Received: 30 October 2024 | Revised: 17 February 2025 | Accepted: 10 March 2025 | Published online: 18 April 2025

RESEARCH ARTICLE

Journal of Computational and Cognitive Engineering
2025, Vol. 00(00) 1–11
DOI: 10.47852/bonviewJCCE52024683

BON VIEW PUBLISHING

Development and Implementation of an Advanced Fuzzy Expert System for the Assessment of Information Security Risks

Alibek Barlybayev[1,*] and Alua Turginbayeva[2]

[1]*Higher School of Information Technology and Engineering, Astana International University, Kazakhstan*

[2]*Department of Computer and Software Engineering, L.N. Gumilyov Eurasian National University, Kazakhstan*

Abstract: This research paper describes an improved fuzzy expert system for assessing information security (IS) risks. More and more organizations are facing significant IS problems. These problems arise in protecting corporate information systems from these threats. Traditional IS risk assessment methodologies often have difficulties. Difficulties arise in eliminating ambiguity and uncertainty that are characteristic of these dynamic environments. This study presents a new approach using fuzzy logic. Fuzzy logic is used to accurately identify and evaluate the subtle intricacies of each IS risk factor. Using linguistic variables and fuzzy sets, the proposed system effectively reproduces the reasoning processes. This research paper delineates the formulation of an advanced fuzzy expert system aimed at enhancing IS risk assessments amidst the evolving complexity of cyber threats. By utilizing linguistic variables and fuzzy sets, the proposed system effectively replicates human-like reasoning processes. This allows for a flexible and dynamic framework for risk assessment. This methodology is characterized by the effective integration of both qualitative and quantitative data, resulting in a comprehensive risk assessment model. The usefulness of this model is validated by its application in learning management systems. The systems evaluated include Platonus, SmartENU, Directum, MOOCENU, KPI, and a university website. Quantitative evaluations were conducted according to standards such as NIST 800-30, ISO/IEC 27001, BS 7799, and a proposed model, yielding scores that range from 0.205 to 0.998 across different criteria and systems. Correlation analysis between the standards and the expert-proposed model revealed high consistency, with correlation coefficients ranging from 0.994 to 0.996. These results underline the robustness of the proposed model in aligning closely with established IS standards and suggest its potential for broader application in IS risk assessment.

Keywords: fuzzy logic, information security risk assessment, cybersecurity, expert systems, decision-making, risk management

1. Introduction

Risks materialize in different dimensions and manifest themselves at different hierarchical levels. Each of these levels has a differentiated impact and requires individual preventive strategies. Modern organizations face a variety of security threats, including malware, ransomware, phishing, eavesdropping, impersonation, and denial-of-service attacks, among others. These threats collectively pose significant challenges to the security of information systems. The primary concern in these organizations is IT operational risk. It arises from inadequately defined internal processes, personnel issues, and system vulnerabilities or from external threats such as natural disasters or cyberattacks. Risk management is therefore recognized as a critical element of IT security strategies. Various international frameworks and standards, including ISO/IEC 27005, ISO Guide 73:2009, COSO, and NIST SP 800-30, provide different perspectives and definitions of risk. This study focuses on risk assessment, a systematic process for identifying, evaluating, and prioritizing information security (IS) risks. The process involves a detailed analysis of threat and vulnerability data to assess the potential impact on the organization and the likelihood of their occurrence. Risk assessment is considered a critical and central step in the development of an Information Security Management System in the broader context of risk management. It is essential that risks are maintained within acceptable limits determined by the defined risk appetite of the organization. Initiating an IS risk assessment requires a clear definition and understanding of the chosen methodology. Methodologies can be broadly divided into two types: qualitative and quantitative. These approaches are critical to ensuring that organizational risks are systematically assessed and managed in accordance with the risk tolerance levels of senior management.

