sets. The highest accuracy was recorded on the MQTTset set, which confirms the effectiveness of the approach for protocol-oriented IoT scenarios. On the IoTID20 and CICIoT2023 sets, the model demonstrated slightly lower, but stable metric values, which is due to a greater variety of attacks and high dimensionality of features. In general, the results of the

experimental study confirm the feasibility of using the proposed fuzzy approach with automated term set formation for anomaly detection in IoT networks and its suitability for use in real resource-constrained environments.

The Accuracy indicator reflects the total proportion of correctly classified samples relative to the total number of records in the test sample and characterizes the overall correctness of the model regardless of class affiliation.

The Precision indicator characterizes the accuracy of attack detection and is defined as the ratio of the number of true positives to the total number of cases classified by the model as an attack. High values of this indicator indicate a low level of false positives.

The Recall indicator (completeness) reflects the ability of the model to detect actual attacks and is defined as the proportion of true positives among all real attack cases. A high Recall value means that the model misses the minimum number of attacks. The F1-score indicator is a harmonious average between Precision and Recall and is used for a generalized assessment of the quality of classification, especially in conditions of class imbalance. It allows you to simultaneously take into account both the accuracy of attack detection and the completeness of their recognition.

According to the results of testing the proposed model for all used data sets, high values of the main performance indicators, presented in percentage format, were recorded. For the MQTTset set, the overall classification accuracy is 98.30%, with the attack detection accuracy (Precision) and completeness (Recall) reaching 98.66% and 98.64%, respectively, and the F1-score value is 98.65%, which indicates a balanced model performance without a significant bias between false positives and false negatives. For the IoTID20 set, the model demonstrated an overall accuracy of 98.26%, with slightly higher Precision (98.89%) and Recall (99.03%), indicating the high ability of the model to correctly detect most attacks even in conditions of multi-class data structure.

The F1-score value, which is 98.96%, confirms the consistency of the accuracy and completeness results. The highest values of the metrics are recorded for the CICIoT2023 dataset, where the overall classification accuracy is 98.44%, and the Precision and Recall indicators reach 99.06% and 99.05%, respectively.

The F1-score value of 99.05% indicates the effective operation of the model even under conditions of high dimensionality of features and a significant variety of attacks. Overall, the results obtained confirm that the proposed model provides consistently high performance indicators for all studied datasets, and the Accuracy, Precision, Recall and F1-score values exceeding 98% indicate its suitability for practical application in real IoT environments with heterogeneous and intensive network traffic.

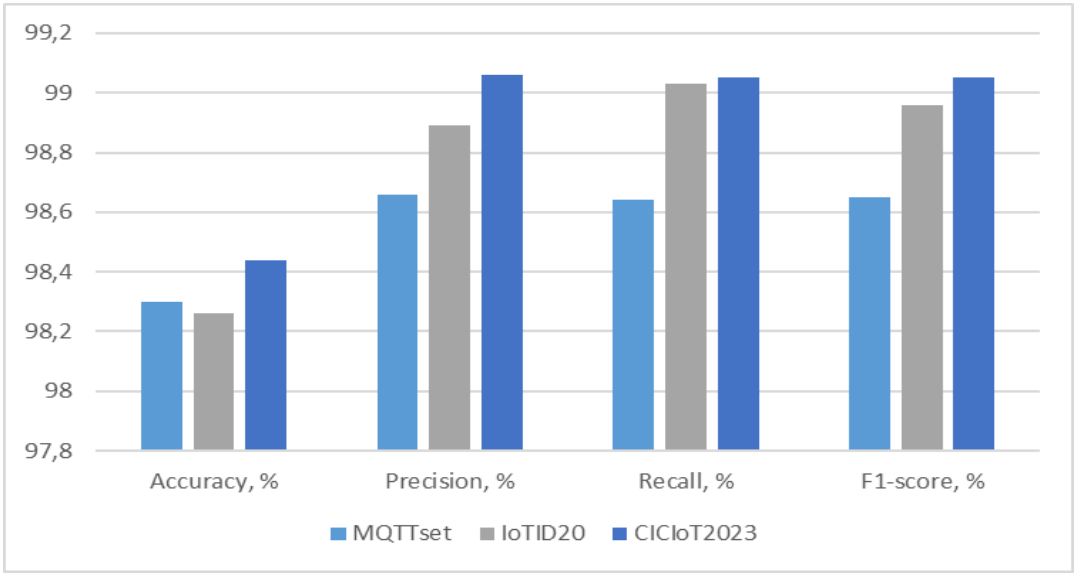

Figure 4: Comparative chart of Accuracy, Precision, Recall and F1-score values for the MQTTset, IoTID20 and CICIoT2023 datasets.

The results obtained demonstrate consistently high performance indicators of the proposed model for all studied datasets and confirm its ability to generalize in conditions of heterogeneous and intensive IoT traffic.

