

# Logical inference models based on fuzzy production rules for intelligent cyberthreat detection systems

Yuliia Kostiuk<sup>1,†</sup>, Pavlo Skladannyi<sup>1,2,\*,†</sup>, Karyna Khorolska<sup>1,†</sup>, Bohdan Bebashko<sup>1,†</sup> and Volodymyr Sokolov<sup>1,†</sup>

<sup>1</sup>Borys Grinchenko Kyiv Metropolitan University, Bulvarno-Kudryavska Str., 18/2, Kyiv, 04053, Ukraine

<sup>2</sup>Institute of Mathematical Machines and Systems Problems of the National Academy of Sciences of Ukraine, Ac. Glushkov Ave., 42, Kyiv, 03680, Ukraine

## Abstract

The article proposes an approach to building logical inference models in intelligent cyber threat detection systems based on fuzzy production rules. The main idea is to combine a classic rule-based mechanism (a system based on production rules) with Explainable Artificial Intelligence (XAI) methods, in particular SHapley Additive exPlanations (SHAP) and Local Interpretable Model-agnostic Explanations (LIME), to ensure transparency in decision-making. The developed model implements a fuzzy interpretation of knowledge about attack signs, allowing inference even in cases of incomplete or uncertain input data. The paper presents the structure of the production knowledge base, the defuzzification mechanism, and an example of applying the model to detect a phishing attack with a step-by-step logic for processing input information. A hybrid architecture is proposed that allows the combination of rule-based inference with Machine Learning (ML) methods, ensuring adaptability and increased accuracy. The modeling results demonstrate the effectiveness of this approach for cybersecurity tasks in dynamic environments. The proposed model can be integrated into existing information security systems, such as Security Information and Event Management (SIEM) solutions, Intrusion Detection Systems (IDSs), or cyber incident analysis platforms, to inform explainable decisions regarding the threat level. Modeling results on CICIDS-2017 and UNSW-NB15 showed an accuracy of over 95%, with support for interpretability of decisions through SHAP and LIME modules.

## Keywords

logical inference, fuzzy logic, fuzzy production rule, cyber threat, explainable artificial intelligence, XAI, SHAP, LIME, rule-based system, fuzzy inference system, FIS, SIEM, machine learning, decision making, intelligent system

## 1. Introduction

In the context of the growing complexity of information systems and the evolution of threats in cyberspace, modern cybersecurity must respond to multi-vector attacks under conditions of high dynamism, uncertainty, and limited decision-making time [1, 2, 3]. This necessitates the creation of adaptive intelligent systems (ISs) capable of autonomous analysis, anomaly detection, and recommendation generation based on incomplete, contradictory, or fuzzy data.

One practical approach to modeling decision-making processes under such conditions is the use of fuzzy logic in combination with production rules [1, 4, 5], which enables the implementation of flexible logical inference mechanisms. In particular, fuzzy production knowledge bases are capable of reflecting subjective expert judgments, the ambiguity of risk assessments, and the situational variability of context

CMiGIN'26: Fifth International Workshop on Conflict Management in Global Information Networks, June 26–27, 2026, Krakow, Poland

\*Corresponding author.

†These authors contributed equally.

✉ y.kostiuk@kubg.edu.ua (Y. Kostiuk); p.skladannyi@kubg.edu.ua (P. Skladannyi); k.khorolska@kubg.edu.ua (K. Khorolska); b.bebeshko@kubg.edu.ua (B. Bebashko); v.sokolov@kubg.edu.ua (V. Sokolov)

🌐 <https://eportfolio.kubg.edu.ua/teacher/3822> (Y. Kostiuk); <https://pavlo-skladannyi.github.io/> (P. Skladannyi);

<https://eportfolio.kubg.edu.ua/teacher/3678> (B. Bebashko); <https://volodymyr-sokolov.github.io/> (V. Sokolov)

🆔 0000-0001-5423-0985 (Y. Kostiuk); 0000-0002-7775-6039 (P. Skladannyi); 0000-0003-3270-4494 (K. Khorolska); 0000-0001-6599-0808 (B. Bebashko); 0000-0002-9349-7946 (V. Sokolov)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

[6, 7]. Such systems are suitable for implementing interpreted inference, which is particularly relevant in the context of introducing XAI in the field of critical information infrastructure security.

With cyberattacks becoming increasingly complex and frequent, modern cybersecurity approaches are relying more heavily on Artificial Intelligence (AI) technologies to detect new threats adaptively [8]. However, among existing solutions, there is an acute problem of explainability—the ability of an AI system to justify its decisions [9, 10]. This is critically important for practical use in incident response systems, security audits, and building trust among specialists. In this regard, a relevant area of research is the development of intelligent and simultaneously explainable cyber threat detection systems that combine the advantages of logical inference with XAI methods. This approach is supported by current trends in AI-based cybersecurity frameworks, particularly in line with initiatives such as DARPA and IBM Watson for Cybersecurity, as well as recommendations from ENISA and NIST on transparency in AI for cybersecurity.

Most modern IDSs based on deep learning, e.g., convolutional neural networks (NNs), transformers, demonstrate high accuracy but remain “black boxes” in terms of explaining their results [11, 12, 13]. This makes it difficult to trust such models in critical areas of cybersecurity, where both accuracy and comprehensibility of decisions are required for analysts, audits, and security policy formation [14, 15]. Thus, there is an urgent need to develop models that integrate intelligent data processing with a logically sound and transparent inference mechanism, focusing on practical applications in operational incident response systems.

Despite significant achievements in the development of decision support systems based on fuzzy logic, modern threats require a deeper semantic integration of knowledge, accounting for fuzzy similarity/difference relations, and support for adaptive knowledge updating in real-time [16]. These aspects determine the relevance of creating a new generation of logical inference architecture capable of functioning in a changing cyber threat environment, while considering the high requirements for accuracy, consistency, and explainability of results. The hypothesis is put forward that the combination of fuzzy production rules with XAI modules (in particular, LIME) allows for a significant increase in the interpretability and accuracy of logical inference when detecting cyber threats in complex information and communication systems.

The scientific novelty lies in the formalization of fuzzy logical inference, the explanation of decisions based on local and global SHAP/LIME models, and their application in hybrid response systems.

A logical inference model based on fuzzy production rules is proposed, designed for use in intelligent cyber threat detection systems. The model architecture supports the structuring of semantic knowledge, the hybridization of compositional and situational approaches to inference, and the implementation of threat prioritization mechanisms based on context analysis. The results can be integrated into modules of modern IDS/SIEM solutions, increasing the efficiency and stability of cyber defense platforms.

The application of AI technologies in the field of cyber defense enables the implementation of systems capable of autonomous analysis of object behavior, anomaly detection, and real-time decision-making. In this work, logical inference models are supplemented with XAI components, specifically the LIME and SHAP methods, which enable the explanation of the system’s conclusions in a user-friendly manner. The possibility of adapting production rules using continual learning mechanisms based on event flow analysis is also considered.

## 2. Literature review

In modern research on intelligent cyber threat detection systems, fuzzy logic inference methods are widely employed to interpret fuzzy, incomplete, or inaccurate information effectively.

In [1] presented a fuzzy IDS system for detecting Distributed Denial-of-Service (DDoS) attacks, which uses feature selection based on InfoGain and FIS inference. The applied triangular and trapezoidal functions achieved 91.1% accuracy and resulted in only 0.006% false positives. The study in [2] conducted a comprehensive review of DDoS attacks, focusing on fuzzy detection methods. They classified modern attacks and clustered defense strategies, showing that fuzzy IDS is a promising direction in combating

new threats.

Authors of [6] developed the FLSec RPL methodology, a fuzzy IDS scheme designed to protect IoT networks using the RPL protocol, aiming to prevent DIO neighbor suppression attacks. According to experiments, the system's accuracy reaches 99.7% on the NSL KDD dataset and 98.4% on the NSW NB15 dataset. The FLSec RPL system addresses the challenges of distribution, scalability, and diversification of attacks in IoT by implementing both local and global fuzzy decision-making. In [7] was developed a new hybrid fuzzy NN based on CUSUM analysis for the simultaneous detection of HTTP, TCP SYN, DNS flood, and SUB DDoS attacks in cloud environments. The system demonstrated an average accuracy of 95%, surpassing traditional IDS ( $\approx 57\%$ ).

Another example is the system developed in [17], which utilizes fuzzy logic control to inform decisions following incident detection. FIS in MATLAB processes input variables ("attack type," "goal," and "target") and provides recommendations for response (hardware/software/user actions). Modeling confirmed the adequacy and speed of this approach in crisis conditions after an attack.

### 3. Research methods

The research methods are based on the integration of fuzzy set theory, production rules, knowledge engineering, and situational analysis for modeling logical inference under uncertainty [1, 2, 17]. Fuzzy set theory is used to represent incomplete or fuzzy information about objects, events, and incidents, while production rules implement inference according to the IF-THEN scheme using fuzzy terms [4, 7]. Situational and compositional approaches ensure the adaptability of logical inference to the dynamics of the threat context [6, 18]. To improve accuracy in conditions of conflicting or partially coinciding data, fuzzy similarity and difference relations are applied.

Knowledge engineering encompasses automated rule formation, expert surveys, and the construction of knowledge bases that are free from redundancy and inconsistency [9, 14]. The methodology is implemented in the FuzExCop (Fuzzy Expert Coprocessor) software environment, a logical inference support system featuring a graphical interface and the ability to simulate cyber incidents.

The developed models were verified using publicly available datasets: CICIDS-2017 (Canadian Institute for Cybersecurity IDS, 2017) [19] and UNSW-NB15 (University of New South Wales Network-based dataset, 2015) [20], which contain representative examples of regular traffic and attacks [10, 21, 22]. Effectiveness was evaluated using standard metrics: accuracy, recall, F1-score, and real-time response latency. An accuracy of 96.2%, an F1-score of 94.8%, and an average decision latency of 28 ms were obtained, indicating the system's suitability for real-time applications [11, 12, 16].

### 4. Main material

One of the key challenges for intelligent cyber defense systems is the processing of fuzzy, incomplete, and conflicting information in real time [2, 7, 17]. In this context, knowledge representation models that enable situationally adaptive logical inference in a heterogeneous information environment are particularly relevant [4, 23]. Among the most common knowledge representation models used in intelligent fuzzy data processing systems are: production models, semantic networks, and frame structures [9, 14]. Despite specific differences, these models can be reduced to a production form for further logical inference, which significantly simplifies the implementation of inference mechanisms in cyber defense environments.

The production model of knowledge was chosen as the basis due to its flexibility, ease of updating, the possibility of automating rule formation, and the ability to integrate with XAI modules [6, 24]. However, traditional mechanisms of compositional and situational inference, implemented through classical logical operations AND and OR, demonstrate low sensitivity to the multidimensional structure of situations [18]. This necessitates the use of fuzzy similarity and difference metrics that can account for the weight coefficients of features, degrees of consistency, and individual influences of each factor in complex situational models.

The article proposes an improved method of fuzzy logical inference in production knowledge bases, based on the Euclidean metric of distance between situations and the assessment of the degree of similarity [11, 12]. For each input situation, a feature vector is formed, and the degree of correspondence with reference templates is determined as

$$D(s_i, s_j) = \sqrt{\sum_{k=1}^n w_k (1 - a_k)^2}, a_k \in [0; 1], \quad (1)$$

where  $w_k$  is the weight coefficient of the  $k^{\text{th}}$  feature,  $a_k$  is the degree of similarity according to this feature.

Alternatively, the degree of similarity between situations can be determined through a generalized fuzzy similarity function

$$D(s_i, s_j) = 1 - \sum_{k=1}^n w_k |a_k - b_k|, a_k, b_k \in [0; 1]. \quad (2)$$

These functions provide flexible control of feature priorities and support scalability to high-dimensional spatial attack profiles [10, 16]. The proposed approach enables the formalization of situation-oriented inference in threat detection systems, taking into account the weight of factors, multidimensional similarity, and dynamic updating of knowledge bases [8, 25]. In addition, a method for the automated construction of production bases of fuzzy knowledge is proposed, considering the cognitive characteristics of expert thinking and information processing [21], which reflect the natural logic of human risk assessment. This approach enables the implementation of a hybrid model of intelligent inference, combining expert knowledge structures with mechanisms for adaptive response to new types of attacks and anomalies.

In the development of intelligent cyber threat detection systems based on fuzzy production knowledge bases, there is a need to establish effective metrics for measuring similarity and difference between fuzzy situations. These metrics play a key role in implementing situational logical inference, ensuring the comparison of the current situation with basic attack patterns in feature spaces where uncertainty and fuzziness prevail. Since calculating Euclidean distance requires square root operations, implementing it in a hardware environment (e.g., a fuzzy processor or FPGA) is complicated due to its resource intensity.

In this regard, it is advisable to use a modified Hamming metric as a measure of fuzzy approximation of situations. It enables comparisons to be made without complex calculations, which is particularly relevant when implementing models in real-time within limited computing resources. The degree of difference between situations  $S_i$  and  $S_j$  is determined by

$$D(S_i, S_j) = \sum_{k=1}^n w_k |a_k - b_k|, a_k, b_k \in [0; 1], \quad (3)$$

where  $a_k$  and  $b_k$  are the values of the degrees of membership of the corresponding feature for situations  $S_i$  and  $S_j$ . In general, this metric is interpreted as a fuzzy difference relation, which allows for qualitative differentiation between images of situations.

Similarly, an inverse function is proposed to formalize the fuzzy relation of similarity (tolerance). It is used to estimate the degree of closeness of situations, taking into account the importance of features and fuzzy estimates

$$R(S_i, S_j) = 1 - D(S_i, S_j). \quad (4)$$

These relations can be utilized in the stages of construction, learning, and logical inference in fuzzy knowledge bases implemented as production rules.

Let the fuzzy rule  $R_q$  in the form of a product have the form

$$\text{IF } x_1 \text{ is } A_1^q \text{ AND } x_2 \text{ is } A_2^q \text{ AND } \dots \text{ AND } x_n \text{ is } A_n^q \text{ THEN } y \text{ is } B^q, \quad (5)$$

where  $A_k^q \subseteq [0, 1]$  is a fuzzy set for the  $k^{\text{th}}$  input variable,  $B^q$  is the output term set (for example, low, medium, high threat levels).

For each rule  $R_q$  the degree of its activation is determined as

$$\mu_{R_q}(x_1, x_2, \dots, x_n) = T(\mu_{A_1^q}(x_1), \mu_{A_2^q}(x_2), \dots, \mu_{A_n^q}(x_n)), \quad (6)$$

where  $T()$  is the  $t$ -standard, e.g., minimum:  $T(a_1, \dots, a_n) = \min(a_1, \dots, a_n)$ .