In quantitative risk analysis, monetary and numerical values are assigned to every aspect of the risk evaluation process. Each component is quantified and incorporated into a mathematical framework to calculate both the aggregate and residual risks. Due to its intricate nature, time-consuming characteristics, and overall complexity, this form of risk assessment is seldom employed independently in practical applications. It is more frequently integrated with a qualitative approach. Moreover, the execution of

***Corresponding author:** Alibek Barlybayev, Higher School of Information Technology and Engineering, Astana International University, Kazakhstan. Email: alibek_barlybayev@aiu.edu.kz

such assessments can incur substantial costs. Qualitative analysis of risk depends on the subjective evaluations of team members within the IS risk assessment framework to assess the overall risk to information systems. This approach involves analyzing various risk scenarios, ranking the severity of threats, and evaluating potential mitigation strategies. The reliance on expert judgment, established best practices, intuitive understanding, and the assessor's prior experiences characterizes qualitative methods. Instead of numerical values, qualitative risk analysis categorizes risks into a hierarchy, typically labeled as low, medium, high, and critical. The choice of an optimal method is crucial for effective IS risk management, acknowledging that no single risk analysis or assessment method is suitable for every situation or objective.

The primary goal of IS and business is to safeguard the organization and its associated IT assets, ensuring the confidentiality, integrity, and availability of information and information systems involved in the reception, processing, storage, and distribution of such information and securing organizational resources. The intricacy of the process for decision-making is directly related to the complexity of the problem at hand. Assessing the risk to an information system and choosing suitable security measures or IT solutions is a complex and challenging task. This complexity often stems from limited information, scarce resources, and organizational time constraints. As a result, this situation can be described as a problem of multi-criteria decision-making (MCDM).

Decision support methodologies can be divided into three main types [1]: (1) MCDM, (2) programming, and (3) artificial intelligence (AI).

1) Multi-attribute Utility Methods: Analytic Hierarchy Process (AHP) and Analytic Network Process.
2) Outranking Methods: Electre, Promethee, and Qualiflex [2].
3) Trade-off Methods: Topsis and Vikor.
4) Additional MCDM Approaches: Simple Multi-Attribute Rating Technique [3], Decision-Making Trial and Evaluation Laboratory, and Simple Additive Weighting [4].

IS risk management requires a comprehensive assessment of potential threats and vulnerabilities. This is necessary to assess their impact on organizational assets. In accordance with the principles of MCDM, this complex task requires the integration of various types of data and expert judgment. The main challenge is to effectively assess and prioritize across multiple criteria. These criteria range from the likelihood of a threat occurring to the potential severity of the impact. Security measures can be informed by the assessment. The relevance of this study is due to the urgent need to improve IS risk assessment methodologies. This is caused by the emergence of rapidly evolving and increasingly complex cyber threats. Traditional approaches often fail to manage the ambiguity and complexity inherent in modern cyber environments. Poor ambiguity management can lead to significant security breaches and vulnerabilities. Moreover, the dynamic nature of cyber threats requires adaptive and flexible strategies. These strategies must keep up with the pace of technological progress. By applying fuzzy logic, this study aims to provide a more nuanced and context-sensitive approach to risk assessment. This study seeks to bridge the gap between traditional methods and the practical needs of organizations in managing and mitigating IS risks.

To address these issues, our methodology incorporates an MCDM framework. It uses fuzzy logic to integrate qualitative and quantitative judgments into a single decision-makers framework. Fuzzy logic excels at managing the inherent ambiguities and subtle dynamics of risk factors. A fuzzy logic-based system can approach human reasoning under uncertainty.

This study addresses significant challenges that organizations face in protecting their information systems. An innovative integration of fuzzy logic with traditional risk assessment methods is presented. The system allows for a more efficient identification of subtle dynamics of IS threats. Linguistic variables and fuzzy sets are used to simulate human thinking. This creates a more dynamic and flexible framework for risk assessment. This approach not only facilitates the management of ambiguity and uncertainty common in cybersecurity risk assessments. The proposed approach also enhances the system's ability to combine both qualitative and quantitative data into a comprehensive risk analysis model.

This paper contributes to the field of IS risk assessment. It presents an advanced fuzzy expert system designed to skillfully navigate the ambiguity and dynamic nature of cyber threats. By incorporating fuzzy logic, the system not only improves the adaptability and accuracy of risk assessments. It also bridges the gap between quantitative data and qualitative judgments, providing a more comprehensive approach to security threat management. Moreover, the application of this system to the assessment of learning management system (LMS) platforms highlights its practical relevance and adaptability.

The paper is organized as follows: Section 1 introduces the study context and the motivation for employing fuzzy logic in IS risk assessment. Section 2 reviews relevant literature to establish a theoretical foundation and identify existing gaps. Section 3 details the methodology, describing the design and implementation of the fuzzy expert system and the criteria for risk assessment. Section 4 discusses the results of applying the system across various LMS platforms and the implications of these findings. Section 5 concludes the paper by summarizing key contributions, discussing limitations, and suggesting directions for future research.

