COMPUTER SCIENCE
КОМПЬЮТЕРЛІК ҒЫЛЫМДАР
КОМПЬЮТЕРНЫЕ НАУКИ

UDC 004.056
GRNTI 20.23.29

https://doi.org/10.55452/1998-6688-2026-23-3-144-159

Amirbayeva A.,
Master's, ORCID ID: 0009-0009-3180-2990,
e-mail: adinaxanova2@gmail.com

Kazakh-British Technical University,
Almaty, Kazakhstan

HYBRID INTELLIGENT DECISION-SUPPORT SYSTEM FOR CYBERSECURITY RISK ASSESSMENT AND SECURITY ACTION SELECTION

Abstract

Selecting appropriate information security systems is a complex task influenced by organizational risks, infrastructure characteristics, evolving cyber threats, and regulatory requirements. Traditional approaches based on manual analysis and expert judgment often lack adaptability, scalability, and consistency in dynamic cybersecurity environments. This study proposes a hybrid intelligent decision-support system that combines fuzzy logic, machine learning, and ISO-based cybersecurity standards for risk assessment and security action recommendation. The fuzzy inference module evaluates cybersecurity events under uncertainty using parameters such as attack frequency, vulnerability level, and defense efficiency. Based on the calculated risk level, the system generates standardized response actions aligned with international ISO/IEC standards. In addition, a Random Forest machine learning model is used to evaluate whether the selected actions are likely to mitigate the attack successfully. Experimental evaluation performed on a synthetic dataset demonstrated that the proposed hybrid architecture achieves high predictive performance and improves both interpretability and adaptability of cybersecurity decision support systems in complex operational environments.

Keywords: cybersecurity, decision support systems, fuzzy logic, machine learning, risk assessment, information security

Received April 13, 2026; revised May 25, June 8, 18, 2026; accepted June 26, 2026.

Introduction

The rapid growth of cyber threats and the increasing complexity of digital infrastructures significantly complicate the task of ensuring organizational information security. Modern organizations operate in highly dynamic technological environments characterized by diverse attack vectors, continuously evolving threat landscapes, and increasingly strict regulatory requirements.

As digital transformation accelerates across industries, organizations face growing challenges in protecting critical assets, sensitive information, and ensuring operational continuity.

Information security architecture typically consists of multiple protective mechanisms, including firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), data loss prevention (DLP) solutions, and security monitoring platforms. The selection and configuration of these mechanisms depend on numerous interrelated factors, such as organizational size, industry sector, infrastructure complexity, risk exposure, and available resources. These factors create a complex decision-making environment in which security solutions must be carefully evaluated and aligned with organizational security policies and risk management strategies.

However, in practice, the selection of cybersecurity solutions is often performed using expert judgment, manual risk analysis, or static evaluation frameworks. While these approaches remain widely used, they may lead to subjective assessments, inconsistencies in decision-making, and limited scalability in complex infrastructures. Traditional approaches also struggle to effectively process large volumes of security-related data and to address the uncertainty inherent in cybersecurity risk assessment processes.

To address these limitations, recent advances in artificial intelligence have opened new opportunities for improving cybersecurity decision-support systems. Machine learning techniques enable automated analysis of large datasets, anomaly detection, and prediction of potential security incidents, significantly enhancing the ability to respond to emerging threats [1]. In parallel, fuzzy logic has been widely applied in cybersecurity risk assessment because it allows modeling uncertainty and imprecision using linguistic variables and rule-based reasoning [2]. Fuzzy inference systems have demonstrated effectiveness in evaluating information security risks by integrating factors such as threat probability, potential damage, and system vulnerabilities [3].

Intelligent decision-support systems are increasingly used to assist organizations in complex decision-making environments by integrating artificial intelligence techniques with domain knowledge and expert rules [4]. In cybersecurity management, such systems can support risk analysis, automate the selection of security countermeasures, and improve the overall effectiveness of defensive strategies.

In this context, the development of hybrid intelligent approaches that combine multiple artificial intelligence techniques has attracted significant attention in recent cybersecurity research. Integrating fuzzy logic with machine learning allows combining human-like reasoning under uncertainty with data-driven predictive capabilities, thereby improving both interpretability and adaptability of cybersecurity solutions.

This study proposes a hybrid intelligent decision-support model for the selection and evaluation of information security measures. Existing cybersecurity studies often focus on separate stages of the decision-making process. Machine learning-based approaches are mainly used for intrusion detection, anomaly classification, or prediction tasks [1, 7, 8]. Fuzzy logic-based studies usually concentrate on risk assessment under uncertainty and the formalization of expert reasoning [2, 3, 10]. AI-based decision-support systems provide general frameworks for assisting complex decisions, but they do not always connect risk estimation with standard-based response actions and mitigation evaluation [4]. In contrast, the proposed approach integrates these stages into one closed-loop workflow: fuzzy risk assessment, ISO/IEC-based action recommendation, Random Forest-based mitigation prediction, and structured reporting. This integration distinguishes the proposed prototype from approaches that address only detection, only risk scoring, or only rule-based recommendation. Unlike traditional cybersecurity decision-support approaches that focus mainly on attack detection, risk scoring, or rule-based recommendation separately, the proposed model combines these stages into a single closed-loop workflow. The system first evaluates risk under uncertainty using fuzzy logic, then maps the identified attack type and risk level to ISO/IEC-based security actions, and finally applies a Random Forest model to estimate whether the selected actions are likely to mitigate the incident. Therefore, the novelty of the proposed approach lies not in using fuzzy logic or machine learning separately, but in their integration with standard-based action selection and structured

reporting within one decision-support architecture. The proposed approach integrates fuzzy logic-based risk assessment, ISO-based security action recommendation, and Random Forest-based mitigation prediction. The main contribution of the study is the development of a unified decision-support pipeline that connects risk estimation, standardized response recommendation, and predictive evaluation of selected cybersecurity actions.