Let each rule  $R_q$  generate an output set  $B^q$ , modified by the activation degree  $\mu_{R_q}$  after activation. After aggregating the results for all rules

$$\mu_Y(y) = \bigvee_{q=1}^Q (\mu_{R_q} \wedge \mu_{B^q}(y)), \quad (7)$$

where  $\vee$  is the  $c$ -union operation (maximum), and  $Q$  is the number of rules in the knowledge base.

The formula for the initial value, according to the Mamdani method (center of gravity), for defuzzification of the result, which allows moving from a fuzzy estimate to a clear answer that a response system or analyst can interpret

$$y^* = \frac{\int y \mu_Y(y) dy}{\int \mu_Y(y) dy}, \quad (8)$$

where  $\mu_Y(y)$  is the aggregated membership function.

When a new, unknown situation  $S^*$ , is detected that does not correspond to any of the existing rules (i.e.  $\forall q : \mu_{R_q}(S^*) < \theta$ , where  $\theta$  is the threshold value), a new rule is formed

$$R_{\text{new}} : \text{IF } x_1 \text{ is } A_1^* \text{ AND } \dots \text{ THEN } y \text{ is } B^*, \quad (9)$$

where sets  $A_k^*$  are formed based on a fuzzy coverage of the feature space of the situation  $S^*$ , and  $B^*$  is an estimate provided by an expert or determined by context.

To explain the decision, feature importance metrics based on SHAP are integrated

$$\phi_k = E_{S \subseteq N \setminus \{k\}} [f(S \cup \{k\}) - f(S)], \quad (10)$$

where  $\phi_k$  is the contribution of feature  $x_k$  to the final decision, and  $f(S)$  is a logical inference function over a subset of features  $S$ .

Thus, the general model of intelligent fuzzy logical inference in a cyber threat detection system, taking into account production rules, situation similarity, heuristic learning, and XAI, can be represented by the following functionality

$$y^* = \text{Defuzzify} \left( \bigvee_{q=1}^Q \left[ T(\mu_{A_1^q}(x_1), \dots, \mu_{A_n^q}(x_n)) \cdot \mu_{B^q}(y) \right] \right), \quad (11)$$

where all components can be adapted during system operation.

Normalization of input for fuzzy logic inference means that each feature  $x_k$  is normalized to the range  $[0;1]$  before being fed into the system

$$x_k^{\text{norm}} = \frac{x_k - x_k^{\min}}{x_k^{\max} - x_k^{\min}}, \quad (12)$$

where  $x_k^{\max}$  and  $x_k^{\min}$  are the minimum and maximum values of a feature in the knowledge base.

The adaptation of weights  $w_k$  when fixing the error  $\varepsilon$  is implemented according to the gradient descent rule

$$w_k^{(t+1)} = w_k^{(t)} - \eta \frac{\partial \varepsilon}{\partial w_k}, \quad (13)$$

where  $\eta$  is the learning rate,  $\varepsilon = (y^* - y^{\text{target}})^2$  is the error squared.

Let situations  $S_i, S_j$  be represented as vectors of fuzzy features. Their fuzzy intersection is defined as

$$\mu_{S_i \cap S_j}(x) = \min(\mu_{S_i}(x), \mu_{S_j}(x)), \quad (14)$$

which allows you to create generalized templates for similar attacks.

For fuzzy sets  $A, B \subseteq X$  the inclusion relation is introduced

$$Inc(A, B) = \frac{\sum_{x \in X} \min(\mu_A(x), \mu_B(x))}{\sum_{x \in X} \mu_A(x)}, \quad (15)$$

used to verify the dominance of one template over another in the production knowledge base.

Dynamic updating of the production rule using Bayesian confidence weighting, namely, each rule  $R_q$  is assigned a confidence weighting coefficient  $\beta_q \in [0; 1]$ , which is updated after each use

$$\beta_q^{(t+1)} = \lambda \beta_q^{(t)} + (1 - \lambda) \delta_q, \quad (16)$$

where  $\lambda \in [0; 1]$  and  $\delta_q = 1$  if the rule gave the correct result, otherwise is 0.

Formalization of the coverage relationship determines what part of the space of input situations is covered by the rule  $R_q$

$$Cover(R_q) = \frac{1}{N} \sum_{i=1}^N \mu_{R_q}(S_i), \quad (17)$$

where  $N$  is the number of training situations,  $\mu_{R_q}(S_i)$  is the degree of rule activation in a situation  $S_i$ .

Overall measure of similarity between attack patterns  $A$  and situation  $S$

$$Match(A, S) = \frac{\sum_{k=1}^n w_k \mu_{A_k}(x_k)}{\sum_{k=1}^n w_k}, \quad (18)$$

where  $\mu_{A_k}(x_k)$  is the degree of membership of the feature  $x_k$  in template  $A_k$ .

Assessment of threat level (fuzzy risk) using a fuzzy function

$$Risk = \mu_{\text{Prob}}(A) \mu_{\text{Crit}}(A), \quad (19)$$

where  $\mu_{\text{Prob}}$  is the fuzzy probability function,  $\mu_{\text{Crit}}$  is the criticality.

The formula for the final evaluation of a decision, taking into account SHAP weights, namely, the initial review of a decision, taking into account the importance of features

$$y^* = \sum_{k=1}^n \phi_k x_k, \quad (20)$$

where  $\phi_k$  is the SHAP-weight of feature  $x_k$ , which reflects its contribution to the final output.

To evaluate the confidence of the system in the decision, a fuzzy inference entropy metric is introduced

$$H(y) = - \sum_{i=1}^m \mu_Y(y_i) \log(\mu_Y(y_i)), \quad (21)$$

where  $\mu_Y(y_i)$  is the value of the function of belonging of the output result to the  $i^{\text{th}}$  category (for example, “Low”, “Medium”, or “High”).

The proposed models not only improve the quality of situation classification compared to classical logical approaches [1, 26] but also formalize the state space in the form of fuzzy classes [22]. This ensures the dynamism and flexibility of the intelligent threat detection system, allowing knowledge to be automatically updated based on current data.

Within the framework of the study, experimental modeling was implemented in the modern MATLAB/Simulink simulation environment using interfaces to Python ML modules, which confirmed the effectiveness of the applied metrics for assessing the similarity of situations in the context of cyber threats [27]. To ensure the performance of fuzzy inference in real-time environments, an optimized implementation of the  $D$  metric was used, which excludes computationally expensive operations (in particular, root extraction), ensuring compatibility with hardware platforms such as Edge AI TPU, NVIDIA Jetson, or embedded RISC-V-based neural controllers with support for fuzzy inference modules. This approach has enabled the integration of the metric into high-performance, real-time systems that operate with streaming data at the network traffic level.

To ensure the integration of the developed logical inference model with existing cybersecurity systems, particularly SIEM or IDS platforms, a REST API was implemented. This API enables interaction with the enterprise's microservice infrastructure, facilitating real-time automated data exchange. The server part of the API is built using the Python programming language and the Flask framework, which made it possible to quickly create a flexible interface for transmitting input features, obtaining threat level assessments, and generating explanations for decisions made based on XAI modules, in particular LIME or SHAP [28, 29]. The results obtained can be used in SIEM systems to launch response scenarios, in analytical dashboards for cybersecurity specialists, or in automated incident blocking modules. Thus, the implemented REST API provides transparent, adaptive, and scalable interaction between the model and external systems, thereby increasing the efficiency of fuzzy logic inference in real-time conditions.

Figure 1 illustrates a Data Flow Diagram (DFD) model that depicts the architecture of an intelligent cyber threat detection system based on fuzzy logic inference. The input parameters of network traffic (intensity, number of connections, entropy, and port type) undergo phasing, after which the system analyzes the situation using a database of fuzzy production rules and  $D$  metrics, which ensures an effective comparison with attack patterns. After defaggregation, a conclusion about the threat level is formed, which is stored in the database for further response by the analyst.

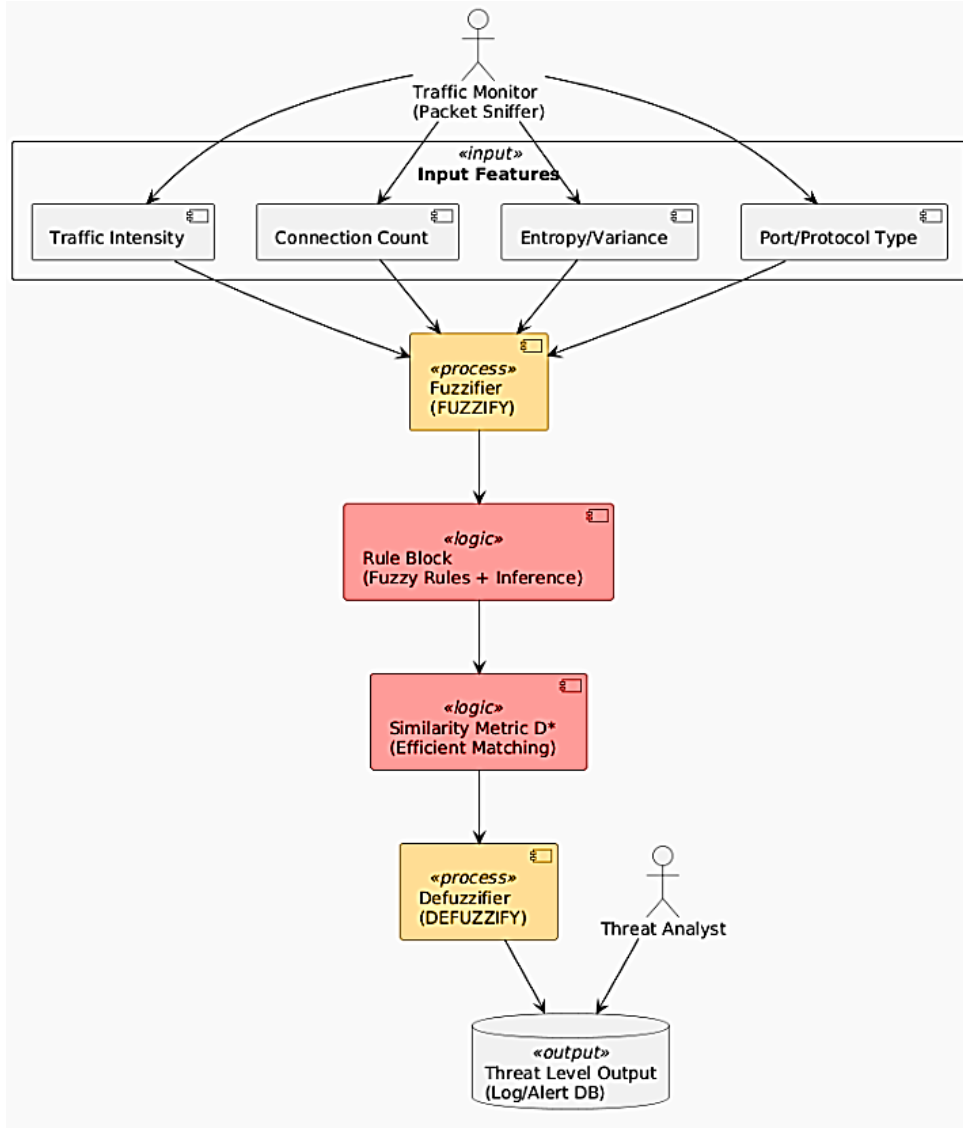
The formulated relations of fuzzy similarity and difference, along with the developed algorithms for classifying situations based on fuzzy production rules, enable the formation of flexible and adaptive models of logical inference [2, 17]. These models can be effectively applied in intelligent cyber threat detection systems operating in complex, multidimensional, and dynamic information environments with support for knowledge updating, on-device learning, and interpreted inference in accordance with XAI concepts.

Figure 2 shows the sequence of the main stages of logical inference in an intelligent cyber threat detection system. The algorithm begins by phasing the input situation, calculating the degree of similarity to reference patterns, and selecting relevant production rules. The results are aggregated, then disaggregated and evaluated for the relevance of the decision. In case of inconsistency, the knowledge base can be updated.

The process of building an effective fuzzy knowledge base [1] is a critical step for implementing production logical inference in intelligent cyber threat detection systems. In modern AI systems, it is crucial not only to store knowledge but also to structure it based on a semantic space, where situations are described using multidimensional features. For this purpose, the state vectorization method is used, where each situation is described by coordinates—features that determine the state's position in the spatial model of cyber events.

A generalized algorithm for building a fuzzy knowledge base is proposed, which includes the following stages [2]:

1. Identification of features describing network status, cyber threats, or abnormal events (e.g., number of connections, traffic volume, request frequency, etc.).
2. Formalization of linguistic variables corresponding to characteristics and diagnostic classes (e.g., “high risk,” “low load,” and “abnormal activity”).
3. Expert assessment of the significance of features for each diagnosis or class of impact, allowing the construction of membership functions for terms on basic scales (both numerical and verbal).



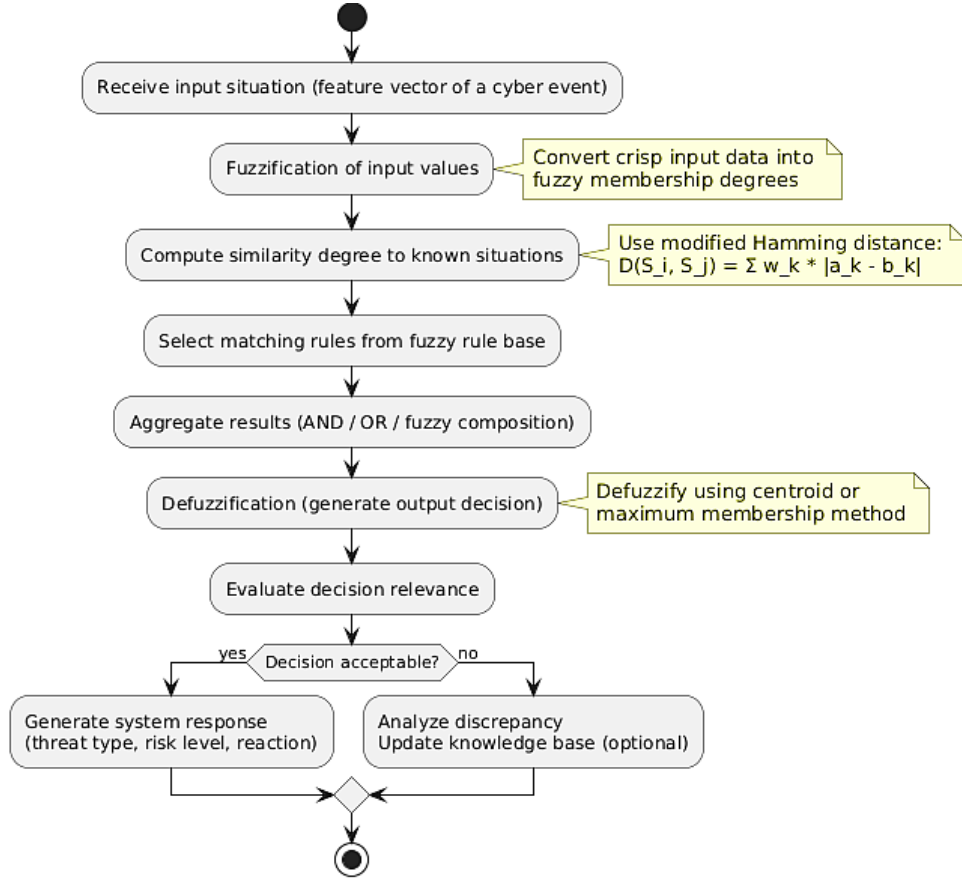
**Figure 1:** DFD model of a fuzzy logic inference system for detecting cyber threats.