2. Literature Review

The researchers Abdymanapov et al. [5] in this study propose the use of a fuzzy inference system to evaluate the risks of IS. This system is specifically demonstrated through the analysis of LMS. The primary objective of this paper is to delineate a comprehensive approach to risk assessment within the realm of IS, with a particular focus on LMS. This study aims to address the specific vulnerabilities and challenges associated with these platforms, providing a robust framework for identifying, analyzing, and mitigating potential security threats effectively.

Kerimkhulle et al. [6] investigate the application of fuzzy logic in modeling human reasoning processes. They focus on IS risk assessment in the Industrial Internet of Things (IIoT). Their study demonstrates the adaptability of fuzzy logic in complex decision-making scenarios. This is particularly relevant for the IIoT dynamics. The paper discusses both the challenges and opportunities associated with implementing fuzzy logic in this context. It argues for the usefulness of fuzzy logic in managing the uncertainties typical of IIoT environments. But it also highlights the need for careful attention to rule base construction, membership function design, and deployment of inference engines.

In this research, Alonge et al. [7] present a model for information asset classification and labeling using a fuzzy approach to enhance security risk assessment. The authors detail the components of their model, including the use of fuzzy logic to handle uncertainties in classifying information assets based on their sensitivity and criticality. They also discuss how this model can contribute to more effective security risk assessment within organizations.

Ershadi and Forouzandeh [8] created a hybrid framework that combines several methodologies to improve IS risk management.

They selected research information systems as the subject area. The hybrid framework combines fuzzy failure mode and effects analysis (FMEA), AHP, TOPSIS, and Shannon entropy. The application of this multifaceted approach in both real and simulated settings effectively demonstrates its usefulness. It facilitates comprehensive risk identification, prioritization, and mitigation. The empirical results highlight the effectiveness of the framework in IS risk management.

Peisheng et al. [9] explore the enhancement of information system risk assessment by integrating the AHP with fuzzy theory. This synthesis aims to achieve a more precise and comprehensive evaluation of risks within information systems. The inclusion of fuzzy logic components allows the AHP framework to address and quantify the uncertainties typically associated with risk assessments, thereby yielding more dependable outcomes. The paper also details the real-world applicability of this method, providing insights into how it can be implemented to refine risk management practices effectively.

Kumar et al. [10] introduce a fuzzy symmetric MCDM model tailored to address the uncertainties and imprecisions prevalent in evaluating the security threats to health information systems. This model integrates fuzzy logic to effectively represent and manage ambiguous information in decision-making scenarios, ensuring that each criterion is considered equally, thereby promoting a balanced and impartial assessment of risks. The study emphasizes the urgent need to evaluate a range of adverse factors—such as cyberattacks, data breaches, insider threats, system vulnerabilities, and compliance issues—that could compromise the security of health information systems. The proposed fuzzy symmetric MCDM approach allows decision-making to assess and prioritize these threats based on their potential impact, thereby enhancing the robustness of security measures.

Yang et al. [11] present an advanced method for intelligent IS risk assessment. This method uses causality analysis to refine IS risk assessments in supervisory control and data acquisition (SCADA) systems. Their methodology combines causality inference methods with established risk assessment models. This enables the uncovering of complex interdependencies inherent in SCADA systems and their impact on safety. By applying causality analysis, the method more quickly reveals hidden relationships and dependencies in SCADA networks. This enables more accurate identification of potential safety risks.

The methodology presented in this paper by Erdoğan et al. [12] combines fuzzy logic with MCDM methods. The aim of the study is to create a comprehensive framework for assessing cybersecurity technologies. The authors describe the sequential steps involved in the risk assessment process. These steps cover the selection of criteria, the definition of linguistic variables, the formation of a fuzzy rule base, and the implementation of decision-making using fuzzy inference systems. In addition, an example is provided to illustrate the practical application of the proposed methodology. This example not only demonstrates the applicability of the methodology but also its effectiveness. The method effectively facilitates nuanced and informed decision-making in the field of cybersecurity technology assessment.

A study by Kotenko and Parashchuk [13] highlights the effectiveness of fuzzy algorithms and predicates in managing imprecise or uncertain data. Such data are often encountered in safety assessments. The authors detail how predicates can be strategically used to define safety requirements. This approach significantly improves both the accuracy and practicality of safety assessments in complex industrial automation systems.