Material and methods

Modern information security systems represent a comprehensive set of technical, software, and organizational measures aimed at ensuring the confidentiality, integrity, and availability of information. With the rapid development of digital technologies and the increasing complexity of IT infrastructures, organizations are exposed to a growing number of cyber threats, which necessitates the use of multi-layered protection mechanisms.

Contemporary cybersecurity architectures are typically based on the principle of defense-in-depth, which involves the use of multiple complementary components such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), firewalls, and Security Information and Event Management (SIEM) platforms. These systems work together to monitor, detect, and respond to cyber threats in real time, providing a layered approach to security management [5, 6]. Cyber threats can be classified into several categories, including network attacks (e.g., DDoS and port scanning), authentication attacks (e.g., brute-force), application-level attacks, and malware-based attacks such as botnets. These threats can be described using parameters such as frequency of occurrence, system vulnerability, and defense efficiency. Proper classification and modeling of these threats are essential for effective cybersecurity management in dynamic environments [7, 8].

Risk assessment is a central component of cybersecurity systems. Traditionally, risk is defined as the product of the probability of a threat and its impact:

$$R = P \times I$$

where R denotes risk, P is the probability of occurrence, and I represents the impact or damage caused by the threat. However, such models are limited in real-world scenarios due to uncertainty, incomplete information, and the subjective nature of expert evaluations [9].

To address these limitations, modern approaches increasingly apply fuzzy logic for cybersecurity risk assessment. Fuzzy systems allow modeling uncertainty using linguistic variables and membership functions. In general, a fuzzy risk model can be expressed as:

$$RiskScore = f(A, F, V, D)$$

where A represents the attack type, F is the frequency of the attack, V is the vulnerability level, and D is the defense efficiency. This formulation reflects a more realistic representation of cybersecurity conditions. Each numerical variable is transformed into fuzzy sets using triangular membership functions. For example, frequency, vulnerability, and defense efficiency are represented by the linguistic values low, medium, and high, while the output variable damage is represented by very low, low, medium, high, and very high.

The numerical RiskScore is converted into risk levels using the following thresholds: values below 250 are interpreted as LOW risk, values from 250 to below 650 are interpreted as MEDIUM risk, and values equal to or above 650 are interpreted as HIGH risk. These thresholds were selected to support practical prioritization of cybersecurity events in the prototype.

In fuzzy inference systems, numerical input values are transformed into fuzzy sets using membership functions. One of the most commonly used forms is the triangular membership function:

$$\mu(x) = \begin{cases} 0, & x \le a \\ \dfrac{x-a}{b-a}, & a < x \le b \\ \dfrac{c-x}{c-b}, & b < x < c \\ 0, & x \ge c \end{cases}$$

This function defines the degree of membership of a variable x to a fuzzy set. Triangular functions are widely used due to their simplicity and interpretability [10].

The decision-making process in fuzzy systems is based on a set of rules that describe relationships between input variables.

Fuzzy inference can be expressed as:

$$R_i = \min\left(\mu_F, \mu_V, \mu_D\right)$$

Where R_i represents the activation level of a specific of rule i. The final risk value is obtained through defuzzification, commonly using the centroid method:

$$RiskScore = \frac{\sum_{i=1}^{n} \mu_i \cdot x_i}{\sum_{i=1}^{n} \mu_i}$$

Fuzzy logic has been widely applied in cybersecurity risk assessment due to its ability to handle uncertainty and incorporate expert knowledge. Recent studies confirm its effectiveness in evaluating complex systems and industrial environments [2, 3].

In addition to risk assessment, cybersecurity systems must provide appropriate response actions. In practice, system administrators perform a set of actions depending on the type of attack. These actions can be divided into automated and manual categories. Simple actions, such as blocking suspicious IP addresses or applying traffic limits, can be executed automatically through external services. More complex actions require human intervention and include system reconfiguration or incident investigation.

To standardize these actions, international cybersecurity standards are used. ISO/IEC 27001 defines the overall framework for information security management systems, while ISO/IEC 27002 provides detailed guidelines for implementing security controls. ISO/IEC 27035 focuses on incident response, ISO/IEC 27033 addresses network security, and ISO/IEC 27034 deals with application security. These standards ensure that response strategies follow best practices and are applicable in real-world scenarios [11].

Within the proposed system, cybersecurity actions are mapped to specific attack types based on ISO recommendations. For example, brute-force attacks require authentication strengthening and password policy enforcement, while DDoS attacks require traffic filtering and resource scaling. This mapping enables systematic and consistent decision-making. The mapping between cyberattack types and ISO-based response actions, presented in Table 1, plays a key role in the proposed decision-support system.

Table 1 – Mapping of cyberattacks to ISO-based security actions

Attack Type	ISO Standard	Recommended Actions
Brute Force	ISO/IEC 27002	Block IP, enforce MFA, reset passwords
DoS/DDoS	ISO/IEC 27033	Rate limiting, enable DDoS protection, scale resources
Botnet	ISO/IEC 27035 / ISO/IEC 27001	Isolate host, enable IDS alerts, collect indicators of compromise
Port Scan	ISO/IEC 27035	Logging, firewall rules, incident response
Web Attack	ISO/IEC 27034	Enable WAF, patch application, review logs

This mapping ensures that each detected attack is associated with a set of standardized and well-established countermeasures derived from international information security standards. For example, brute-force attacks are addressed through authentication-related controls such as blocking suspicious IP addresses, enforcing multi-factor authentication, and resetting compromised credentials, in accordance with ISO/IEC 27002. Similarly, DDoS attacks are mitigated through network-level measures including rate limiting, traffic filtering, and resource scaling, as recommended by ISO/IEC 27033. Other attack types, such as botnets, port scanning, and web-based attacks, are handled through corresponding ISO standards, ensuring that the recommended actions reflect best practices in cybersecurity management. It improves the consistency and reliability of the system's recommendations, while also making them more applicable in real-world environments. By aligning decision-making with recognized standards, the proposed approach reduces subjectivity and enhances the practical value of the system for system administrators and cybersecurity specialists.