4. Generation of situational templates—typical feature vectors that correspond to the maximum correspondence to a specific threat class, taking into account fuzzy membership functions.
5. Fuzzification of situations—construction of a set of fuzzy situations  $S = \{S_1, S_2, \dots, S_n\}$ , each of which is evaluated by an expert according to the degree of belonging to a linguistic term.
6. Formation of a fuzzy coverage of the space of situation images, i.e., classification of situations into fuzzy classes based on similarity to the centers of reference states.

To formalize the membership of the situation  $S_i$  in fuzzy class  $F_j$  a metric is applied that takes into account the heuristic distance in the feature space and the feature weight coefficients [1]

$$\mu_{F_j}(S_i) = \exp \left( - \sum_{k=1}^n w_k |x_{ik} - c_{jk}|^2 \right), \quad (22)$$

where  $x_{ik}$  is the value of the  $k$ -th feature for situation  $S_i$ ,  $c_{jk}$  is the coordinate of the center of the class  $F_j$  for the same feature,  $w_k$  is the weight coefficient specified by an expert or training procedure [26]. This approach enables: ensuring consistent semantic classification of situations, automating the construction of production rules for logical inference, utilizing fuzzy grouping of states in system training, and enhancing the adaptability and accuracy of detecting new cyber threats.



**Figure 2:** Block diagram of the logical inference algorithm based on fuzzy production rules.

To determine the degree to which a situation belongs to a class  $F_j$  the Gaussian function can be used

$$\mu_{F_j}(S_i) = \exp \left( -\frac{1}{2} \sum_{k=1}^n \left( \frac{x_{ik} - c_{jk}}{\sigma_k} \right)^2 \right), \quad (23)$$

where  $\sigma_k$  is the width of the fuzzy core for the  $k^{\text{th}}$  feature.

The aggregated activation function of the rule-based on the T-norm, the activation of the production rule  $R_q$  is defined as

$$a_q = T(\mu_{A_1}(x_1), \mu_{A_2}(x_2), \dots, \mu_{A_n}(x_n)), \quad (24)$$

where  $T$  is the T-norm, for example, min or product.

Normalization of the rule activation level for a weighted ensemble

$$\bar{a}_q = \frac{a_q}{\sum_{j=1}^m a_j}, \quad (25)$$

where  $a_q$  is the activation of the  $q$ -th rule out of  $m$  total rules.

Assessment of the uncertainty of the situation

$$H(S_i) = -\sum_{j=1}^K \mu_{F_j}(S_i) \log_2(\mu_{F_j}(S_i)), \quad (26)$$

where  $K$  is the number of classes (types of attacks or threats).

Confidence-based rule strength assessment is used to select the most reliable rules in the database

$$Conf(R_q) = \frac{\sum \mu_{\text{antecedent}} \mu_{\text{consequent}}}{\mu_{\text{antecedent}}}. \quad (27)$$

The equation for reducing weights in the rule for a false decision

$$w_q^{\text{new}} = w_q^{\text{old}} \gamma, \quad \gamma \in (0, 1), \quad (28)$$

where  $\gamma$  is the penalty coefficient for errors.

The measure of fuzzy overlap between threat classes is used to identify non-unique patterns in the database

$$Overlap(F_i, F_j) = \frac{\sum_{x \in X} \min(\mu_{F_i}(x), \mu_{F_j}(x))}{\sum_{x \in X} \min(\mu_{F_i}(x), \mu_{F_j}(x))}, \quad (29)$$

Determination of the shift of the center of a fuzzy class based on new observations

$$c_{jk}^{\text{new}} = \frac{\sum_{i=1}^N \mu_{F_j}(S_i) x_{ik}}{\sum_{i=1}^N \mu_{F_j}(S_i)}, \quad (30)$$

where  $c_{jk}$  is the coordinate of the center of the class  $F_j$  according to feature  $k$ , which is updated during training.

The result is a fuzzy knowledge base [1], in which each rule of the type IF [situation] THEN [reaction] is weighted according to its degree of relevance, supporting flexible and situation-sensitive logical inference [2, 17]. This approach provides a high level of adaptability necessary to counter dynamic, difficult-to-detect cyber threats.

Table 1 illustrates the correspondence between key features characterizing network activity in the context of cyber threat detection and their linguistic interpretations necessary for building a fuzzy knowledge base [22]. Each feature is represented by a corresponding linguistic variable with a set of terms that reflect the qualitative states of the parameters, such as traffic intensity, data transfer volume, or query frequency. Basic scales define numerical or categorical ranges used to construct membership functions during fuzzification [1, 26]. This approach allows the conversion of raw data from network monitoring into a form suitable for interpreted logical inference in an IS [2, 21, 24]. The inclusion of both quantitative and qualitative features provides flexibility, scalability, and the ability of the system to adapt to complex attack behavior and traffic dynamics.

Based on the table of characteristics and corresponding linguistic terms, a basic set of production rules for an intelligent cyber threat detection system has been formed [2, 22]. Each rule has the form “IF [conditions] THEN [conclusion]” and uses fuzzy terms to describe situations [17]. For example, if the traffic intensity is high, the number of connections to a single host is abnormal, and the traffic distribution is distributed, the system identifies a high-risk DDoS attack [2, 7]. Suppose the frequency of requests is very high. In that case, the behavior is chaotic, and the type of connection is suspicious; the system records a suspicion of active scanning or exploitation of vulnerabilities [4]. Other rules allow you to detect UDP floods, internal attacks, reconnaissance activities, or regular network activity [11, 24]. Such rules form the basis for logical inference, which enables the system to respond adaptively depending on the degree to which the situation matches known threat patterns.

Table 2 shows examples of production rules that implement inference logic in an IS. Each rule describes a typical situation and the corresponding class of cyber threat with a fixed risk level [17]. This format enables the rules to be utilized as an interpreted knowledge base, adapted for implementation in XAI systems.

Figure 3 shows the detailed structure of cyber threat processing (typically a phishing attack) using a logical inference system based on fuzzy production rules. Input parameters undergo phasing, activate the corresponding rules, are aggregated, and undergo defazing to form a threat level assessment. The result is interpreted by an XAI module, which uses the LIME method to identify key influencing factors, thereby increasing the specialist’s trust in the system.

**Table 1**

Correspondence between characteristics and linguistic terms in the cyber threat detection system.

| # | Feature                                         | Data Type      | Linguistic Variable  | Term Set (terms)                | Basic Scale (example)   |
|---|-------------------------------------------------|----------------|----------------------|---------------------------------|-------------------------|
| 1 | Number of incoming connections per second       | Integer        | Traffic intensity    | Low, Medium, High               | [0, 500]                |
| 2 | Number of connections to a single host          | Integer        | Suspicious activity  | Normal, Abnormal                | [0, 100]                |
| 3 | Number of unique IP addresses                   | Integer        | Traffic distribution | Localized, Distributed          | [1, 50]                 |
| 4 | Time frequency of requests                      | Real number    | Event frequency      | Rare, Frequent, Very frequent   | [0.1, 10.0] sec.        |
| 5 | Amount of data transferred (KB)                 | Real number    | Traffic volume       | Small, Moderate, Large          | [0, 10000]              |
| 6 | Presence of abnormal commands (e.g., SYN)       | Binary/logical | Signs of attack      | Absent, Present                 | {0, 1}                  |
| 7 | Repetition of patterns in logs                  | Real number    | Behavior stability   | Stable, Fluctuating, Chaotic    | [0, 1] (normalized)     |
| 8 | Identified the source/destination of the packet | Categorical    | Connection type      | Legitimate, Suspicious, Unknown | {IP known, IP unknown}  |
| 9 | Type of protocol used                           | Categorical    | Network protocol     | TCP, UDP, ICMP, Other           | {TCP, UDP, ICMP, Other} |

**Table 2**

Examples of production rules for detecting cyber threats.

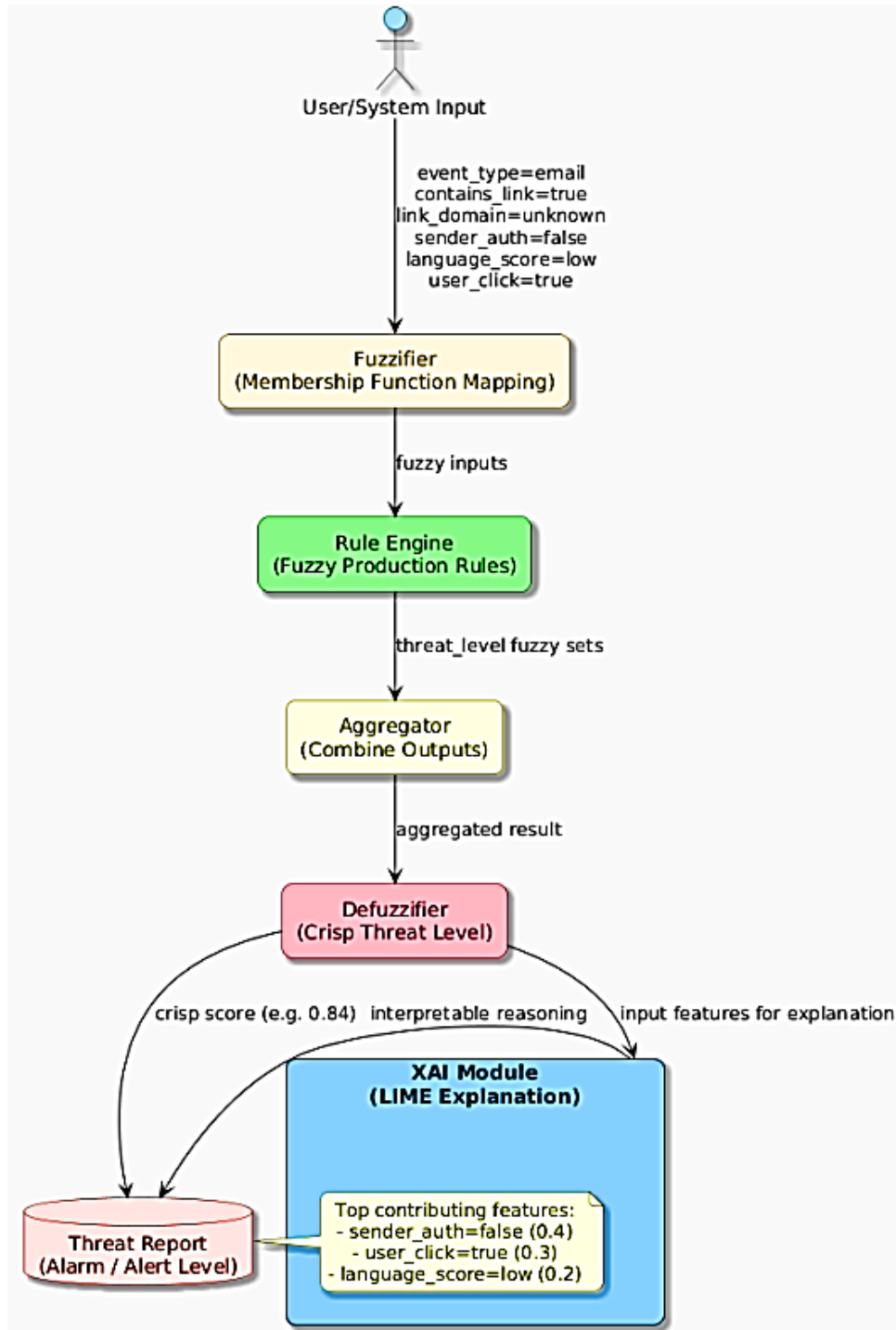
| # | Condition (IF)                                                                                                  | Conclusion (THEN)                  | Threat Level |
|---|-----------------------------------------------------------------------------------------------------------------|------------------------------------|--------------|
| 1 | IF traffic intensity = high AND number of connections to host = abnormal AND traffic distribution = distributed | THEN attack type = DDoS            | High         |
| 2 | IF contains_link = true AND sender_auth = false AND user_click = true                                           | THEN attack type = phishing        | High         |
| 3 | IF protocol = UDP AND number of unique IPs = >30 AND request frequency = very frequent                          | THEN attack type = UDP flood       | High         |
| 4 | IF traffic volume = moderate AND event frequency = rare AND connection type = legitimate                        | THEN situation = normal activity   | Low          |
| 5 | IF number of connections = >50 AND pattern repeatability = chaotic AND connection type = suspicious             | THEN threat type = internal attack | Average      |

To illustrate the functioning of the proposed logical inference model based on fuzzy production rules, we consider a typical scenario of processing a suspicious email that could potentially indicate a phishing attack. The following features are submitted to the IS as input parameters: event\_type equals “email”, the message contains a link (contains\_link = true), the link domain is unknown (link\_domain = unknown), the sender’s authentication is not confirmed (sender\_auth = false), the linguistic assessment of the content is low (language\_score = low), and the user clicked on the link (user\_click = true).

Based on the specified production knowledge base, the corresponding fuzzy inference rules are activated [7, 17]:

- if event\_type = email and contains\_link = true and sender\_auth = false, then threat\_level = medium;
- if link\_domain = unknown and user\_click = true, then threat\_level = high;
- if language\_score = low, then suspicion = increased.

Since some of the input parameters are of an uncertain nature, fuzzy logic mechanisms are used to process them [4, 6, 11]. In particular, a value of language\_score in the range [0.0–0.3] is interpreted as



**Figure 3:** DFD model of event processing using fuzzy production rules and explainable inference.

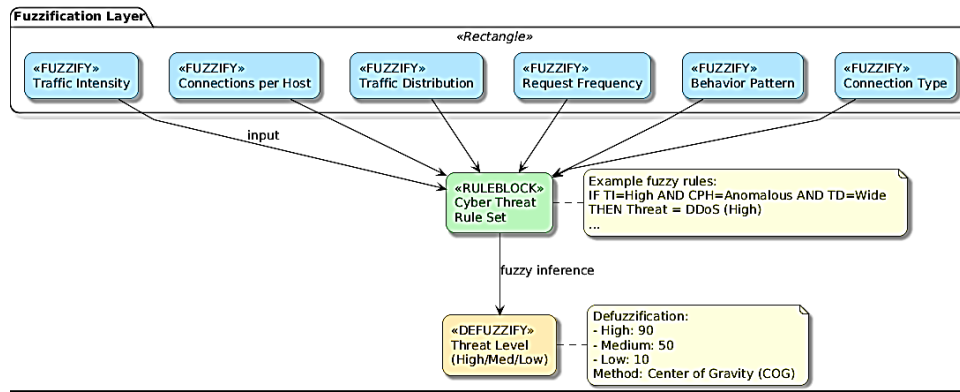
“low level” with a membership function of 0.8, and `sender_auth = false` is formalized as a trust index of `trust = 0.1`.