Researchers Hart et al. [14] use fuzzy logic to improve the efficiency and effectiveness of privacy risk assessment and prioritization. This method is carefully designed to provide a comprehensive analysis of potential privacy threats and their severity. This allows for more informed risk management decisions for both organizations and individuals. By adopting this approach, stakeholders gain a deeper understanding of privacy vulnerabilities. This allows for more effective measures to be implemented to address and mitigate these risks.

Alfakeeh et al. [15] use oscillating fuzzy sets to provide a unique approach to address the uncertainty in security risk assessments. Traditional fuzzy sets assign a single membership value to each element, ranging from 0 to 1. However, oscillating fuzzy sets allow multiple membership values for each element. This feature more accurately reflects the variability and uncertainty typical in security risk assessment scenarios. By integrating these oscillating fuzzy sets, the model significantly improves the accuracy of risk assessments. It skillfully adapts to the complexities and ambiguities inherent in security-related data management. But implementing such an IS assessment system with oscillating fuzzy sets is a complex and challenging task.

Kumar et al. [16] develop a robust methodology aimed at evaluating the resilience and security of web applications. At the heart of their approach is a fuzzy rule-based system that combines fuzzy logic with rule-based systems to effectively model the intricate interdependencies impacting web application resilience and security. This methodology excels at managing imprecise and uncertain data, facilitating the creation of decision rules grounded in expert knowledge and empirical evidence. Additionally, it incorporates an MCDM component that considers multiple criteria essential for a comprehensive evaluation of key aspects such as scalability, maintainability, reliability, sustainability, authentication, authorization, encryption, and vulnerability assessment. Acknowledging the varying importance of these criteria, the authors employ a weighted approach. This approach is based on expert opinions and literature to prioritize each criterion effectively. This hybrid framework merges the scores from individual criteria to compute an overall sustainability-security score for each web application, which is subsequently used to rank the applications based on their performance in both sustainability and security domains. The validation of this framework through a case study involving real-world web applications confirms its effectiveness. The hybrid MCDM framework based on fuzzy rules not only provides detailed robustness and security for web applications but also provides valuable information to developers, researchers, and stakeholders seeking to improve the design of web applications.

Buldakova and Mikov [17] describe in detail the development process of an IS risk analysis application. They explain the software architecture, describe the algorithms used, and discuss key features. The application included statistical analysis, data visualization, and customizable risk models. This allowed for significant improvements in IS management practices. This integration facilitates a more dynamic and effective approach to managing and mitigating IS risks.

This study [18] examines the common problem of cybersecurity threats in organizations. These threats often arise due to human errors or malicious actions. The authors present a fuzzy methodology aimed at assessing and mitigating these risks. Particular attention is paid to the potential leakage of classified information. Vaczi et al. [18] emphasized that fuzzy logic is adept at modeling and analyzing uncertainties and imprecisions. The paper provides a detailed description of the key components of the methodology, including the use of linguistic variables, the formulation of fuzzy rules, and the implementation of membership functions. All of these are adapted to assess the risk of information leakage due to human

error. The authors further discuss how real-world data can be incorporated into their fuzzy model to assess both the likelihood and potential impact of such security breaches. This demonstrates the effectiveness and applicability of their approach to solving specific cybersecurity problems.

The manuscript by Komazec et al. [19] examines the use of AHP in risk assessment and prioritization. These risks are associated with a rail corridor connecting Piraeus, Belgrade, and Budapest. This study is important because it examines a critical infrastructure project. The project plays a crucial role in improving connectivity and trade across Europe.

Kushwaha et al. [20] developed a new adaptation of the FMEA methodology. Their study focuses on reducing the risks associated with sudden failures in turbine and generator units. The paper describes an integrated decision-makers framework. The study demonstrates the practical application and effectiveness of the modified FMEA approach in real-world conditions.