The mapping is not intended to represent full ISO/IEC compliance. It is used as a standard-based recommendation layer that connects common attack scenarios with relevant security domains. Brute-force attacks are linked to ISO/IEC 27002 because they require authentication and access control measures. DoS/DDoS attacks are linked to ISO/IEC 27033 because they mainly affect network availability and require network-level countermeasures. Web attacks are linked to ISO/IEC 27034 because they concern application security. Port scanning and botnet-related activities are connected with incident detection and response logic described in ISO/IEC 27035.

Another important aspect of modern cybersecurity systems is the evaluation of defense effectiveness. Traditional approaches focus mainly on risk estimation, but do not analyze whether applied actions successfully mitigate threats. To address this limitation, machine learning models are used.

The machine learning component can be formalized as:

$$y = ML(A, F, V, D, S)$$

Where y is a binary variable indicating whether the attack was mitigated and S represents the strength of applied actions. The action strength can be calculated as:

$$S = \sum_{i=1}^{n} \omega_i \cdot a_i$$

where a_i indicates whether action i was applied, and ω_i denotes the relative weight of action i.

This formulation allows the model to consider not only system conditions but also the effectiveness of response actions.

Machine learning methods, particularly ensemble algorithms such as Random Forest, have demonstrated strong performance in cybersecurity tasks, including intrusion detection and classification. These models can capture complex relationships between variables and adapt to new data, making them suitable for dynamic environments [1, 12].

Recent research highlights the growing role of artificial intelligence in decision support systems. AI-based systems combine data-driven approaches with expert knowledge to improve decision-making processes in complex domains such as cybersecurity. They enable automation, scalability, and improved accuracy in threat detection and response [4].

Modern systems increasingly include automated reporting mechanisms. Reports can be generated on a daily, weekly, or monthly basis and include detailed information about events, timestamps, recommended actions, and execution results. The integration of large language models (LLMs) allows generating structured and human-readable reports, improving the usability of cybersecurity systems.

The integration of fuzzy logic, machine learning, and standardized response strategies forms the basis of hybrid intelligent decision-support systems. Such systems provide a comprehensive framework for cybersecurity management by combining risk assessment, action recommendation,

automation, and effectiveness evaluation. This approach improves the adaptability, consistency, and efficiency of cybersecurity processes in dynamic environments.

The proposed system is designed as a hybrid intelligent decision-support model for cybersecurity management. Its main objective is to support the selection of appropriate information security measures by combining fuzzy risk assessment, standards-based action recommendation, automated response, and machine learning–based evaluation of defense effectiveness. Such hybrid approaches are increasingly considered effective in cybersecurity because they combine interpretability and uncertainty handling with data-driven predictive capability [1, 2, 4].

The overall architecture of the system is shown in Figure 1. This architecture reflects the idea that cybersecurity decision support should not be limited to attack detection alone, but should also include response recommendation, automation, and evaluation of countermeasure effectiveness.

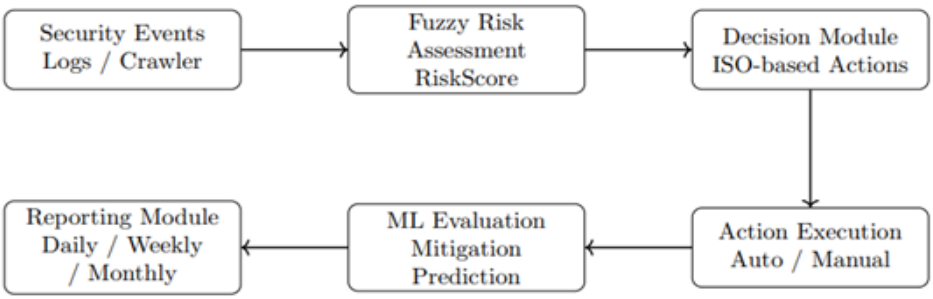

Figure 1 – Architecture of the hybrid intelligent cybersecurity system

The fuzzy risk assessment module is used to estimate the severity of a cybersecurity event under uncertainty. Traditional risk models often rely on exact numerical values, but cybersecurity parameters are frequently uncertain, incomplete, or more naturally expressed in linguistic form. Fuzzy logic is well suited for such tasks because it allows numerical inputs to be converted into interpretable linguistic categories and processed through expert-defined rules [2, 3].

The fuzzy model uses triangular membership functions for the input variables frequency, vulnerability, and defense efficiency. Each variable is defined on a scale from 0 to 10 and represented by three linguistic terms: LOW, MEDIUM, and HIGH. The output variable is damage or RiskScore, defined on a scale from 0 to 1000 and represented by five linguistic terms: VERY LOW, LOW, MEDIUM, HIGH, and VERY HIGH. As shown in Table 2, values closer to 1 indicate stronger membership, while values close to 0 indicate weak or no membership.

Table 2 – Interpretation of fuzzy membership values

Membership degree range	Interpretation
0	No membership
$0 < \mu(x) < 0.3$	Weak membership
$0.3 \leq \mu(x) < 0.7$	Partial/moderate membership
$0.7 \leq \mu(x) < 1$	Strong membership
1	Full membership

The membership degree $\mu(x)$ is a continuous value from 0 to 1. It is not limited to fixed values such as 0.2, 0.4, 0.6, or 0.8. These values may be used only for interpretation, while the actual membership degree is calculated by the corresponding membership function.

Representative fuzzy rules used in the model include the following:

1. If frequency is HIGH, vulnerability is HIGH, and defense efficiency is LOW, then risk is VERY HIGH.

2. If frequency is HIGH and defense efficiency is LOW, then risk is HIGH.
3. If vulnerability is HIGH and defense efficiency is LOW, then risk is HIGH.
4. If defense efficiency is HIGH and frequency is LOW, then risk is VERY LOW.
5. If frequency, vulnerability, and defense efficiency are MEDIUM, then risk is MEDIUM.