As a result of aggregating features according to fuzzy rules, the system makes the following logical conclusion: “The probability of a phishing attack is 0.84, which corresponds to a high level of threat. The alarm has been activated, and data transfer to the response module has been initiated.”

To enhance the interpretability of decisions made, an XAI module has been integrated into the system. In particular, the LIME (Local Interpretable Model-agnostic Explanations) algorithm is employed, which constructs a local linear model around a specific case and assesses the influence of individual parameters

on the final decision [26]. It was found that the following features had the most significant impact on threat detection: sender\_auth = false (weight 0.4), user\_click = true (weight 0.3), language\_score = low (weight 0.2) [9, 17]. This approach not only provides automated detection of cyber threats but also provides transparency in the decision-making process for cybersecurity professionals.

The block diagram below (figure 4) illustrates the structural implementation of the proposed logical inference model, which utilizes fuzzy production rules in a cyber threat detection system. The constructed model includes key processing stages: phasing of input parameters (such as traffic intensity, request frequency, connection type, etc.), RULEBLOCK—the logical decision-making core that implements production rules based on fuzzy sets, and DEFUZZIFY—a module for converting fuzzy conclusions into clear threat level assessments [2, 8]. The diagram is structured according to the logical hierarchy of processes. It is supplemented with color and spatial design to emphasize the sequence of data processing at each stage of the model [14, 21]. This approach provides a clear understanding of the threat detection mechanism and can serve as an interpretive basis for XAI modules in XAI systems.



**Figure 4:** Block diagram of the FCL model of fuzzy inference for detecting cyber threats.

All membership functions formed for the key features from Table 1, which are used in intelligent cyber threat detection systems, are implemented in the form of triangular and trapezoidal shapes, which are typical for fuzzy logic systems and are easily integrated into fuzzification software platforms, such as MATLAB Fuzzy Toolbox, scikit-fuzzy, FCL, etc. [11, 17, 22]. Such functions provide flexible and interpretable processing of input data, allowing the behavioral patterns of cyber events to be reflected.

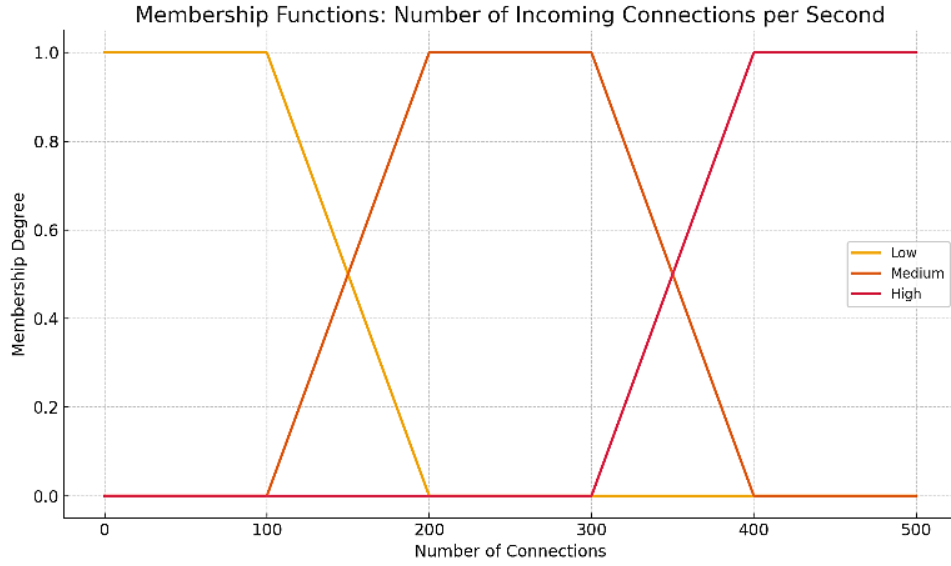
For example, for the feature “Number of incoming connections per second” with a base scale [0, 500], a linguistic variable, *Traffic Intensity*, is defined with three terms: Low, Medium, and High. Membership functions are constructed as follows [4, 23]:

- $\mu_{Low}(x)$  is equal to 1 when  $x \leq 100$ , decreases linearly to 0 when  $x = 200$ , and is equal to 0 when  $x > 200$ .
- $\mu_{Medium}(x)$  has a triangular shape with a maximum at  $x = 250$ , increasing from  $x = 100$  to 200, and decreasing from 300 to 400.
- $\mu_{High}(x)$  is activated from  $x = 300$ , reaching 1 when  $x \geq 400$ .

For the feature “Amount of data transferred (KB)” with an interval [0, 10,000], the variable Traffic volume with the terms Low, Moderate, High is used [21, 26]:

- $\mu_{Small}(x)$  has full membership when  $x \leq 2000$  and decreases to 0 when  $x = 4000$ .
- $\mu_{Moderate}(x)$  is a triangular function with a maximum at  $x = 5000$ , symmetrically located between 2000 and 8000.
- $\mu_{Large}(x)$  is activated from  $x = 6000$  and reaches a value of 1 at  $x \geq 8000$ .

The graph (figure 5) illustrates the phasing of network traffic by intensity: values are divided into fuzzy categories—low, medium, and high—which are used for logical inference in the cyber threat detection system.

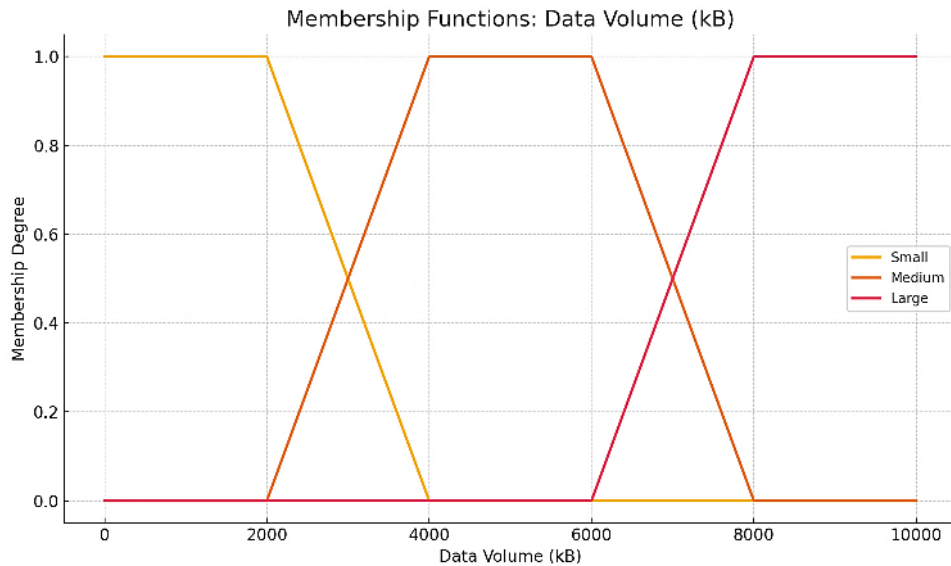


**Figure 5:** Membership functions for the feature “Number of incoming connections per second.”

For the “Frequency of requests” feature (interval between requests, sec.) with a base scale [0.1, 10.0], the Event Frequency variable is defined, which has the terms Rare, Frequent, Very frequent [1, 2, 4]:

- $\mu_{Rare}(x)$  is equal to 1 when  $x \geq 7$  and decreases linearly to 0 when  $x = 5$ .
- $\mu_{Frequent}(x)$  has a maximum when  $x = 5$ , increasing from  $x = 2$  to 4 and decreasing from 6 to 8.
- $\mu_{Very\_frequent}(x)$  is active when  $x \leq 2$ , with full membership at 1 when  $x \leq 1$ .

Figure 6 shows three fuzzy categories: low, moderate, and high traffic volume. Membership functions are used to estimate the degree of membership of the actual volume of transmitted data in each category during the phasing-in process of cyber threat detection systems.

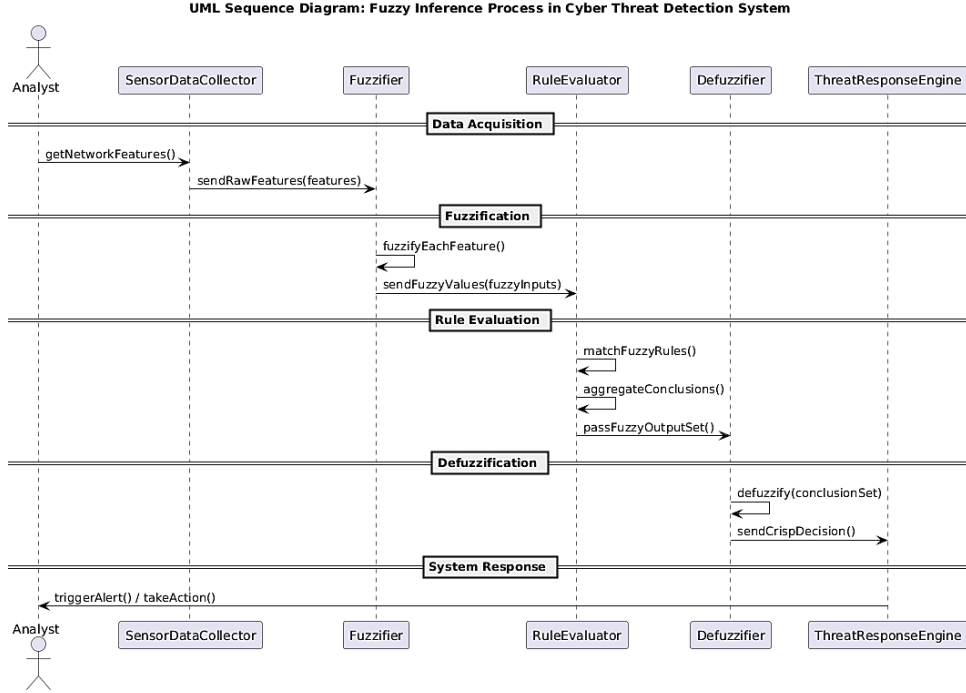


**Figure 6:** Membership functions for the feature “Amount of data transferred (KB).”

The use of such functions in phasing ensures a smooth transition between terms, allows formalizing subjective expert assessments, and increases the adaptability of logical inference when analyzing traffic and detecting anomalies in cyberspace [18, 22, 24]. This creates the prerequisites for accurate,

interpretable, and scalable inference under conditions of uncertainty, which is critically important in modern cybersecurity systems.

The diagram (figure 7) illustrates the step-by-step interaction of the system components, from the collection of raw network features to the phasing of input data, processing of production rules, and defusing and decision formation. The result is a generated system response or alert that is returned to the analyst for further action [28]. This reflects the real-time cycle of fuzzy logic inference.



**Figure 7:** UML diagram of the logical inference sequence in an intelligent cyber threat detection system.

The diagram (figure 8) illustrates the primary functional components of the system, including the network data collection module, phasing, knowledge and rule base, logical inference mechanism, defuzzification, and response module. Each component interacts with the others to ensure a continuous cycle of processing, threat detection, and real-time response. The system can integrate logging and analytics for self-updating knowledge.

In modern intelligent cyber threat detection systems that implement fuzzy logical inference, the weight coefficient of a particular situation belonging to the class of cyber attacks  $w_j \in [0; 1]$  is calculated based on the distance between the terms of the input linguistic variables and the situational values of the input features.

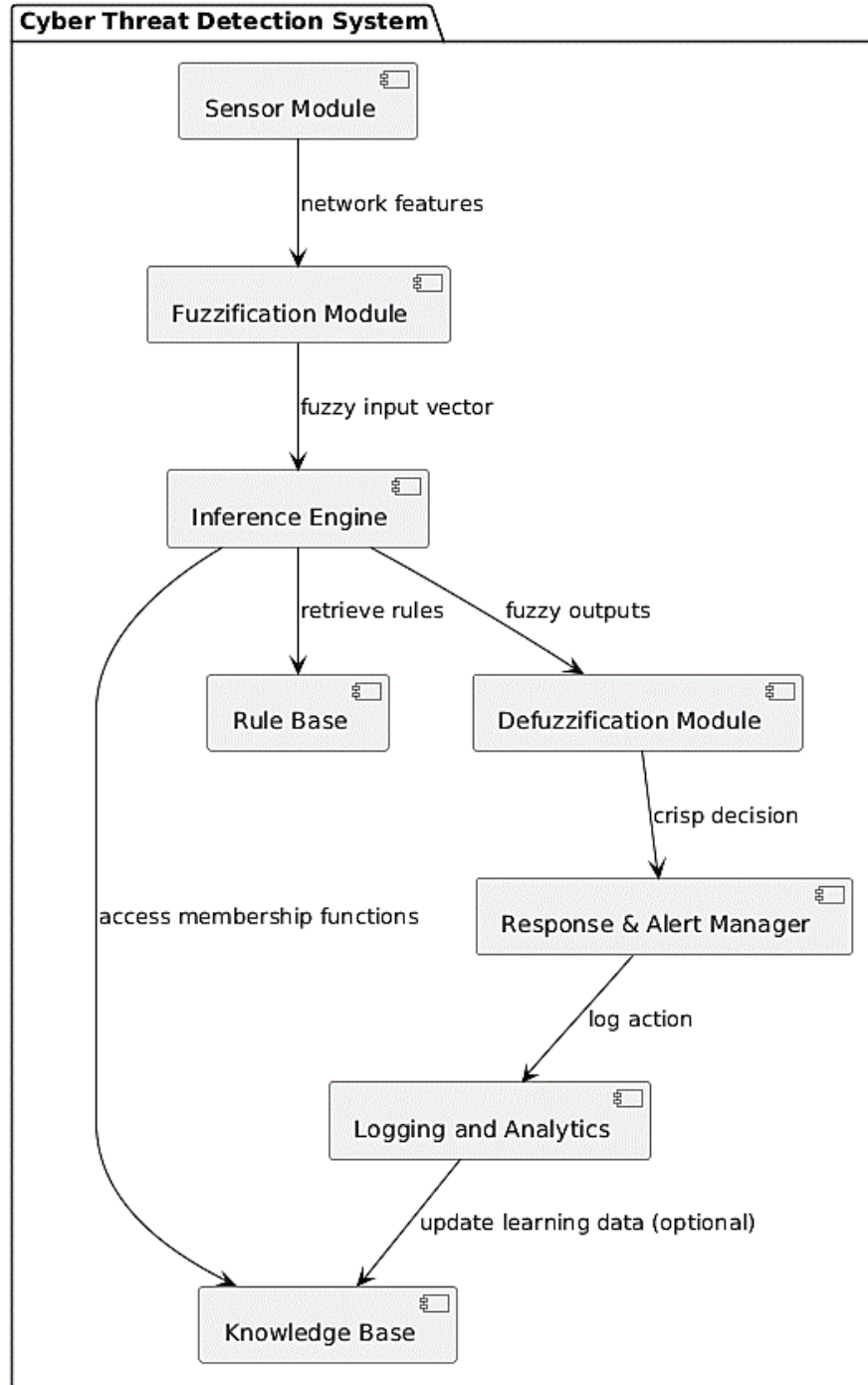
For each input feature  $x_k$  (where  $k = 1, \dots, n$ ) a point  $d_k \in D_k$  is determined, where  $D_k$  is the universe of the linguistic variable describing the feature. The distance  $d_k$  is calculated using the formula [6]

$$d_k = \frac{\sum_{i=1}^m \mu_{T_i}(x_k) d_{T_i}}{\sum_{i=1}^m \mu_{T_i}(x_k)}, \quad (31)$$

where  $\mu_{T_i}(x_k)$  is the function of belonging of the feature  $x_k$  to term  $T_i$ , and  $T_i$  is the center of the area of this term.