Risk prioritization is an essential component of operational management in crowd-shipping, which utilizes a distributed network of individuals to transport goods. The research by Švadlenka et al. [21] investigates the identification and prioritization of risks within the context of crowd-shipping providers, utilizing the Cumulative Impact Multi-Attribute Scoring (CIMAS) method. This methodology systematically assesses risks by evaluating their probability and potential impact, thereby enabling providers to efficiently allocate resources and address potential vulnerabilities. The CIMAS method applies a scoring mechanism whereby each risk is evaluated and assigned scores reflecting its likelihood (e.g., low, medium, high) and impact (e.g., minor, moderate, severe). These scores are aggregated to derive a cumulative risk score for each identified risk. Subsequent to the scoring process, risks are organized in descending order based on their cumulative risk scores. This ordered list assists crowd-shipping providers in concentrating efforts on the most critical risks, thereby optimizing operational resilience. Effective risk management with the CIMAS method facilitates superior decision-making concerning resource distribution and operational adjustments in crowd-shipping. Recognizing the most significant risks—such as logistical delays from traffic or driver reliability issues—enables providers to devise targeted strategies that bolster service dependability and enhance customer satisfaction. For example, recognizing driver availability as a high-priority risk due to its substantial influence on delivery timelines might prompt a provider to invest in improved communication tools or driver incentives, ensuring heightened availability during peak demand periods.

Previous studies have extensively explored various MCDM methods, including AHP, TOPSIS, and fuzzy approaches. All of them aim to improve the accuracy of decision-making under uncertainty. However, traditional methodologies often prove inadequate in dynamic and complex environments. This is especially true in IS risk assessment, where rapid changes and ambiguous data are common. Many models face challenges in effectively integrating both qualitative and quantitative data. The difficulty lies in the process of transforming the data so that it is flexible and adaptive. Fuzzy systems are well known for their ability to cope with uncertainty. But such systems often require significant expertise in defining accurate rule bases and membership functions. In IS risk assessment, these may not be available or feasible in practical scenarios.

To overcome these challenges, our approach combines fuzzy logic with MCDM in a universal framework for IS risk assessment [22]. This robust framework is able to adapt to changing data and conditions without constant expert intervention. This synergy facilitates dynamic risk interpretation. The model effectively uses both numerical data and expert judgment. Partial automation of the decision-making process reduces the dependence on expert knowledge at each decision point. This makes it more feasible for organizations with limited access to specialized knowledge. Thus, this integrated approach offers a more practical and scalable solution for IS risk management in various organizational contexts.

3. Research Methodology

This study employs a sophisticated approach using fuzzy logic and the MCDM framework to assess IS risks. This approach is specifically designed to address the inherent uncertainties and imprecisions in cybersecurity threats. The proposed methodology is based on the use of fuzzy sets to encapsulate linguistic uncertainty in qualitative IS risk assessments. These assessments are then quantitatively analyzed to assign risk levels. This assessment takes into account both the predicted impact and the probability of occurrence of each identified risk. To validate the effectiveness of this methodology, it is applied to several real-world scenarios in an educational context. This demonstrates the broad applicability and adaptability of the fuzzy expert system to various information system environments. This practical application highlights the robustness of the approach.

3.1. Risk assessment criteria for software information security

In order to thoroughly assess the IS of software, it is essential to define precise criteria and metrics. This can be done through a detailed analysis of relevant standards. Based on the findings of our previous study [19], a carefully selected list of 79 IS risks was developed. This model serves as a fundamental component for assessing the security posture of software systems. The model ensures that the assessments are both comprehensive and compliant with established industry standards. This study represents a significant advance in IS risk assessment. It presents a comprehensive and innovative approach that synthesizes standards and norms, specialized insights, AI methods, and semantic modeling. The combination of IS standards and specialized knowledge creates a solid foundation for subsequent model development, facilitating a holistic understanding of IS risks. The application of cluster analysis, in particular using k-means in IS standards, is an innovative approach to data-driven risk expansion. This approach reveals patterns and relationships that are not easily observed using conventional methods. Thus, the scope of IS risk evaluation is expanded. In addition, the integration of machine learning algorithms in the development of the IS risk dendrogram represents a significant contribution. The effective application of advanced computational methods to improve risk identification and classification is demonstrated. The use of a heat map as a tool for representing IS risks adds another level of innovation to this study. This new visualization technique facilitates a nuanced understanding of risk relationships and priorities, thus providing a valuable tool for decision-makers in IS management. In addition, the development of a thesaurus containing definitions of concepts, synonyms for the identification of relationships between concepts, and their antonyms represents a semantic improvement strategy. The thesaurus improves the accuracy and flexibility of IS risks. The thesaurus ensures a comprehensive and relevant characterization of risks by classifying evolving terminologies in the dynamic IS field. An ontology model for a structured classification of IS risks was created. This model facilitates the categorization of IS risks using semantic relationships. IS risk semantics offers a systematic method for organizing and managing various risks.