The fuzzy rule base was organized into several logical groups. The first group defines baseline risk levels for different attack types, including normal activity, port scanning, brute-force attempts, web attacks, DoS/DDoS, and botnet-related events. The second group covers high-risk conditions where high frequency and high vulnerability are combined with low defense efficiency. The third group describes cases where strong defense efficiency reduces the final risk level. The fourth group contains attack-specific escalation rules for DoS/DDoS, botnet, web attack, and brute-force scenarios. The fifth group covers balanced medium-risk cases, where the input parameters have moderate values. Finally, fallback rules are included to ensure that the fuzzy inference system produces an output even when a specific input combination is not fully covered by detailed rules. This structure makes the fuzzy rule base systematic and suitable for prototype-level cybersecurity risk assessment.

After fuzzy inference, the aggregated fuzzy output is converted into a numerical RiskScore using centroid-based defuzzification. The numerical RiskScore is then interpreted as LOW, MEDIUM, or HIGH risk for the recommendation module.

The pseudocode of the overall hybrid model is given in Algorithm 1. The role of the fuzzy stage in this workflow is to provide the first analytical layer for assessing event severity before security actions are selected.

Algorithm 1 – Hybrid Cybersecurity Decision Model

Input: Security event (A, F, V, D)
1. Compute RiskScore using fuzzy model;
2. Determine risk level (LOW, MEDIUM, HIGH);
3. Generate recommended actions based on ISO standards;
4. if action is simple then
   Execute action automatically;
   else
   Recommend action to the administrator;
5. Compute action strength S;
6. Predict mitigation using the machine learning model;
   Generate report;

After the risk level is determined, the system generates a set of recommended actions for the administrator. This module is based on the principle that specific classes of attacks require specific countermeasures. To make the recommendations more consistent and practical, the mapping between attacks and actions is aligned with international information security standards.

In particular, the developed system uses the following standards as a reference:
- ISO/IEC 27001 for general information security management,
- ISO/IEC 27002 for access control and authentication-related controls,
- ISO/IEC 27033 for network security measures,
- ISO/IEC 27035 for incident detection and response,
- ISO/IEC 27034 for application security.

For example, brute-force attacks are associated with actions such as IP blocking, password reset, and multi-factor authentication, which are consistent with ISO/IEC 27002. DDoS attacks are mapped to rate limiting, DDoS protection, and resource scaling in accordance with ISO/IEC 27033. Port scanning events are linked to logging, firewall rule tightening, and incident handling procedures corresponding to ISO/IEC 27035. Web attacks are associated with WAF activation, patching, and application log review in line with ISO/IEC 27034.

An important feature of the proposed module is the distinction between simple and complex actions. Simple actions, such as block ip, rate limit, or enable waf rule, can be executed automatically by calling an external service. More complex actions, such as host isolation, forensic analysis, or security policy adjustment, remain under administrator control. This combination of automation and expert intervention improves the flexibility of the system and reflects practical cybersecurity workflows.

Unlike traditional decision-support systems that stop at the stage of recommending actions, the proposed approach includes an additional evaluation layer. Its purpose is to estimate whether the selected actions are likely to mitigate the attack. This task is formulated as a binary classification problem:

$$y = ML(A, F, V, D, S)$$

Where y indicates whether the attack is mitigated, A is the attack type, F is the frequency, V is the vulnerability level, D is the defense efficiency, and S is the action strength.

$$S = \sum_{i=1}^{n} w_i a_i$$

Where a_i indicates whether action i was applied and w_i is its relative effectiveness weight. The machine learning model uses the following input features:

- attack type,
- frequency,
- vulnerability,
- defense efficiency,
- action strength.

The target variable is a binary label indicating whether the cybersecurity incident was successfully mitigated. The machine learning component of the system is implemented using a Random Forest classifier. The model is trained on synthetic data using the following procedure:

rf_model = RandomForestClassifier(random_state=42)

rf_model.fit(X_train, y_train)

The Random Forest classifier was implemented using the scikit-learn library. In the current prototype, the default RandomForestClassifier configuration was used with random_state = 42 to ensure reproducibility. This means that the number of trees was set to 100, maximum tree depth was not explicitly restricted, and no class weighting was applied. The attack type was encoded as a fixed numerical identifier for prototype simplicity, while the remaining features were numerical. Since Random Forest is a tree-based algorithm, feature normalization was not required. However, for a more rigorous production-level implementation, one-hot encoding or categorical encoding of attack types should be applied, and hyperparameter tuning should be performed.

This implementation allows the model to learn the relationship between cybersecurity parameters and mitigation outcomes. The Random Forest algorithm was selected because of its strong performance on structured tabular data, robustness to nonlinear relationships, and interpretability compared to more complex black-box models. Random Forest has also been widely used in cybersecurity applications for classification and anomaly analysis [1].

Since real labeled datasets describing the effectiveness of administrator actions are difficult to obtain, a synthetic training dataset was generated using expert-inspired rules. The training procedure includes dataset generation, train/test split, model fitting, and evaluation using accuracy, confusion matrix, precision, recall, and F1-score.

For empirical reproducibility, the synthetic dataset generation procedure was explicitly defined. In this study, the dataset consisted of 3000 cybersecurity events. Each event was assigned to one of six attack categories: Botnet, Brute Force, DoS/DDoS, Normal, Port Scan, and Web Attack. The numerical features, including attack frequency, vulnerability level, and defense efficiency, were

generated within a normalized continuous range from 0 to 10. These values were used to simulate different cybersecurity conditions, from low-risk events to high-risk attack scenarios. A risk proxy value was calculated using attack frequency, vulnerability level, and defense efficiency. The action strength feature was calculated as a weighted sum of selected or executed response actions. The binary target variable indicated whether the attack was mitigated or not. The dataset was divided into training and testing subsets using an 80/20 split, and the Random Forest classifier was evaluated on unseen test data.