5. Conclusions

The paper proposes an adaptive fuzzy model for detecting anomalies in the network traffic of the Internet of Things, focused on the analysis of non-stationary and high-dimensional data in resource-constrained environments. Unlike traditional signature and most modern deep approaches, the developed model combines automated formation of informative features and a decision-making procedure within a single fuzzy mechanism, which ensures both interpretability of results and computational efficiency.

The scientific novelty of the work lies in the integration of the Fuzzy C-Means algorithm for automated formation of linguistic terms, generation of a fuzzy rule base without an expert assignment, and implementation of a formalized rule aging mechanism. This approach allows the model to adapt to changes in the network traffic profile and the evolution of attacks without complete re-initialization, which is fundamentally important for real IoT scenarios with dynamic network behavior.

The experimental evaluation was performed on three different open datasets — MQTTset, IoTID20 and CICIoT2023, which differ in attack types, scale and complexity. The obtained results confirm the consistently high performance indicators of the proposed model for all studied scenarios. The values of Accuracy, Precision, Recall and F1-score for all datasets exceed 98%, which indicates the high ability of the model to correctly distinguish between normal and anomalous traffic even under conditions of significant class imbalance and high dimensionality of features. The highest indicators were recorded for the MQTTset set, which confirms the effectiveness of the approach for protocol-oriented IoT environments, while the results for IoTID20 and CICIoT2023 demonstrate good generalization ability and scalability of the model.

Additional analysis of the results of repeated experiments with different initial clustering conditions showed insignificant fluctuations in the indicators, which confirms the convergence of the algorithm and the reproducibility of the obtained results. This indicates the model's resistance to random factors and the correctness of the chosen experimental procedure.

In general, the research results confirm the feasibility of using adaptive fuzzy approaches with automated term set generation for anomaly detection problems in IoT networks. The proposed model combines high detection quality, interpretability of solutions, and suitability for operation in resource-constrained conditions, which makes it promising for practical implementation in IoT security monitoring systems.

Further research can be aimed at expanding the model by integrating contextual information about network services, adapting rule aging mechanisms to long-term traffic changes, and combining the proposed fuzzy approach with distributed and federated learning schemes to increase the scalability and confidentiality of data processing in large IoT infrastructures.

Declaration on Generative AI

During the preparation of this work, the author(s) used Grammarly in order to check grammar, spelling, and improve the linguistic flow and style of the text. Additionally, the author(s) used Gemini to assist with the correct formatting and syntax of mathematical notations. After using these tools, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

References

[1] A. Momand, S. U. Jan, N. Ramzan, ABCNN-IDS: Attention-Based Convolutional Neural Network for Intrusion Detection in IoT Networks, Wireless Personal Communications 136 (2024) 1981–2003. doi:10.1007/s11277-024-11260-7.

[2] D. Adhikari, W. Jiang, J. Zhan, D. B. Rawat, A. Bhattarai, Recent advances in anomaly detection in Internet of Things: Status, challenges, and perspectives, Computer Science Review 54 (2024). doi:10.1016/j.cosrev.2024.100665.

[3] K. Yang, J. Wang, M. Li, An improved intrusion detection method for IIoT using attention mechanisms, BiGRU, and Inception-CNN, Scientific Reports 14 (2024) 19339. doi:10.1038/s41598-024-70094-2.

[4] Y. Zhang, R. C. Muniyandi, F. Qamar, A review of deep learning applications in intrusion detection systems: Overcoming challenges in spatiotemporal feature extraction and data imbalance, Applied Sciences 15 (3) (2025) 1552. doi:10.3390/app15031552.

[5] R. W. Anwar, M. Abrar, A. Salam, F. Ullah, Federated learning with LSTM for intrusion detection in IoT-based wireless sensor networks: A multi-dataset analysis, PeerJ Computer Science 11 (2025) e2751. doi:10.7717/peerj-cs.2751.

[6] R. Jablaoui, O. Cheikhrouhou, M. Hamdi et al., Deep learning enabled intrusion detection system for IoT security, Journal of Wireless Communications and Networking (2025) 66. doi:10.1186/s13638-025-02477-6.

[7] M. Berhili, O. Chaieb, M. Benabdellah, Intrusion detection systems in IoT based on machine learning: A state of the art, Procedia Computer Science 251 (2024) 99–107. doi:10.1016/j.procs.2024.11.089.

[8] M. A. Alsoufi, M. M. Siraj, F. A. Ghaleb, M. Al-Razgan, M. S. Al-Asaly et al., Anomaly-based intrusion detection model using deep learning for IoT networks, Computer Modeling in Engineering & Sciences 141 (1) (2024) 823–845. doi:10.32604/cmes.2024.052112.

[9] B. Omarov, O. Auelbekov, A. Suliman, A. Zhaxanova, CNN-BiLSTM hybrid model for network anomaly detection in Internet of Things, International Journal of Advanced Computer Science and Applications 14 (3) (2023). doi:10.14569/IJACSA.2023.0140349.