The resulting list serves as a practical tool for enterprises, facilitating the identification and management of IS risks, as the mitigation and reduction of these risks fundamentally underpin the process of ensuring the IS of the enterprise. This meticulously curated list also provides a foundation for constructing threat models, which are instrumental in the development of robust IS systems. Moreover, the risks identified are crucial for evaluating the effects of implemented IS measures on the overall operational efficiency of enterprises. For clarity and as a reference, this research [22] lists these IS risks, providing a systematic framework that assists organizations in improving their comprehension and proactive administration of IS challenges. The IS risk table is presented in a format that aligns comprehensively with the aim of evaluating IS risk associated with hardware and software. Addressing the challenge involves resolving three key questions: the scale of software security, the regulation of user behavior, and the delineation of developers' software criteria. In response, we introduce a methodology for assessing IS that employs fuzzy logic [22].

3.2. Fuzzy logic-based IS risk assessment model

Implementation of fuzzy logic is necessary to increase the flexibility of the IS assessment model. Fuzzy logic provides expert systems with adaptability and variability. These properties allow dynamic assessment of parameters that are initially considered fixed. Fuzzy methodology supports decision-making in scenarios with multiple options, uncertainties, and vulnerabilities. This makes it especially effective in managing complexities and ambiguities. IS is characterized by processes with controversial issues.

Fuzzy logic is particularly useful in dealing with uncertainty. It also formulates decisions on complex and contentious issues easily. The work by Tariq et al. [23] explores the fuzzy AHP method for prioritizing IS management tools. Organizations can facilitate the optimal selection of cost-effective and efficient IS tools. The formalized approach and prioritization processes are in line with ISO/IEC 27001:2013 standards.

The results of this study [24] highlight the advantages of fuzzy logic over purely objective methods. The results show increased accuracy of risk assessment and more favorable return on investment in IS. In addition, Tarik [25] presented a framework for assessing IS in cloud systems using a fuzzy inference system. The effectiveness of the framework in protecting information in a cloud computing environment is confirmed by fuzzy results in real applications using Matlab.

We advocate for a three-tiered approach to evaluating the IS of a software application. The first level utilizes external and internal elements of IS to serve as metrics for the objective of risk evaluation. Here, the risk objective is established. At the second level, risks are characterized, or a segment of the risk taxonomy is defined. The third level expounds on risks, presuming that the second level failed to offer a detailed description. This structural framework can be applied both item by item for the evaluation of particular groups and subgroups of risks and holistically for a comprehensive evaluation of the IS of the software app deployed within the organization.

Building upon the categorization of IS risk assessment measures, we have developed 16 fuzzy machines that utilize the Mamdani inference algorithm. The Matlab framework is optimally configured to facilitate these simulations, as demonstrated in references [26, 27]. This configuration allows for precise execution of the fuzzy logic processes, enabling the fuzzy machines to effectively model and manage the complexities associated with IS risk assessments. This setup highlights the capability of Matlab not only in implementing fuzzy logic but also in enhancing the robustness and reliability of the risk assessment procedures through sophisticated computational techniques.

The 16 fuzzy machines show a close relationship. In the system, features encapsulate numerical representations of individual subclasses. These subclassifications, in turn, clarify the meanings associated with more general classifications. In the field of fuzzy logic, linguistic variables are defined using membership functions to represent imprecise values. An example of the linguistic variable "16. External Risks" is shown in Figure 1. The linguistic variables "Low," "Moderate," and "High" are associated with triangular membership functions ('trimf'). These membership functions play a crucial role in establishing fuzzy boundaries for each linguistic variable. This facilitates the representation and modeling of imprecision and uncertainty within the system. Specifically, their parameterizations are as follows:

"Low": 'trimf', [−0.4, 0, 0.4]
"Moderate": 'trimf', [0.1, 0.5, 0.9]
"High": 'trimf', [0.6, 1, 1.4]

Figure 2 illustrates an expert system designed to evaluate IS risks using fuzzy logic. The system, labeled as ISRISKS, comprises 16 interconnected fuzzy machines. Each fuzzy machine receives specific input variables, processes them using triangular membership functions and the centroid defuzzification technique, and generates corresponding output variables. Below is a structured overview of the inputs and outputs for each of the 16 fuzzy machines:

1) Governance and Compliance Framework. Inputs: Information Security Policies and Procedures, Defining Roles and Responsibilities, Legal Risk, Regulatory Requirements Risk, Risk of Non-Compliance and Inadequate Security Practices,

Figure 1
Linguistic variable external risks

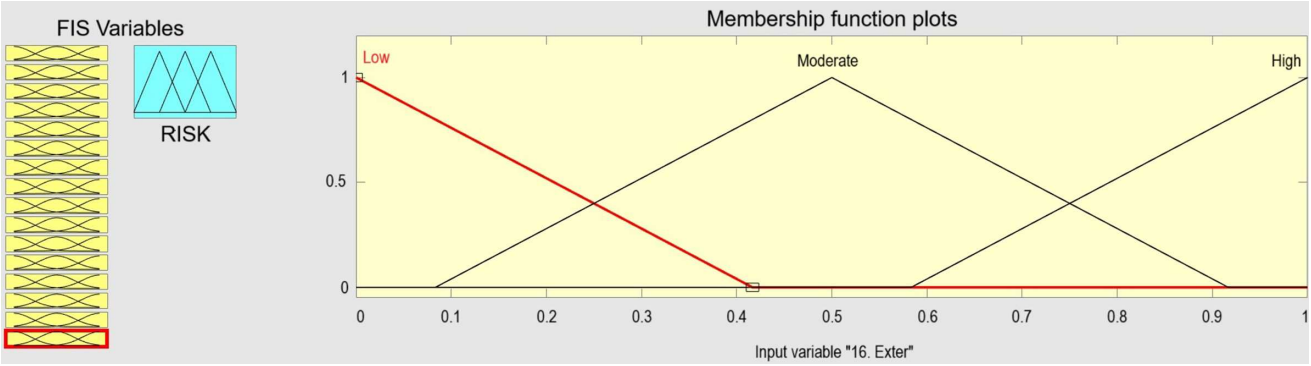
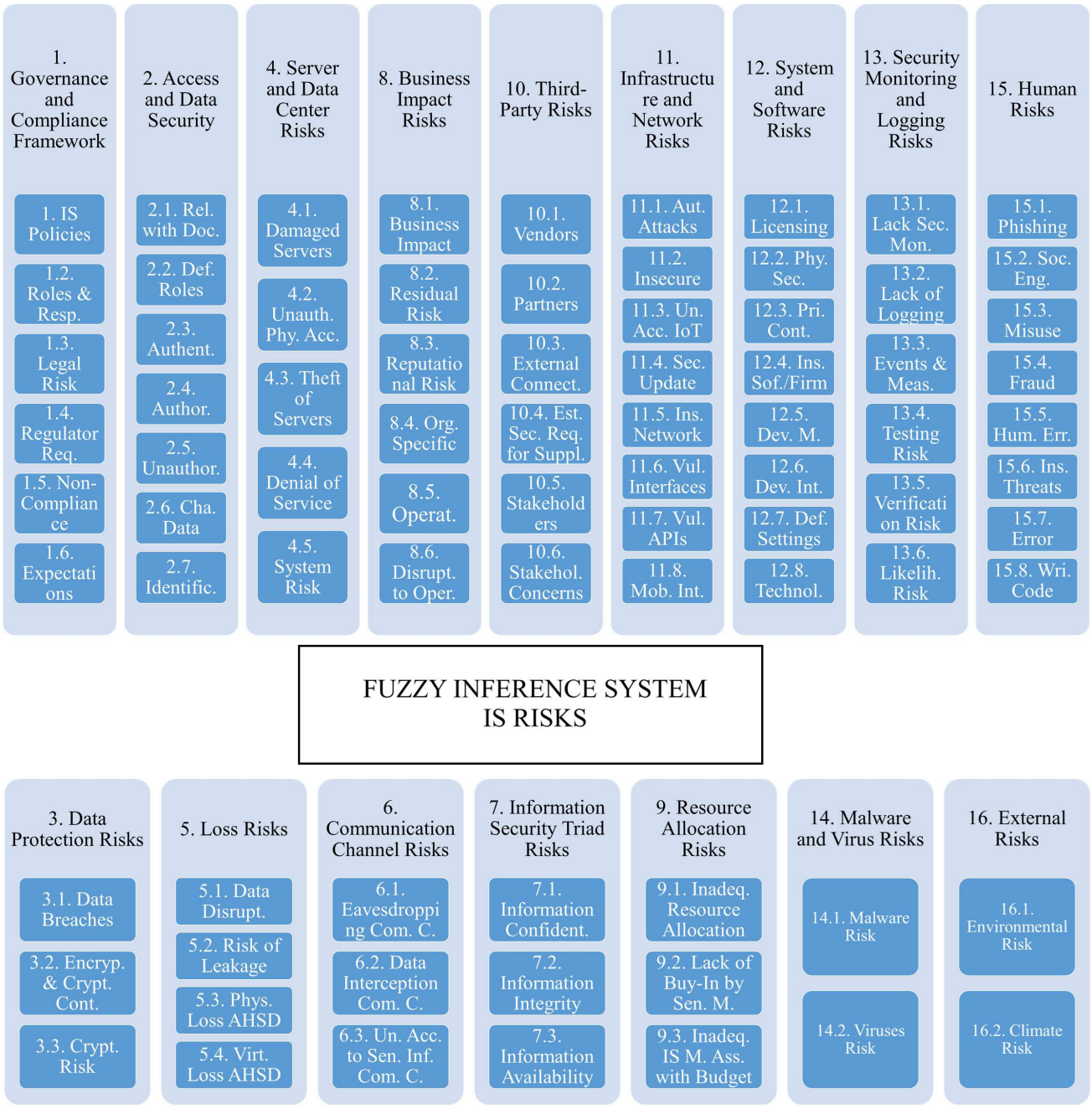