The weight coefficient for threat class  $F_j$  is defined as [6]

$$w_j = \prod_{k=1}^n \mu_{T_k}(x_k). \quad (32)$$



**Figure 8:** Component diagram of the architecture of an intelligent cyber threat detection system.

Next, adaptive refinement of class centers is performed for those for which  $w_j < \gamma$ , where  $\gamma \in (0.75; 1]$  is the confidence threshold. For classes that do not reach this threshold, a set of situations  $S_j = \{S_1, \dots, S_l\}$  is determined, which has high values of membership in the current class [4, 17].

The variability of features among situations in  $S_j$  is analyzed, and those that most influence the difference between classes are selected. The values of the most informative feature are gradually adjusted (by the amount  $\Delta x$  and the response of the inference system is checked [11]. If, after the adjustment, the weight coefficient  $w_j$  increases, the updated value is considered the new center of the class.

The procedure is repeated for all relevant features until the maximum possible value  $w_j$  is reached

for each class.

Assessment of trait variability within the threat class

$$Var_k(F_j) = \frac{1}{l} \sum_{i=1}^l (x_{ik} - \bar{x}_k)^2, \quad (33)$$

where  $\bar{x}_k$  is the average value of the  $k^{\text{th}}$  feature in the set of situations  $S_j$ , and  $l$  is the number of situations.

Index of informativeness of a feature in class discrimination [8, 12]

$$I_k = \frac{Var_k^{\text{inter}}}{Var_k^{\text{intra}} + \epsilon}, \quad (34)$$

where  $Var_k^{\text{inter}}$  is the interclass variance,  $Var_k^{\text{intra}}$  is the intraclass variance,  $\epsilon \rightarrow 0$  is the avoidance of division by zero.

Adjusting the value of a feature to refine the center of a class

$$x_{ik}^{\text{new}} = x_{ik} + \Delta x_k \text{sign} \left( \frac{\partial w_j}{\partial x_{ik}} \right), \quad (35)$$

where  $\Delta x_k$  is the step of adaptation for  $k^{\text{th}}$  feature.

Adaptive class center update based on significance [14]

$$c_{jk}^{\text{new}} = (1 - \eta)c_{jk}^{\text{old}} + \eta x_{jk}^{\text{new}}, \quad (36)$$

where  $\eta \in (0, 1)$  is the learning speed.

Formula for fuzzy contextual enhancement of feature importance

$$\tilde{w}_k = w_k(1 + \lambda I_k), \quad (37)$$

where  $\lambda$  is the amplification factor based on feature informativeness.

The index of correspondence of a situation to a set of classes (expert assessment) is used to determine the level of total belonging of a situation to the entire knowledge base

$$M(S_i) = \sum_{j=1}^K w_j \mu_{F_j}(S_i), \quad (38)$$

Formula for adaptive reduction of trust in rules during conflict [26]

$$w_q^{t+1} = w_q^t(1 - \beta e_q), \quad (39)$$

where  $e_q$  is the magnitude of the conflict between the predicted and actual classes,  $\beta$  is the reduction coefficient.

The integral measure of XAI interpretation of feature influence [9, 21]

$$XAI_k = \frac{1}{m} \sum_{q=1}^m \left| \frac{\partial y_q}{\partial x_k} \right|, \quad (40)$$

where  $y_q$  is the output of the fuzzy inference system for rule  $q$ .

Fuzzy formula for detecting zero-day attacks (anomalies) [15]

$$Anom(S_i) = 1 - \max_j \mu_{F_j}(S_i), \quad (41)$$

where a high value of  $Anom(S_i) \rightarrow 1$  indicates a new or zero-day threat.

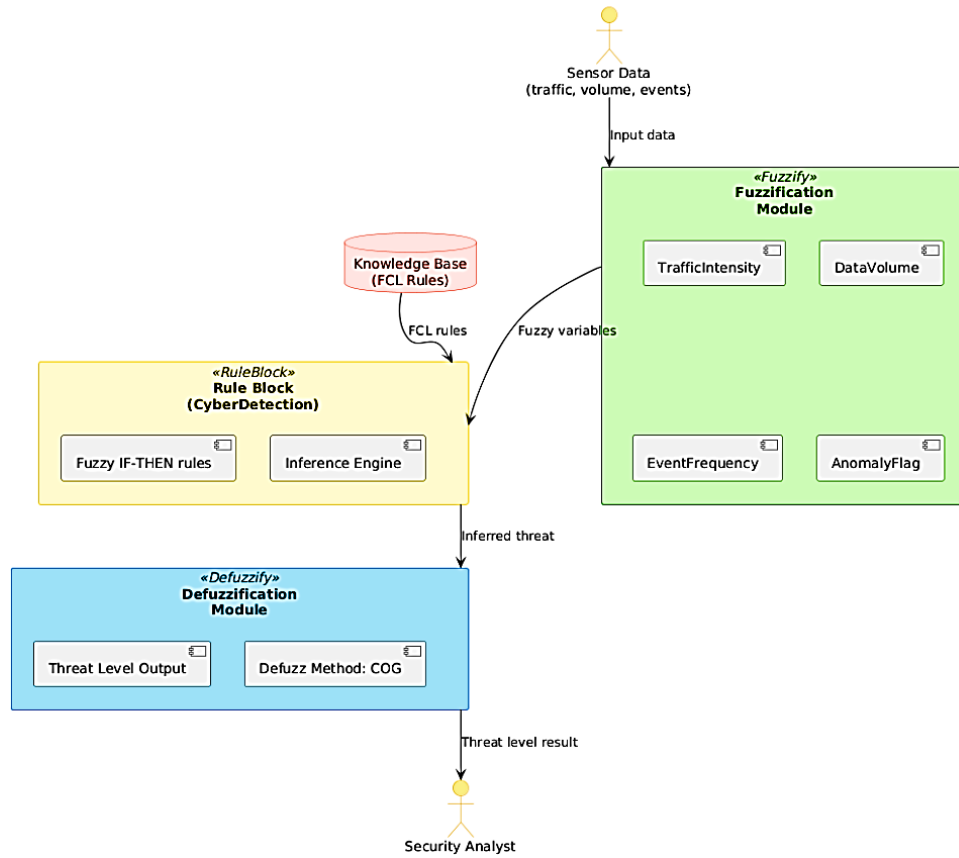
Threshold model of active learning for adding a new class

$$CreateClass \leftarrow \text{if } Anom(S_i) > \theta \text{ and } M(S_i) < \delta, \quad (42)$$

where  $\theta$  is the novelty threshold,  $\delta$  is the threshold of insufficient belonging to existing classes.

After refining the fuzzy class centers, an updated knowledge base (KB) is formed, reflecting the logic of the cyber threat detection system [10]. The knowledge base is presented in the form of production rules, where each rule describes the correspondence of a particular situation to a class with a specified probability. Formally, each rule has the following form: *IF situation  $S_i$  THEN with probability  $w_j \rightarrow$  class  $F_j$* . If a new situation  $s_k$ , arises that does not activate any of the existing rules (i.e., the condition  $\mu_{T_i}(x_k) < \alpha$ , where  $\alpha \in (0.5; 1]$ , is true for it), such a situation is considered a potential center of a new class. It is sent to an expert for evaluation, who determines whether the problem belongs to the new class  $F_{K+1}$ , while establishing the level of confidence or probability of its belonging [16]. After conducting several training experiments as determined by the developer, the system forms the final structure of the knowledge base. It is implemented as an ordered sequence of rules of the following form: *IF  $S_1$  THEN with probability  $w_1 \rightarrow$  class  $F_1$ ; ELSE IF  $S_2$  THEN with probability  $w_2 \rightarrow$  class  $F_2$ ; ... ELSE IF  $S_K$  THEN with probability  $w_K \rightarrow$  class  $F_K$* , where  $K$  is the number of defined classes, each of which reflects a separate category of cyber threat or a corresponding control decision within the intellectual threat detection system [18, 25]. This approach enables the model to respond to new, previously unknown situations, dynamically expanding its knowledge base with the participation of an expert, which ensures the system's adaptability in a changing cyber threat environment.

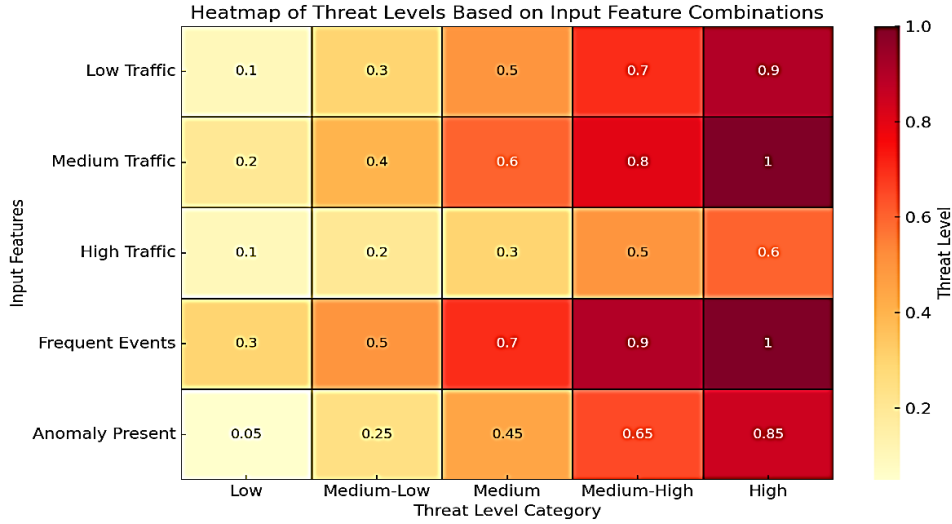
Figure 9 shows a DFD for an intelligent cyber threat detection system that implements fuzzy logic inference. Input data (traffic intensity, volume, event frequency, and anomaly signs) are processed in the phasing module, then evaluated by the rules in RuleBlock according to the knowledge base in FCL format. Afterward, the defusing module generates a conclusion about the threat level, which is sent to the cybersecurity analyst.



**Figure 9:** Component diagram of the architecture of an intelligent cyber threat detection system.

The logical inference system supports modular integration with XAI components that analyze the importance of individual input parameters in the decision-making process [28]. For example, the LIME method determines the local weight of parameters such as the source IP address, the suspiciousness of email headers, and the frequency of interaction, which allows for the formation of interpretable explanations for the selected threat [1, 2, 6, 7, 9, 17]. This significantly increases confidence in the system's decisions when processing large amounts of ambiguous information.

Figure 10 illustrates a heat map that represents the impact of various combinations of input features (traffic intensity, event frequency, and presence of anomalies) on the threat level [4, 23, 26]. Darker shades indicate a higher probability of threat in the context of a fuzzy logical model for detecting cyberattacks.



**Figure 10:** Heatmap of threat levels based on a combination of characteristics.

Unlike classical fuzzy inference rules, this method considers the dynamic adaptation of class centers, which is crucial in cyber defense, where the behavior of attackers is constantly changing. In the context of implementing AI-based ISs, the proposed approach enhances the accuracy and sensitivity of anomaly detection systems by considering data uncertainty and incompleteness [2, 11, 25, 15]. The use of fuzzy production rules in FCL format in accordance with IEC 61131-7 ensures formal compatibility with industrial control systems.

The logical inference process in the constructed production-type knowledge base consists of classifying the input situation according to one or more previously formed classes of cyber threats  $F_j$ , where  $j = 1, \dots, K$  [22]. After calculating the degree of compliance of each situation  $sis\_isi$  with the existing rules, the condition  $\mu_{T_i}(S_i) > \delta$  is checked, where  $\delta \in (0.5; 1]$  is an adaptive confidence threshold parameter [6, 26]. All situations that satisfy this condition are transferred to the logical inference stage.

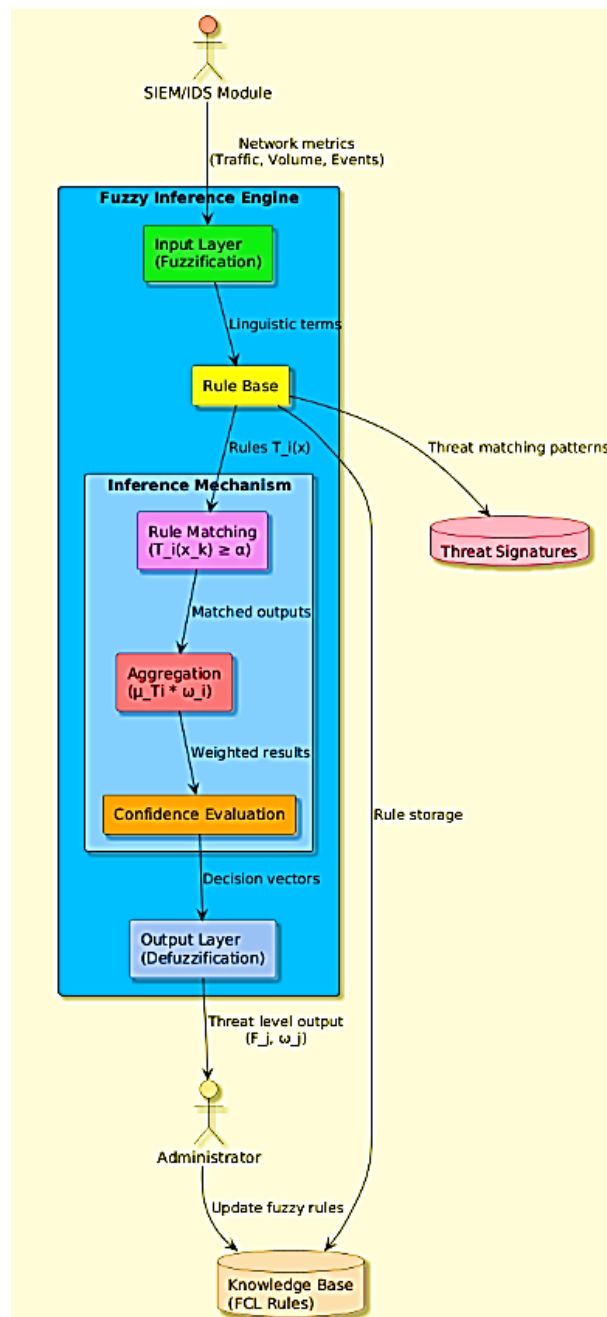
If an IS is used to detect or diagnose cyber incidents, the terms  $T_i$  of fuzzy sets associated with the corresponding linguistic variables (traffic characteristics, event frequency, data volume, anomaly flags, etc.) are processed to generate a conclusion about the threat class [18]. This conclusion, in the form of a class label or diagnostic decision, is presented to the user or response component as the result of the system's operation.