The numerical features were generated from a uniform distribution in the range from 0 to 10. A fixed random seed was used to ensure reproducibility of the generated dataset.

The experimental dataset was generated synthetically because publicly available cybersecurity datasets usually contain traffic features and attack labels, but do not include ISO-based recommended actions, executed actions, action strength, and final mitigation outcomes. These variables are necessary for evaluating the full decision-support process proposed in this study. Table 3 summarizes the main parameters used to generate the synthetic cybersecurity dataset.

Table 3 – Parameters of synthetic dataset generation

Parameter	Value
Dataset size	3000 cybersecurity events
Random seed for dataset generation	7
Attack categories	Botnet, Brute Force, DoS/DDoS, Normal, Port Scan, Web Attack
Frequency distribution	Uniform distribution in the range from 0 to 10
Vulnerability distribution	Uniform distribution in the range from 0 to 10
Defense efficiency distribution	Uniform distribution in the range from 0 to 10
Action execution probability	0.75 for each recommended action
Noise distribution	Normal distribution with mean 0 and standard deviation 0.8
Target variable	Binary mitigation outcome: 1 = mitigated, 0 = not mitigated
Train/test split	80/20
Random state for model training	42
Machine learning model	Random Forest classifier

These parameters make the experimental procedure reproducible because the dataset size, feature distributions, random seeds, action execution logic, noise level, and target generation rule are explicitly defined.

This module allows the system not only to recommend actions, but also to estimate whether these actions are likely to be sufficient. Such a feedback oriented design significantly strengthens the practical value of the system.

To reduce data leakage during model evaluation, the dataset was divided into training and testing subsets before model evaluation, and the test set was not used during model fitting. Stratified splitting was applied to preserve the distribution of mitigated and non-mitigated cases. At the same time, since the mitigation label is generated using action strength in the synthetic dataset, the relationship between action strength and the target variable is intentionally embedded in the prototype. This is acknowledged as a limitation of synthetic validation, and future work should use real incident response outcomes as target labels.

The sequence of system operations is illustrated in Figure 1. First, a cybersecurity event is collected from the data source. The event is passed to the fuzzy inference module, which computes the $RiskScore$ and assigns a risk level. Based on the attack type and risk level, the decision-support module generates ISO-based recommendations. If the selected action belongs to the set of simple automated actions, the system executes it automatically through an external service. Otherwise, the action is left for manual execution by the administrator.

Next, the machine learning model receives the event parameters together with the action-related features and predicts whether the implemented actions are likely to mitigate the threat. Finally, the processed event data is sent to the reporting module, where it is included in daily, weekly, or monthly reports.

This sequence reflects a closed-loop decision-support process: event detection → fuzzy risk estimation → action recommendation → action execution → ML (Random Forest) effectiveness evaluation → reporting.

Such a workflow is especially useful in complex environments where administrators must process many events in a short time and require not only alerts but also interpretable recommendations and outcome estimates.

Results and discussion

The experimental evaluation of the proposed hybrid intelligent system was conducted to assess its performance in cybersecurity risk estimation, action recommendation, and prediction of defense effectiveness. The evaluation considered both the individual behavior of the fuzzy risk assessment module and the performance of the machine learning classifier within the integrated system pipeline.

The experiments were designed to answer three main questions. First, whether the fuzzy model produces interpretable and stable risk estimates under different attack conditions. Second, whether the machine learning model can reliably predict whether the selected actions are sufficient to mitigate the attack. Third, whether the integration of fuzzy logic, ISO-based recommendation rules, and machine learning improves the overall quality of decision support.

To evaluate the proposed approach, a synthetic dataset consisting of 3000 cybersecurity events was generated. Each event was described by the following attributes:

- attack type,
- frequency,
- vulnerability level,
- defense efficiency,
- strength of applied actions.

The attack type corresponds to one of the predefined categories used in the system, including Botnet, Brute Force, DoS/DDoS, Normal, Port Scan, and Web Attack. The remaining parameters were generated within normalized ranges and represent simplified but realistic characteristics of cybersecurity incidents. Such a design made it possible to simulate different combinations of weak and strong system states and different response strategies.

The fuzzy inference module was applied to each generated event in order to compute a numerical risk score. The risk score was then converted into one of three discrete categories: LOW, MEDIUM, and HIGH. These values were used by the decision-support module to select ISO-based response actions.

For the machine learning stage, the target variable was defined as a binary mitigation outcome:

$$y \in \{0, 1\}$$

where y = 1 indicates that the attack was mitigated and y = 0 indicates that the attack was not mitigated.

The action strength feature was calculated as a weighted sum of the recommended or executed actions:

$$S = \sum_{i=1}^{n} w_i \, a_i$$

where a_i denotes the application of action i, and w_i is the relative weight of this action.

The dataset was divided into training and testing subsets using an 80/20 split. The machine learning component was implemented using a Random Forest classifier, which was selected because of its robustness and suitability for structured cybersecurity data [1].

The fuzzy module was evaluated by analyzing the generated RiskScore values under different combinations of input parameters. In general, the model produced higher risk scores when attack frequency and vulnerability were high while defense efficiency was low. Conversely, the system assigned lower scores to events with strong defense efficiency and low attack intensity.

The results indicate that the fuzzy model is consistent with expert reasoning and allows interpretable risk assessment. This is particularly important in cybersecurity applications, where uncertainty and incomplete information are common [2, 3].

For practical interpretation, the following thresholds were used:

- LOW risk: $0 \leq \text{RiskScore} < 250$,
- MEDIUM risk: $250 \leq \text{RiskScore} < 650$,
- HIGH risk: $\text{RiskScore} \geq 650$.

These categories were later used by the recommendation module to determine the severity of the incident and assign suitable actions.