[10] B. Velichkovska, A. Cholakoska, V. Atanasovski, Machine learning based classification of IoT traffic, Radioengineering 32 (2) (2023) 256–263. doi:10.13164/re.2023.0256.

[11] Petliak, N., Klots, Y., Karpinski, M., Titova, V., Tymoshchuk, D. Hybrid system for detecting abnormal traffic in IoT. 3rd International Workshop on Computer Information Technologies in Industry 4.0, CITI 2025. CEUR Workshop Proceedings, 2025, 4057, pp. 1–17.

[12] T. S. Alashkar, Hybrid IDS architecture for IoT security enhancing threat detection with CPBNN and CNN models, International Journal of Advanced Technology and Engineering Exploration 11 (120) (2024) 1579–1591. doi:10.19101/IJATEE.2024.111100172.

[13] R. S. Ramya, S. Jayanthy, A methodological framework to hybrid machine learning for detecting unusual cyberattacks in Internet of Things, IET Information Security (2025). doi:10.1049/ise2/8381148.

[14] B. Xu, L. Sun, X. Mao, R. Ding, C. Liu, IoT intrusion detection system based on machine learning, Electronics 12 (20) (2023) 4289. doi:10.3390/electronics12204289.

[15] B. Seyedi, O. Postolache, Securing IoT communications via anomaly traffic detection: Synergy of genetic algorithm and ensemble method, Sensors 25 (13) (2025) 4098. doi:10.3390/s25134098.

[16] K. A. Alaghbari, H.-S. Lim, M. H. M. Saad, Y. S. Yong, Deep autoencoder-based integrated model for anomaly detection and efficient feature extraction in IoT networks, IoT 4 (3) (2023) 345–365. doi:10.3390/iot4030016.

[17] R. A. Zidan, G. Karraz, Towards an efficient Internet of Things intrusion detection by using support vector machine, Baghdad Science Journal 22 (5) (2025). doi:10.21123/bsj.2024.11067.

[18] H. Zhou, H. Zou, P. Zhou, Y. Shen, D. Li, W. Li, CBCTL-IDS: A transfer learning-based intrusion detection system optimized with the Black Kite algorithm for IoT-enabled smart agriculture, IEEE Access 13 (2025) 46601–46615. doi:10.1109/ACCESS.2025.3550800.

[19] A. AlHayan, J. Al-Muhtadi, A hybrid STL-deep learning framework for behavioral-based intrusion detection in IoT environments, Applied Sciences 15 (12) (2025) 6421. doi:10.3390/app15126421.
[20] R. Y. Bukhowah, A. K. Bu Dookhi, M. Frikha, Enhanced IoT security using machine learning technology, International Journal of Advanced Computer Science and Applications 16 (9) (2025). doi:10.14569/IJACSA.2025.0160971.
[21] F. S. Alsubaei, Smart deep learning model for enhanced IoT intrusion detection, Scientific Reports 15 (2025) 20577. doi:10.1038/s41598-025-06363-5.
[22] S. A. R., J. Katiravan, Enhancing anomaly detection and prevention in Internet of Things (IoT) using deep neural networks and blockchain based cyber security, Scientific Reports 15 (2025) 22369. doi:10.1038/s41598-025-04164-4.
[23] O. Savenko, S. Lysenko, A. Nicheporuk, B. Savenko, Approach for the unknown metamorphic virus detection. In: Proceedings of the 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS 2017), Bucharest, Romania, September 21–23, 2017, pp. 71–76.
[24] M. Stetsiuk, Y. Klots, D. Tymoshchuk, M. Karpinski, N. Petliak. Detection of multi-vector attacks in IoT networks: a graph attention network-based approach. 5th International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP-2025). CEUR Workshop Proceedings, 2025, 4146, pp. 1–18.
[25] D. Tymoshchuk, A. Sverstiuk, Y. Klots, N. Petliak, V. Titova. An explainable artificial intelligence approach for detecting network attacks. Advanced AI in Explainability and Ethics for the Sustainable Development Goals (ExplAI-2025). CEUR Workshop Proceedings, 2025, 4141, pp. 38–51.
[26] Y. Klots, V. Titova, N. Petliak, D. Tymoshchuk, N. Zagorodna. Intelligent data monitoring anomaly detection system based on statistical and machine learning approaches. Cyber Security and Data Protection (CSDP-2025). CEUR Workshop Proceedings, 2025, 4042, pp. 80–89.
[27] T. Hovorushchenko, S. Aleksov, S. Talapchuk, O. Shpyluk, and V. Magdin, “Overview of the Methods and Tools for Situation Identification and Decision-Making Support in the Cyberphysical System 'Smart House',” *Computer Systems and Information Technologies*, no. 4, pp. 20–26, 2022. doi:10.31891/csit-2022-4-3.