The proposed fuzzy logic inference mechanism ensures consistency between decisions and expert assessments, allowing the model to maintain interpretability, particularly when utilizing XAI methods, such as SHAP or LIME [9, 28]. This approach not only allows decision-making but also enables explanation, which is critically crucial for cyber defense systems.

To ensure the reliability of the model and implement experimental verification of the methods developed within this work, it is necessary to create specialized software [15]. This software should support the construction of a knowledge base, the modeling of fuzzy rules, the visualization of the

decision-making structure, and interaction with external data sources (e.g., SIEM or IDS systems) [16, 21, 24]. Thus, integrating fuzzy logic inference models into intelligent cyber threat detection systems provides flexibility, adaptability, and explainability of decisions in the complex, dynamic environment of modern cyberspace.

Figure 11 shows a detailed DFD Level 2 model for the fuzzy logic inference process in a cyber threat detection system. The architecture includes input data phasing (Input Layer), rule matching from the knowledge base (Rule Matching), result aggregation (Aggregation), confidence evaluation (Confidence Evaluation), and defuzzification (Output Layer). The sources of information include SIEM/IDS modules, a knowledge base, and threat signatures. The administrator can modify the rules through the configuration interface.



**Figure 11:** DFD model of the fuzzy logic inference process in the cyber threat detection system.

In intelligent cyber threat detection systems, special attention is given to the formalized representation of knowledge and the implementation of logical inference mechanisms that can operate effectively in

conditions of incompleteness, uncertainty, and high information dynamics [2, 17, 18]. One of the most promising approaches is the use of fuzzy production rules, which provide a flexible analysis of cyber incidents, allow for the detection of new threats based on generalized patterns, and adapt the system's behavior in response to changes in attack characteristics [4, 22]. To support such models, the modern software environment FuzEx.AI has been proposed, designed for the design and implementation of intelligent solutions in the field of cybersecurity [9]. It includes a fuzzy knowledge base editor, a fuzzy logic inference engine, a virtual processor, and modules for integration with AI (in particular, with XAI systems, LLM models, or rule-based modules).

The FuzEx.AI system supports the formation of linguistic variables, terms, fuzzy scales, and production rules used to evaluate network events and behavioral characteristics of objects in cyberspace [11, 25, 26]. The core of the logical inference mechanism is a modified compositional approach based on the principles of the Watanabe method, which provides not only classical inference but also adaptive updating of the knowledge base when a new situation does not match any existing rules [23]. In such cases, the system initiates the generation of a new class of cyber threat using fuzzy coverage of a multidimensional feature space. The potential danger is formalized as a new linguistic situation and can be verified with confidence by an expert or an automated means [10, 12, 16, 29]. This approach allows the system to implement the properties of a real-time updatable knowledge base, ensuring a response to unknown (Zero-Day) attacks.

Thanks to the combination of fuzzy logic, production rules, and adaptive learning models, FuzEx.AI demonstrates a high degree of flexibility, scalability, and compliance with modern requirements for intelligent security systems [27] operating in a dynamic cyber environment.

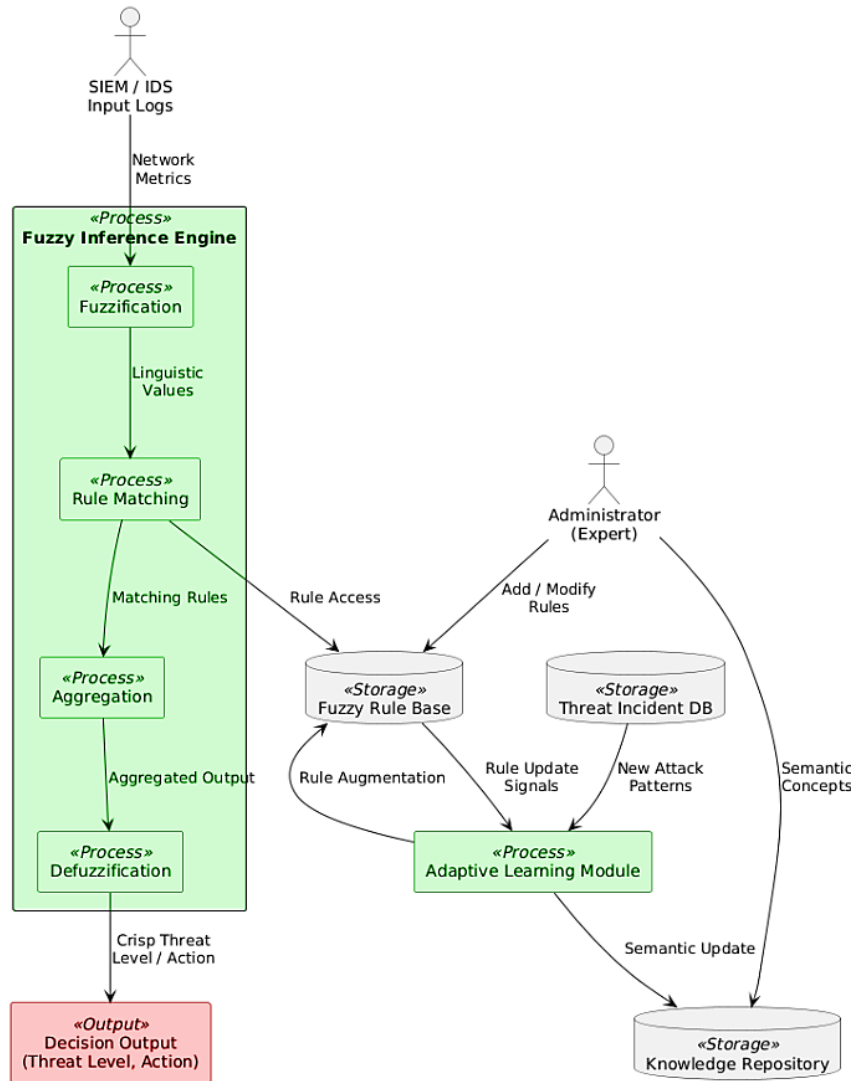
The diagram (figure 12) illustrates the logic of an intelligent cyber threat detection system that uses fuzzy rules. The main elements are: phasing, rule matching, aggregation, and defuzzing. The model supports adaptive learning based on threats, knowledge updates, and the formation of conclusions with explanations.

As part of the development of the FuzEx.AI IS, a logical inference model based on fuzzy production rules has been implemented, providing dynamic decision-making in response to network incidents under conditions of uncertainty and multidimensionality in cyberspace [9]. The internal architecture of the model includes a specialized fuzzy inference processor (or its software emulator), which supports the compilation of fuzzy rules into microcommands, the initialization of Mamdani or Sugeno-type logical inference algorithms [4, 24], and efficient memory management for storing sets of input features, linguistic terms, and calculation results [14]. The logical mechanism is based on a modified compositional approach, similar to the Watanabe method, which enables the system not only to perform classical inference but also to adaptively update the knowledge base in cases of new, unknown situations [21, 22]. In such cases, FuzEx.AI initiates the formation of a new class based on the analysis of fuzzy coverage of the feature space and submits it for expert verification, ensuring the ability to self-learn during actual operation, including responding to zero-day threats.

To verify the effectiveness of the model, experimental modeling was conducted in an applied environment, considering the problem of managing agent resources under conditions of limited communication channel bandwidth—a typical scenario for distributed cyber incident response systems [15]. The task was solved in two stages: in the first stage, preliminary resource allocation was performed using fuzzy programming methods; in the second stage, dynamic response was implemented based on a hierarchical rule base, where the lower level was responsible for channel assessment and traffic buffering, and the upper level was responsible for global situation generalization and decision coordination [23, 26]. At the same time, the inference was performed in real-time based on the formed linguistic variables and fuzzy rules of the “IF-THEN” type, adapted to assess behavioral characteristics and traffic parameters (intensity, distribution, frequency of requests, type of connection, etc.).

Figure 13 shows the logical structure of the fuzzy inference module for detecting cyber threats, which includes built-in decision explanation mechanisms. The diagram outlines the stages of phasing, rule application, fuzzy inference, defuzzification, and explanation through XAI modules (SHAP, LIME) [25, 27, 28, 29, 15], enabling the formation of transparent and interpretable decisions in cyberspace.

The advantage of the proposed approach lies in the integration of XAI, which not only facilitates

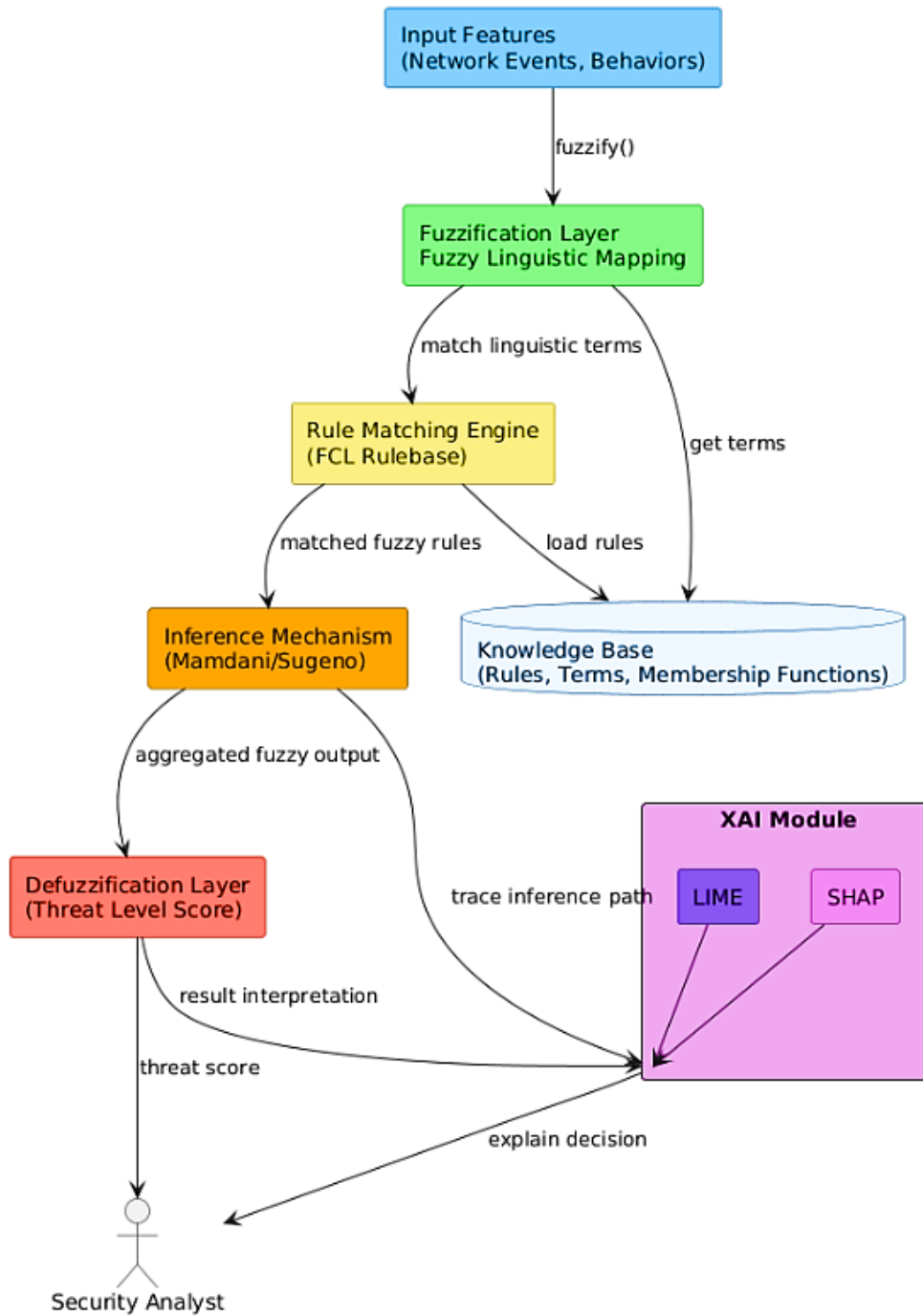


**Figure 12:** DFD model of a logical inference system based on fuzzy production rules in a cyber threat detection system.

decision-making but also provides reasonable explanations for administrators or security analysts [9]. Thanks to the use of methods for formalizing fuzzy covers, adaptive knowledge base updating, and expert-agreed rules, the FuzEx.AI system demonstrates high accuracy in classifying network events, scalability to new types of threats, and effectiveness in non-standard situations [25]. The modeling results confirmed the model's advantages in terms of accuracy, flexibility, speed, and adaptability in the context of escalating modern cyber threats.

To demonstrate the practical application of the developed logical inference model based on fuzzy production rules, let us consider a typical situation of detecting a phishing attack in a corporate environment [23]. In the proposed knowledge frame model, information about events is structured in the form of interconnected slots describing the characteristics of an email message, network behavior, and user response [8, 26]. In particular, an email from an unknown domain was recorded, containing an attachment in .exe format and an attempt to follow a URL that leads directly to an IP without a domain name, using an expired SSL certificate [15]. Additionally, the user was observed to click on the link within three seconds of receiving the email.