The Random Forest classifier was trained to predict whether the selected security actions were sufficient to mitigate the attack. The machine learning model was implemented in Python using the following training procedure:

```
rf_model = RandomForestClassifier(random_state=42)
rf_model.fit(X_train, y_train)
```

The performance of the machine learning model is illustrated in Figure 2. The confusion matrix shows that the model correctly classifies the majority of cybersecurity events. In particular, 344 non-mitigated events and 192 mitigated events were correctly identified. The number of misclassifications is relatively low, with 38 false positives and 26 false negatives. This indicates that the model is capable of distinguishing between effective and ineffective security responses within the synthetic experimental setting.

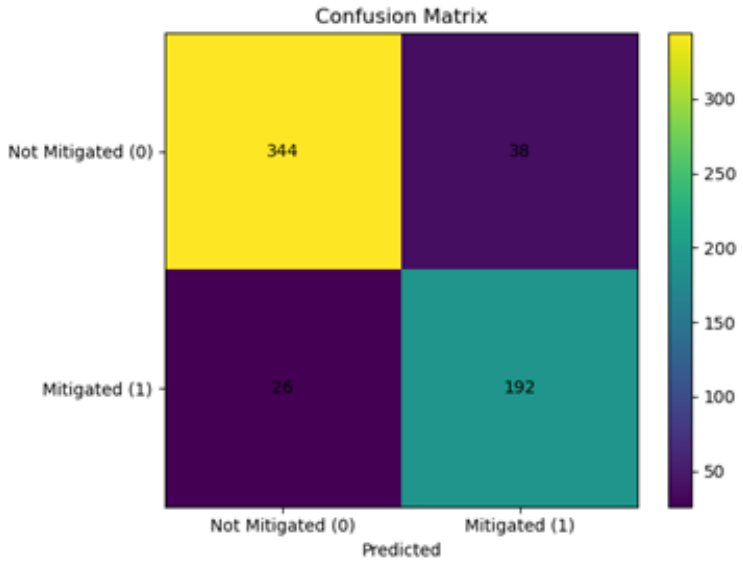

Figure 2 – Confusion matrix of the Random Forest model

In the context of cybersecurity decision support, these two error types have different operational meanings. A false positive means that the model predicts successful mitigation, although the incident is actually not mitigated. This error may be more dangerous because it can create a false sense of security and lead administrators to stop further investigation too early. A false negative means that the model predicts mitigation failure, although the incident is actually mitigated. This may lead to additional review or repeated response actions, but it is generally safer than overlooking an unresolved threat. Therefore, confusion matrix analysis is important because it shows not only overall accuracy, but also the operational risk of different prediction errors.

The overall model accuracy reached 0.89, indicating the model's predictive capabilities within the synthetic experimental environment. Precision and recall values were balanced for both classes, with slightly higher performance for the unmitigated class. This behavior is expected, as the model is trained on synthetic data with varying levels of risks and actions. The detailed classification metrics are summarized in Table 4.

Table 4 – Classification performance of the Random Forest model

Class	Precision	Recall	F1-score
Not Mitigated (0)	0.93	0.90	0.91
Mitigated (1)	0.83	0.88	0.86

To estimate the benefit of the proposed hybrid architecture, its performance was compared with simpler decision-support approaches. The comparison included a rule-based baseline, a fuzzy-only model, and the complete hybrid model that combines fuzzy logic with machine learning.

The comparison results are presented in Table 5. The rule-based baseline provides high interpretability but limited adaptability. The fuzzy-only model improves the handling of uncertainty and provides more flexible decision-making. However, the hybrid model demonstrates the best overall performance because it combines interpretable risk estimation with data-driven evaluation of action effectiveness.

Table 5 provides a conceptual comparison of decision-support approaches. The rule-based and fuzzy-only models are used as baseline approaches to explain the limitations of fixed rules and risk-only assessment. The quantitatively evaluated component of the proposed hybrid system is the Random Forest mitigation prediction model, which achieved an accuracy of approximately 0.89 on the test set.

Table 5 – Conceptual comparison of decision-support approaches

Model	Role in decision support	Adaptability	Interpretability	Experimental status
Rule-based baseline	Fixed mapping between attack type and actions	Low	High	Conceptual baseline
Fuzzy-only model	Risk assessment under uncertainty	Medium	High	Risk assessment component
Hybrid model	Fuzzy risk assessment, ISO-based action selection, Random Forest mitigation prediction, and reporting	High	High	Experimentally evaluated, accuracy ≈ 0.89

To clarify the role of the proposed architecture, the hybrid system was compared conceptually with simpler decision-support approaches. The comparison included a rule-based baseline, a fuzzy-only model, and the complete hybrid model. The rule-based baseline represents fixed mapping between attack types and response actions. This approach is interpretable but limited in adaptability. The fuzzy-only model improves uncertainty handling and provides interpretable risk assessment, but it does not evaluate whether selected actions are likely to mitigate the attack. The complete hybrid model combines fuzzy risk assessment, ISO-based action selection, Random Forest mitigation prediction, and reporting. Table 5 provides a conceptual comparison of these decision-support approaches. The rule-based and fuzzy-only models are used as baseline approaches to explain the limitations of fixed rules and risk-only assessment. The quantitatively evaluated component of the proposed hybrid system is the Random Forest mitigation prediction model, which achieved an accuracy of approximately 0.89 on the test set.

The security action recommendation module is aligned with international cybersecurity standards. Each type of cyberattack is associated with a set of response actions derived from ISO/IEC standards, including ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27033, ISO/IEC 27035, and ISO/IEC 27034.

This mapping ensures that the recommended actions follow best practices in information security management and provides a structured approach for system administrators. The integration of ISO standards enhances the potential applicability of the proposed system for structured cybersecurity decision support.

The action strength feature is important because it allows the model to consider not only attack conditions, but also the expected strength of selected response actions. This reflects practical cybersecurity logic, where the mitigation outcome depends on both the severity of the incident and the quality of the response. In the current prototype, action strength is calculated as a weighted sum of recommended or executed actions. Since these weights are expert-based assumptions, future work should validate or calibrate them using real incident response data. This result is important because it demonstrates that cybersecurity decision support should not depend only on the attack properties themselves. It is also necessary to consider the actual response actions and their potential effectiveness.