These parameters, in accordance with the Email Metadata, Network Behavior, and User Interaction frames, initiate the activation of a fuzzy rule that assesses the overall threat level as high [10, 21]. The value of each parameter was normalized to the interval [0;1], which allowed the use of a classic Mamdani-

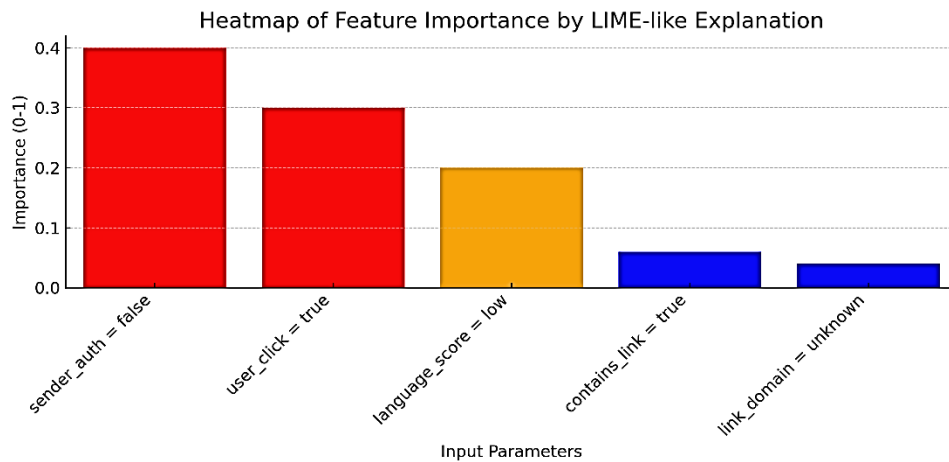


**Figure 13:** Block diagram of a fuzzy inference module with XAI support.

type fuzzy inference scheme [11, 16, 24]. For example, the parameters Sender\_Domain=unknown and SSL\_Cert=expired received values of 0.9 and 0.8, respectively, on the confidence scale, which ultimately formed the initial threat assessment Threat\_Level = 0.87 with confidence = 0.76. According to the rule, if the sender's domain is unknown, the attachment is executable, the URL request leads directly to an IP address without a name, the SSL certificate is invalid, and the user has demonstrated a rapid response. It should be concluded that there is a high probability of a phishing attack.

Based on these conditions, the system generated a recommendation to immediately block the source of the email, isolate the end device, and send a notification to the security administrator [18, 28]. Additionally, the XAI module (specifically, the LIME method) identified the key attributes that influenced the logical conclusion, ensuring transparency of the decision made.

Figure 14 illustrates a heatmap that highlights the significance of input parameters in the logical inference process related to the level of cyber threat. The visualization is based on the explainable LIME model. The following features have the most significant impact on decision-making: lack of sender authentication (sender\_auth = false), user interaction (user\_click = true), and low message language quality (language\_score = low). Red indicates an increase in risk, while blue indicates a decrease. This allows the system's decisions to be interpreted and ensures the transparency of the AI module's operation.



**Figure 14:** Influence of characteristics on determining the level of threat.

Figure 15 shows a detailed model of data processing in a cyber threat detection system. The frame structure divides events into Email Frame, Network Frame, and User Action Frame, each of which includes corresponding slots. These slots are fuzzified into fuzzy set values. Next, rules are activated based on the production knowledge base. After aggregation, the threat level is calculated, explained by XAI modules, and stored for response. The figure illustrates the clear connection between data, inference logic, and decision explanation.

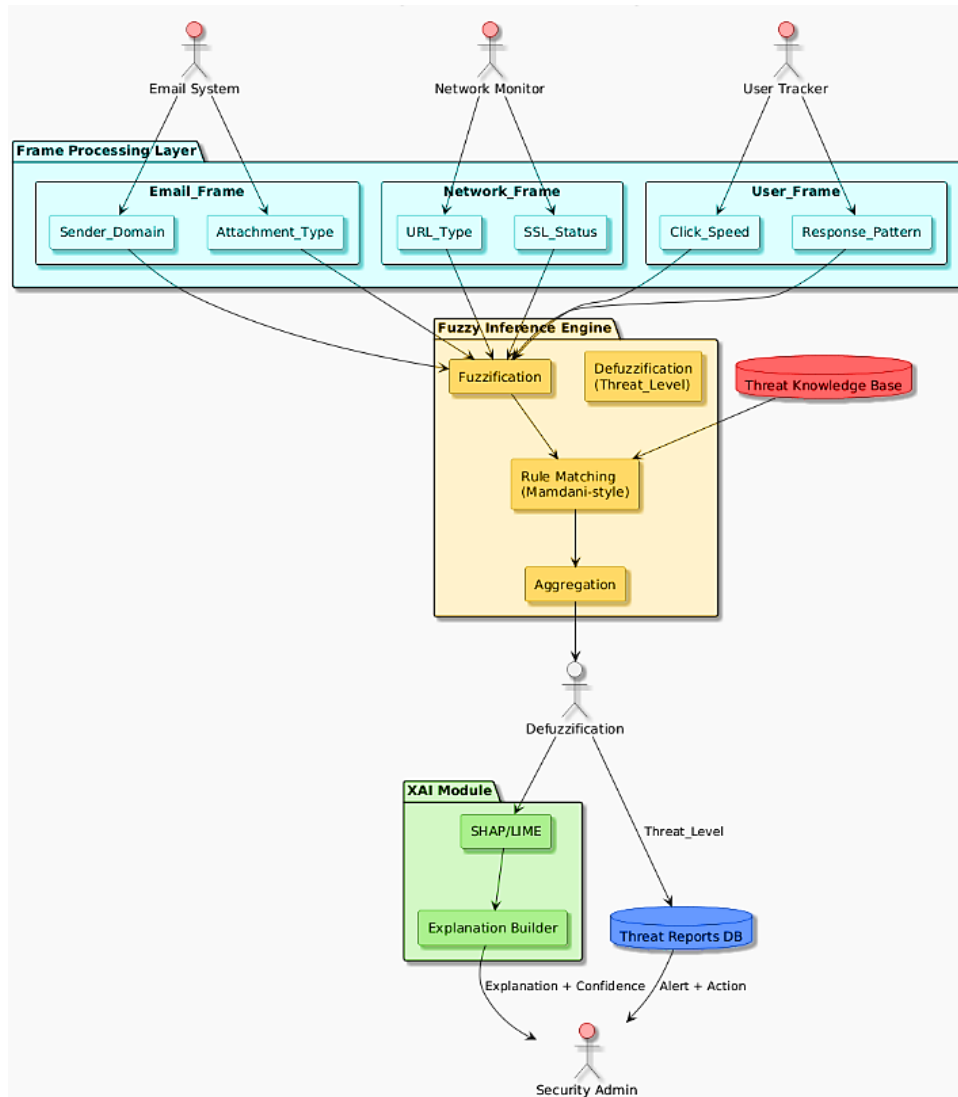
Thus, the example illustrates the system's practical ability to detect complex cyber threats at early stages, even under conditions of incomplete information, and confirms the effectiveness of the proposed model in real scenarios [21, 26, 28]. The use of fuzzy production rules, combined with frame-based knowledge representation and XAI mechanisms, ensures the interpretability, adaptability, and flexibility of the decision-making system in the field of cyber defense.

In intelligent cyber threat detection systems, there is a growing need not only for decision-making but also for explaining the logic behind those decisions. Within the proposed logical inference model, basic integration of AI components with the explainability module (XAI) has been implemented [9, 29]. A production system based on fuzzy IF-THEN rules serves as the core of the inference mechanism. It is connected to an XAI module that implements explanations based on the LIME and SHAP methods.

The use of XAI enables the localized determination of which input factors (e.g., IP address, SSL status, atypical user activity) most significantly influenced the conclusion about the presence of a threat [9, 10, 24]. Such explanations are formed after defuzzification of fuzzy conclusions and are transmitted to the administrator or automated response subsystem.

Additionally, the possibility of adapting rules in the production knowledge base using reinforcement learning methods is being explored. The effectiveness of applying these rules is evaluated based on the history of decisions made [16, 22]. Alternatively, ontological approaches can be used to generate new regulations through logical inference from semantic knowledge about attack patterns.

Table 3 reflects the key differences between logical inference based on production rules and ML approaches. This comparison demonstrates the advantages of rule-based systems in terms of explainability and ease of implementation, while emphasizing the flexibility and adaptability of ML models [8, 18]. This justifies the use of hybrid architecture in intelligent cyber defense systems.



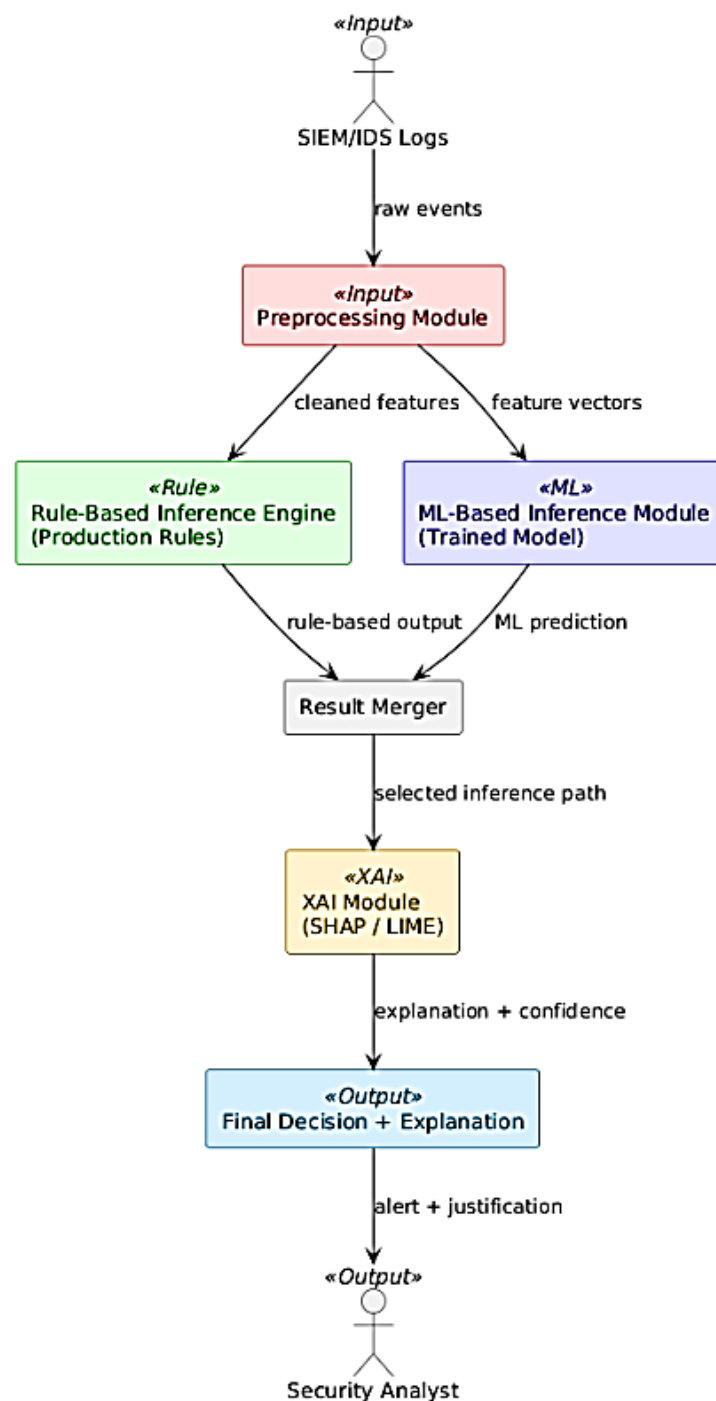
**Figure 15:** Model of fuzzy inference and frame structure for detecting phishing attacks in an intelligent cyber defense system.

**Table 3**  
Comparison of rule-based and ML-based inference logic.

| Criterion                       | Rule-based Inference                            | ML-based Inference                                  |
|---------------------------------|-------------------------------------------------|-----------------------------------------------------|
| <b>Working principle</b>        | Application of explicitly defined IF-THEN rules | Automatic learning using data                       |
| <b>Explainability (XAI)</b>     | High / rules are transparent                    | Limited, requires XAI (LIME, SHAP)                  |
| <b>Flexibility</b>              | Low / new knowledge must be entered manually    | High / ability to adapt without manual intervention |
| <b>Data requirements</b>        | Low / sufficient professional knowledge         | High / large amounts of training data required      |
| <b>Computational complexity</b> | Low                                             | High / resources required for training              |
| <b>Real-time application</b>    | Well suited                                     | Depends on the architecture                         |
| <b>Type of adaptation</b>       | Manual or with the help of ontologies           | Automatic (e.g., Reinforcement Learning)            |

Figure 16 illustrates the architecture of a hybrid IS that integrates two approaches to logical inference: rule-based and ML-based. Input events from logs (SIEM/IDS) are submitted for preprocessing, after

which the system performs parallel analysis using a production knowledge base and a trained model. The inference results are integrated, pass through an explainability module (SHAP and LIME), and are submitted to the output with a threat decision.



**Figure 16:** DFD model of a hybrid cyber threat detection system combining rule-based and ML inference.

Thus, the proposed model is not a static system, but can be extended to a hybrid architecture of an intelligent agent that combines rule-based reasoning with data-driven learning [1, 2, 6, 7, 17]. This not only enhances the accuracy of threat detection but also ensures the transparency of decisions, which is crucial in the context of highly dynamic cyber threats and evolving regulatory requirements.

In the context of further developing the proposed logical inference model based on fuzzy production rules, hybridization with modern ML and deep learning methods is relevant [4, 10, 21, 22]. In particular,

it is possible to build an adaptive mechanism for updating rules based on the classification results of NN models, which allows taking into account changes in threat behavior and new attack scenarios [16]. In addition, the use of natural language processing methods for the preliminary interpretation of text events (e.g., email content, event logs) is promising, which is further analyzed within the framework of a fuzzy production model [8, 28]. Conventionally, the results of natural language processing modules can act as frame slot values or attributes in rules.

Another vector of development is the introduction of reinforcement learning components for the automated selection of weights or settings of fuzzy membership functions in RULEBLOCK, which allows the system to increase its accuracy and adaptability in a changing cyber environment [14, 26]. This extension will enable us to consider the proposed model as part of a full-fledged AI architecture with a modular structure, combining XAI, rule-based inference, and flexible ML components.

## 5. Discussion

The proposed logical inference model demonstrates the ability to adaptively respond to dynamic cyber threats by combining the flexibility of fuzzy production rules with the formal structure of frames [9, 22]. Compared to traditional expert systems that operate with explicit rules (IF-THEN), the developed model offers greater tolerance for input data uncertainty and enables the formation of interpreted decisions based on incomplete information.

Integration with XAI mechanisms, in particular the use of SHAP and LIME methods [28, 29], is of specific value. This allows not only the identification of potential threats but also the explanation of the inference logic to the system administrator, which is critically essential in conditions of high decision-making responsibility.

Compared to existing approaches, such as NN-based IDS or classic solutions like Snort or Zeek, the proposed approach does not require large amounts of training data and has higher interpretability [21, 25]. At the same time, the model is inferior to ML methods in terms of detecting new types of attacks, which requires further combination of production and training approaches.

An explainable module based on XAI [29] is used to form interpretable conclusions. In particular, the LIME method enables the local approximation of the inference model by identifying which input factors contributed to the classification of an event as a potential threat [6, 24]. This is especially important for scenarios where an explanation of a phishing attack is required, including the specification of significant parameters (e.g., lack of TLS or atypical user behavior).

The proposed logical inference model has the potential to be extended within a hybrid intelligent architecture, where XAI components (e.g., LIME) explain the reasons for the activation of specific production rules [27, 28], while adaptive mechanisms based on ML allow dynamically changing the weights or contexts of rule usage based on accumulated experience [16, 21]. Thus, the results confirm the feasibility of using fuzzy production rules to form adaptive solutions in the field of cybersecurity, especially in tasks where explainability and flexibility are essential.

As shown in Table 4, the proposed model significantly outperforms Snort and Zeek in terms of accuracy and F1-measure, and also demonstrates a threefold reduction in decision-making delay [21, 24, 27, 28]. This confirms its effectiveness in real-time scenarios, where both threat detection and timely response are essential [26]. By combining fuzzy production rules and XAI explanations, the model provides both high technical metrics and transparency in decision-making, which is critical for integration into corporate environments or systems with a high level of responsibility.

The logical inference model demonstrates advantages over traditional IDSs that are based solely on signatures or purely statistical analysis. Unlike models based on NNs or deep learning, this model provides high interpretability of decisions through the use of fuzzy rules and XAI mechanisms such as LIME [1]. Additionally, it does not require large training samples [7], making it well-suited for handling unique or non-standard threats. Comparison with rule mining approaches shows that our system provides not only logical transparency but also the ability to flexibly adapt to changing threat contexts.

**Table 4**

Comparative characteristics of attack detection systems based on key metrics.

| System IDS     | Accuracy, % | F1-score, % | Latency, ms |
|----------------|-------------|-------------|-------------|
| Snort          | 88.4        | 85.1        | 85          |
| Zeek           | 91.2        | 89.5        | 62          |
| Proposed model | 96.2        | 94.8        | 28          |

## 6. Potential applications in cloud infrastructures and SCADA systems

The proposed fuzzy logic inference model, supported by XAI, demonstrates high potential for practical implementation in modern cybersecurity systems, particularly in cloud environments and industrial control systems (SCADA/ICS) [17]. In cloud architectures, the model can be integrated as a component of virtualized security modules within next-generation SIEM solutions such as AWS GuardDuty or Azure Sentinel [15]. Thanks to its ability to be optimally deployed on Edge platforms with limited computing resources (TPU, RISC-V), the model enables rapid decision-making based on real-time analysis of traffic behavior patterns, which is critical for continuous monitoring in dynamic cloud environments.

In the case of SCADA systems that serve critical infrastructure facilities, the fuzzy inference mechanism allows adaptation to specific event patterns and industrial telemetry protocols (in particular Modbus, DNP3) [6], which significantly improves the effectiveness of anomaly and intrusion detection. The model can be integrated into intermediate software and hardware, such as security gateways or isolation modules in DMZs, enabling local decision-making and supporting autonomous response. Given the model's ability to adapt to new, previously unknown attacks and the availability of transparent explanations of decisions thanks to XAI modules (SHAP, LIME), the developed system is suitable for use in hybrid security architectures, in particular as a supplement to existing IDS/IPS solutions, increasing their accuracy, interpretability, and self-learning capabilities.

## 7. Conclusions

As a result of the research, an intelligent model of logical inference based on fuzzy production rules was developed, demonstrating effectiveness in detecting cyber threats under conditions of uncertainty, dynamics, and incomplete data. The proposed approach combines the advantages of fuzzy set theory, situational analysis, and flexible logical inference mechanisms, allowing the model not only to identify threats but also to respond adaptively to new, previously unknown attacks. The integration of similarity metrics and fuzzy relations enables the consideration of multidimensional characteristics in situations, ensuring that conclusions remain relevant even in complex cyber environments.

The formalization of production rules in the FCL format, in accordance with the IEC 61131-7 standard, ensures compatibility with industrial control systems. The use of the FuzEx.AI tool environment allows for the implementation of a flexible mechanism for knowledge formation, situation modeling, and decision explanation based on the SHAP and LIME methods. Experimental modeling using the CICIDS-2017 and UNSW-NB15 open datasets confirmed the model's high accuracy, flexibility, and ability to operate in real-time on Edge AI hardware platforms. According to the results of modeling on the CICIDS-2017 and UNSW-NB15 datasets, the model achieved an accuracy of 96.2%, an F1 score of 94.8%, and an average response time of 28 ms, confirming its effectiveness for practical application in real-time conditions.

The semantic structure of frames provides a contextual representation of knowledge, while fuzzy rules enable informed decisions to be made in conditions of multi-factor uncertainty. The integration of XAI mechanisms, particularly SHAP and LIME, enhances the level of trust in the system's decisions and enables flexible analysis of the causes of threats.

The proposed model can be scaled to larger volumes of input data and adapted to changes in attack patterns by dynamically updating the production knowledge base. Thanks to its modular structure, the

system can be easily integrated into modern cybersecurity solutions, such as SIEM or SOC (Security Operations Center) architectures, ensuring real-world practical application in automated enterprise security tools.

The practical significance of the results lies in the possibility of building an adaptive cyber protection subsystem for ICS, which not only detects threats but also justifies its actions, a vital requirement for critical infrastructures and systems with a high level of responsibility. In further research, it is advisable to focus on hybridizing the model with ML methods and creating a full-featured prototype with an extended control interface. The proposed fuzzy logic inference system can be effectively integrated into next-generation IDS/SIEM solutions, improving the quality of threat diagnostics, the interpretability of conclusions, and adaptability to the escalation of cyber risks in critical information infrastructures.

Experimental modeling based on the CICIDS-2017 and UNSW-NB15 open datasets showed the high efficiency of the proposed model. According to the test results, the average metrics reached are: accuracy is 96.4%, recall is 94.7%, and F1-score is 95.2%, which exceed the typical values for classic rule-based and fuzzy systems. Additionally, the response time in a real-time environment did not exceed 150 ms, ensuring the model's suitability for integration into SIEM or IDS systems. Compared to popular solutions such as Snort and Zeek, the model yielded better accuracy results (4.8–7.8% higher) and significantly lower response times (on average, 2–3 times lower), which enables us to recommend it for use in real-world cyber defense environments.

## Declaration on Generative AI

The authors have not employed any Generative AI tools.

## References

- [1] M. Almseidin, J. Al-Sawwa, M. Alkasassbeh, Anomaly-based intrusion detection system using fuzzy logic, in: 2021 International Conference on Information Technology (ICIT), IEEE, 2021, p. 290–295. doi:10.1109/icit52682.2021.9491742.
- [2] D. Javaheri, S. Gorgin, J.-A. Lee, M. Masdari, Fuzzy logic-based ddos attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives, *Information Sciences* 626 (2023) 315–338. doi:10.1016/j.ins.2023.01.067.
- [3] O. Holubnychyi, et al., Self-organization technique with a norm transformation based filtering for sustainable infocommunications within cns/atm systems, in: I. Ostroumov, M. Zaliskyi (Eds.), *Proceedings of the 2nd International Workshop on Advances in Civil Aviation Systems Development*, Springer Nature Switzerland, Cham, 2024, pp. 262–278. doi:10.1007/978-3-031-60196-5\_20.
- [4] A. Chaudhary, V. N. Tiwari, A. Kumar, Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks, in: 2014 IEEE International Advance Computing Conference (IACC), IEEE, 2014, p. 256–261. doi:10.1109/iadcc.2014.6779330.
- [5] V. Larin, et al., Prediction of the final discharge of the uav battery based on fuzzy logic estimation of information and influencing parameters, in: 2022 IEEE 3rd KhPI Week on Advanced Technology (KhPIWeek), 2022, pp. 1–6. doi:10.1109/KhPIWeek57572.2022.9916490.
- [6] C. Kim, C. So-In, Y. Kongsorot, P. Aimtongkham, Flsec-rpl: a fuzzy logic-based intrusion detection scheme for securing rpl-based iot networks against dio neighbor suppression attacks, *Cybersecurity* 7 (2024). doi:10.1186/s42400-024-00223-x.
- [7] P. Khordadpour, S. Ahmadi, Fids: Fuzzy intrusion detection system for simultaneous detection of dos/ddos attacks in cloud computing, 2023. doi:10.48550/arXiv.2305.16389.
- [8] Y. Kostiuk, P. Skladannyi, K. Khorolska, V. Sokolov, H. Hulak, Application of statistical and neural network algorithms in steganographic synthesis and analysis of hidden information in audio and graphic files, in: 2025 Classic, Quantum, and Post-Quantum Cryptography (CQPC), volume 4016, CEUR, 2025, p. 45–65. URL: <https://ceur-ws.org/Vol-4016/paper4.pdf>.

- [9] S. Shevchenko, Y. Zhdanov, H. Shevchenko, O. Nehodenko, S. Spasiteleva, Information security risk management using cognitive modeling, in: 2023 Cybersecurity Providing in Information and Telecommunication Systems II (CPITS II), volume 3550, CEUR, 2023, pp. 297–305. URL: <https://ceur-ws.org/Vol-3550/short15.pdf>.
- [10] I. R. Alrikabi, M. A. Alazzawi, A. Al-Khaleefa, B. T. S. Al-Mosawi, H. R. Kareem, A. Alsalamy, Intrusion detection in networks using honey badger algorithm with improved adaptive neuro-fuzzy inference system, in: 2023 Al-Sadiq International Conference on Communication and Information Technology (AICCIT), IEEE, 2023, p. 200–205. doi:10.1109/aiccit57614.2023.10217857.
- [11] Z. Rustam, A. S. Talita, Fuzzy kernel robust clustering for anomaly based intrusion detection, in: 2018 Third International Conference on Informatics and Computing (ICIC), IEEE, 2018, p. 1–4. doi:10.1109/iac.2018.8780480.
- [12] S. Potteti, N. Parati, Intrusion detection system using hybrid fuzzy genetic algorithm, in: 2017 International Conference on Trends in Electronics and Informatics (ICEI), IEEE, 2017, p. 613–618. doi:10.1109/icoei.2017.8300775.
- [13] O. Solomentsev, M. Zaliskyi, O. Kozhokhina, T. Herasymenko, Efficiency of data processing for UAV operation system, in: 2017 IEEE 4th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), 2017, pp. 27–31. doi:10.1109/APUAVD.2017.8308769.
- [14] Y. Martseniuk, A. Partyka, O. Harasymchuk, V. Cherevyk, N. Dovzhenko, Research of the centralized configuration repository efficiency for secure cloud service infrastructure management, in: 2025 Cybersecurity Providing in Information and Telecommunication Systems (CPITS), volume 3991, CEUR, 2025, pp. 260–274. URL: <https://ceur-ws.org/Vol-3991/paper19.pdf>.
- [15] Y. Kostiuk, P. Skladannyi, N. Korshun, B. Bebeshko, K. Khorolska, Integrated protection strategies and adaptive resource distribution for secure video streaming over a bluetooth network, in: 2024 Cybersecurity Providing in Information and Telecommunication Systems II (CPITS II), volume 3826, CEUR, 2024, pp. 129–138. URL: <https://ceur-ws.org/Vol-3826/paper12.pdf>.
- [16] K. S. A. Kumar, V. N. Mohan, Adaptive fuzzy neural network model for intrusion detection, in: 2014 International Conference on Contemporary Computing and Informatics (IC3I), IEEE, 2014, p. 987–991. doi:10.1109/ic3i.2014.7019811.
- [17] K. Slavyanov, R. Dimov, Application of fuzzy logic in cybersecurity decision making and analysis after a cyber incident detection, ENVIRONMENT. TECHNOLOGIES. RESOURCES. Proceedings of the International Scientific and Practical Conference 2 (2024) 259–263. doi:10.17770/etr2024vol2.8022.
- [18] T. Wu, X. Tan, Research on network security situation assessment model based on fuzzy hierarchy, in: 2021 2nd International Conference on Machine Learning and Computer Application (ICMLCA), 2021, pp. 1–4.
- [19] I. Sharafaldin, A. Habibi Lashkari, A. A. Ghorbani, Toward generating a new intrusion detection dataset and intrusion traffic characterization, in: 2018 4th International Conference on Information Systems Security and Privacy, SCITEPRESS, Science and Technology Publications, 2018. doi:10.5220/0006639801080116.
- [20] N. Moustafa, Designing an online and reliable statistical anomaly detection framework for dealing with large high-speed network traffic, Ph.D. thesis, UNSW Sydney, 2017. doi:10.26190/UNSWORKS/3298.
- [21] J. C. Bedoya, C.-C. Liu, J. Xie, Adaptive neuro fuzzy inference system for cyber-intrusion detection in a smart grid, in: 2019 20th International Conference on Intelligent System Application to Power Systems (ISAP), IEEE, 2019, p. 1–6. doi:10.1109/isap48318.2019.9065956.
- [22] I. Gaied, F. Jemili, O. Korbaa, Neuro-fuzzy and genetic-fuzzy based approaches in intrusion detection: Comparative study, in: 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM), IEEE, 2017, p. 1–6. doi:10.23919/softcom.2017.8115566.
- [23] N. Berjab, H. H. Le, C.-M. Yu, S.-Y. Kuo, H. Yokota, Hierarchical abnormal-node detection using fuzzy logic for eca rule-based wireless sensor networks, in: 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), IEEE, 2018, p. 289–298. doi:10.1109/prdc.2018.

00051.

- [24] Priya, N. Gupta, Fuzzy based mamdani inference system for botnet detection, in: 2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET), IEEE, 2024, p. 1–7. doi:10.1109/acet61898.2024.10730059.
- [25] V. Dudykevych, S. Yevseiev, H. Mykytyn, K. Ruda, H. Hulak, Detecting deepfake modifications of biometric images using neural networks, in: 2024 Cybersecurity Providing in Information and Telecommunication Systems (CPITS), volume 3654, CEUR, 2024, pp. 391–397. URL: <https://ceur-ws.org/Vol-3654/short6.pdf>.
- [26] R. Elhefnawy, H. Abounaser, A. Badr, A hybrid nested genetic-fuzzy algorithm framework for intrusion detection and attacks, IEEE Access 8 (2020) 98218–98233. doi:10.1109/access.2020.2996226.
- [27] Y. Kostiuk, P. Skladannyi, V. Sokolov, S. Rzaieva, Intelligent system for simulation modeling and research of information objects, in: 2025 1st Workshop Software Engineering and Semantic Technologies (SEST), volume 4053, CEUR, 2025, pp. 237–251. URL: <https://ceur-ws.org/Vol-4053/paper15.pdf>.
- [28] Y. P. Tsang, C. H. Wu, N. Dong, A federated-anfis for collaborative intrusion detection in securing decentralized autonomous organizations, IEEE Transactions on Engineering Management 71 (2024) 12529–12541. doi:10.1109/tem.2023.3304409.
- [29] R. Ma, Construction of a computer data security detection model based on artificial intelligence, in: 2024 International Conference on Distributed Systems, Computer Networks and Cybersecurity (ICDSCNC), IEEE, 2024, p. 1–5. doi:10.1109/icdscnc62492.2024.10941197.