In addition to evaluating the fuzzy and machine learning components separately, the entire system was tested as a unified pipeline. The workflow included the following stages:

1. event generation or collection,
2. fuzzy risk estimation,
3. ISO-based action recommendation,
4. automatic or manual action execution,
5. machine learning evaluation of mitigation,
6. report generation.

The integrated system successfully processed simulated events and produced structured outputs that included:

- event identifier,
- timestamp,
- attack type,
- suspicious IP address,
- fuzzy risk score,
- risk level,
- recommended actions,
- executed actions,
- predicted mitigation outcome.

This indicates that the proposed architecture is suitable for prototype-level cybersecurity decision support in multistage workflows. The experimental results suggest that the proposed hybrid model provides a balanced combination of interpretability, flexibility, and predictive capability. The fuzzy component supports reasoning under uncertainty and reflects expert knowledge, while the machine learning model strengthens the system by evaluating the probable effectiveness of the selected response actions.

The obtained results indicate that the machine learning component can be used as an evaluation mechanism within the proposed hybrid intelligent system. Unlike traditional rule-based approaches, the model does not only recommend actions but also estimates whether these actions are likely to be sufficient for threat mitigation. This makes the system more practical for real cybersecurity decision support, since administrators receive not only recommendations but also an additional prediction of response effectiveness.

At the same time, the study has several limitations. First, the experiments were carried out on synthetic data, which may not fully reflect the complexity of real operational cybersecurity environments. Second, the response action weights were assigned heuristically, and further validation with expert knowledge or real incident data is required. Third, the current reporting module is

implemented as a simplified prototype and can be extended in future work using large language models for more advanced report generation.

Another limitation is related to the maintenance of the fuzzy rule base when the number of corporate knowledge assets, attack scenarios, and security controls increases. In large organizations, the expansion of infrastructure may require additional fuzzy rules and more detailed membership functions. This can make manual rule updating more complex and may increase the risk of inconsistent, overlapping, or outdated rules. Therefore, future development of the system should include expert validation procedures, periodic rule revision, adaptive rule tuning, and possible semi-automated knowledge base updating mechanisms. This would help keep the fuzzy rule base scalable and consistent in larger organizational environments.

The obtained results demonstrate that the proposed hybrid architecture can serve as a practical basis for intelligent cybersecurity decision support systems.

Conclusion

This study presented a hybrid intelligent decision-support system for the selection and evaluation of information security measures in organizational environments. The proposed approach integrates fuzzy logic, ISO-based rule systems, and machine learning into a unified multi-stage architecture.

The fuzzy inference module enables the modeling of uncertainty in cybersecurity risk assessment by using linguistic variables such as attack frequency, vulnerability level, and defense efficiency. This provides interpretable and flexible risk estimation that reflects real-world expert reasoning. Based on the computed risk levels, the decision module generates security actions aligned with international standards, including ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27035.

A key contribution of the proposed system is the integration of a machine learning component that evaluates the effectiveness of the selected response actions. The Random Forest classifier demonstrated strong performance, achieving an accuracy of approximately 0.89 and balanced precision and recall values across both classes. This indicates that the model is capable of predicting mitigation outcomes within the synthetic experimental setting.

The experimental results suggest that the proposed hybrid architecture can improve the interpretability and adaptability of cybersecurity decision support within the synthetic experimental environment. Unlike traditional rule-based approaches, the proposed system does not only estimate risk and recommend actions, but also predicts the outcome of these actions. This provides a more complete and practical solution for real-world cybersecurity management.

Another important aspect of the system is the reporting module, which generates structured daily, weekly, and monthly security reports. These reports include detailed information about each event, such as attack type, suspicious IP address, risk level, recommended and executed actions, and predicted mitigation outcome. This functionality demonstrates the applicability of the proposed approach for operational cybersecurity monitoring and decision-making.

Despite the promising results, several limitations should be noted. First, the experimental evaluation was conducted using a synthetic dataset, which may not fully capture the complexity of real-world cybersecurity environments. Second, the effectiveness of response actions was modeled using predefined weights, which may require further validation and tuning based on expert knowledge or real incident data. Third, the current system uses simplified rule sets and can be extended to incorporate more complex attack patterns and dependencies.

Future work will focus on several directions. First, the system can be extended by integrating real-world cybersecurity datasets, such as intrusion detection system logs or SIEM data, in order to improve model robustness and generalization. Second, the fuzzy rule base can be refined using expert knowledge or automated rule learning techniques to enhance risk estimation accuracy. Third, more advanced machine learning models, including deep learning and ensemble methods, can be explored to further improve mitigation prediction performance. Future improvements should also address the scalability of the fuzzy rule base, since larger corporate environments may require more complex rule structures, expert validation, and adaptive updating mechanisms.

Since the evaluation was performed on synthetic data, the obtained results should be interpreted as prototype-level validation rather than evidence of final operational effectiveness. The results demonstrate the feasibility and potential applicability of the proposed hybrid architecture within a controlled experimental environment. Further testing on real SIEM logs, IDS alerts, firewall logs, and organizational incident response records is required to assess the generalization ability of the proposed system in real cybersecurity environments.

Another promising direction is the integration of large language models for intelligent report generation and automated analysis of cybersecurity incidents. Such models can enhance the interpretability of results and provide natural language explanations for recommended actions. In addition, future work may include the development of a fully automated response system integrated with real security infrastructure, such as firewalls, intrusion prevention systems, and cloud-based security services.

Overall, the proposed hybrid intelligent system provides a flexible and extensible framework for cybersecurity decision support. It combines the strengths of fuzzy logic, standard-based reasoning, and machine learning, and can serve as a foundation for the development of next-generation intelligent information security systems.

Acknowledgment:

The author acknowledges the guidance of supervisor A.Zh. Akzhalova and the support of the AI and Cybersecurity research team, which contributed to the development of this work.

REFERENCES

1 Apruzzese, G., et al. The Role of Machine Learning in Cybersecurity. Digital Threats: Research and Practice, 4 (1), 1–38 (2022). https://doi.org/10.1145/3545574

2 Kerimkhulle, S., et al. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things. Symmetry, 15 (10), 1958 (2023). https://doi.org/10.3390/sym15101958

3 Merola, F., Bernardeschi, C., Lami, G. A Risk Assessment Framework Based on Fuzzy Logic for Automotive Systems. Safety, 10 (2), 41 (2024). https://doi.org/10.3390/safety10020041

4 Soori, M., et al. AI-Based Decision Support Systems in Industry 4.0: A Review. Journal of Economy and Technology, 4, 206–225 (2024). https://doi.org/10.1016/j.ject.2024.08.005

5 Singer, P., Friedman, A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press (2014). https://doi.org/10.1093/wentk/9780199918096.001.0001

6 Peltier, T.R. Information Security Policies, Procedures, and Standards. CRC Press (2021).

7 Ahmed, M., Mahmood, A., Hu, J. A Survey of Network Anomaly Detection Techniques. Journal of Network and Computer Applications, 60, 19–31 (2015). https://doi.org/10.1016/j.jnca.2015.11.016

8 Wang, M., et al. Machine Learning for Networking: Workflow, Advances and Opportunities. IEEE Network, 32 (2), 92–99 (2018). https://doi.org/10.1109/MNET.2017.1700200

9 Ludonga, A., Singo, S. Systematic Review Cyber Risk Management: Frameworks, Strategies, and Case Studies in Cybersecurity (2025). https://doi.org/10.5281/zenodo.17372361

10 Zadeh, L.A. Fuzzy Sets. Information and Control, 8 (3), 338–353 (1965). https://doi.org/10.1016/S0019-9958(65)90241-X

11 ISO/IEC 27001:2022 Information Security Management Systems (2022). https://www.iso.org/standard/27001

12 Tukaram, L. Deep Learning in Cybersecurity: Applications, Challenges, and Future Prospects. International Journal of Innovations in Science Engineering and Management, 4 (2), 27–33 (2025). https://doi.org/10.69968/ijisem.2025v4i227-33

Амирбаева А.А.,
магистрант, ORCID ID: 0009-0009-3180-2990,
e-mail: adinaxanova2@gmail.com

Қазақстан-Британ техникалық университет, Алматы қ., Қазақстан

КИБЕРҚАУІПТЕРДІ БАҒАЛАУ ЖӘНЕ ҚОРҒАНЫС ШАРАЛАРЫН ТАҢДАУ ҮШІН ГИБРИДТІ ИНТЕЛЛЕКТУАЛДЫ ШЕШІМ ҚАБЫЛДАУДЫ ҚОЛДАУ ЖҮЙЕСІ

Аңдатпа

Ақпараттық қауіпсіздік жүйелерін таңдау ұйымдық тәуекелдерге, инфрақұрылым ерекшеліктеріне, киберқауіптерге және нормативтік талаптарға байланысты күрделі міндет. Дәстүрлі тәсілдер көбінесе сарапшылық бағалауға және қолмен талдауға негізделетіндіктен, олардың бейімделгіштігі мен икемділігі шектеулі. Бұл жұмыста тәуекелдерді бағалау және қауіпсіздік шараларын ұсыну үшін анық емес логиканы, машиналық оқытуды және ISO стандарттарын біріктіретін гибридті интеллектуалды шешім қабылдауды қолдау жүйесі ұсынылады. Анық емес логика модулі шабуыл жиілігі, осалдық деңгейі және қорғаныс тиімділігі сияқты параметрлер негізінде тәуекелді бағалайды. Есептелген тәуекел деңгейіне сәйкес жүйе ISO/IEC халықаралық стандарттарына негізделген қауіпсіздік шараларын ұсынады. Сонымен қатар, таңдалған қорғаныс шараларының тиімділігін бағалау үшін Random Forest машиналық оқыту моделі қолданылады. Эксперименттік нәтижелер ұсынылған жүйенің жоғары дәлдік пен бейімделгіштік қасиеттерге ие екенін көрсетті.

Түйін сөздер: киберқауіпсіздік, анық емес логика, машиналық оқыту, тәуекелдерді бағалау, шешім қабылдауды қолдау жүйелері, ақпараттық қауіпсіздік

Амирбаева А.А.,
магистрант, ORCID ID: 0009-0009-3180-2990,
e-mail: adinaxanova2@gmail.com

Казахстанско-Британский технический университет, г. Алматы, Казахстан

ГИБРИДНАЯ ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ ОЦЕНКИ КИБЕРРИСКОВ И ВЫБОРА ЗАЩИТНЫХ МЕР

Аннотация

Выбор подходящих систем информационной безопасности представляет собой сложную задачу, зависящую от организационных рисков, характеристик инфраструктуры, киберугроз и нормативных требований. Традиционные подходы, основанные на экспертной оценке и ручном анализе, часто обладают ограниченной адаптивностью и масштабируемостью. В данной работе предлагается гибридная интеллектуальная система поддержки принятия решений, объединяющая нечеткую логику, машинное обучение и стандарты ISO в области информационной безопасности. Модуль нечеткого вывода выполняет оценку риска в условиях неопределенности с использованием параметров частоты атак, уровня уязвимости и эффективности защиты. На основе вычисленного уровня риска система формирует рекомендации по реагированию в соответствии с международными стандартами ISO/IEC. Дополнительно используется модель Random Forest для оценки эффективности выбранных мер защиты. Экспериментальные результаты показали высокую точность и адаптивность предложенной архитектуры.

Ключевые слова: кибербезопасность, нечеткая логика, машинное обучение, оценка риска, системы поддержки принятия решений, информационная безопасность.