Figure 2
Layout of the fuzzy model risks



Risk of Expectations. Output: Governance and Compliance Framework

2) Access and Data Security. Inputs: Risk Related with Document, Defining Roles and Responsibilities, Risk of Authentication, Risk of Authorization, Risk of Unauthorized Access to Data, Risk of Unauthorized Changes in Data, Risk of Identification. Output: Access and Data Security
3) Data Protection Risks. Inputs: Risk of Data Breaches, Risk of Encryption and Cryptographic Controls, Cryptography Risk. Output: Data Protection Risks
4) Server and Data Center Risks. Inputs: Risk of Damaged Servers and Data Centers, Risk of Unauthorized Physical Access to Servers and Data Centers, Risk of Theft of Servers and Data Centers, Denial of Service (DoS) Risk, System Risk. Output: Server and Data Center Risks
5) Loss Risks. Inputs: Risk of Data Disruptions, Risk of Leakage, Risk of Physical Loss or Theft of Critical Assets, Hardware, Software, Data; Risk of Virtual Loss or Theft of Critical Assets, Hardware, Software, Data. Output: Loss Risks
6) Communication Channel Risks. Inputs: Risk of Eavesdropping Through Communication Channels, Risk of Data Interception Through Communication Channels, Risk of Unauthorized Access to Sensitive Information Through Communication Channels. Output: Communication Channel Risks
7) Information Security Triad Risks. Inputs: Risk of Information Confidentiality, Risk of Information Integrity, Risk of

Information Availability. Output: Information Security Triad Risks

8) Business Impact Risks. Inputs: Risk to Potential Business Impact, Residual Risk, Reputational Risk, Organization's Specific Risk, Operational Risk, Risk of Prolonged Disruptions to Operations. Output: Business Impact Risks
9) Resource Allocation Risks. Inputs: Risk of Inadequate Resource Allocation, Risk of Lack of Buy-In by Senior Management, Risk of Inadequate IS Measures Associated with Proper Allocation of Budget and Personnel. Output: Resource Allocation Risks
10) Third-Party Risks. Inputs: Risk Associated with Third-Party Vendors, Risk Associated with Partners Involved in the Industrial Ecosystem, Risk Associated with External Connections, Establishing Security Requirements for Third-Party Suppliers, Risk Associated with Stakeholders, Stakeholder Concerns. Output: Third-Party Risks
11) Infrastructure and Network Risks. Inputs: Risk of Automated Attacks Against Devices, Risk of Insecure or Default Credentials, Risk of Unauthorized Access to IoT Devices, Lack of Secure Update Mechanisms, Risk of Connections to Insecure Networks, Risk of Vulnerable Interfaces, Risk of Vulnerable API Interfaces, Risk of Insecure Mobile Application Interfaces. Output: Infrastructure and Network Risks
12) System and Software Risks. Inputs: Licensing Risk, Risk of Insufficient Physical Security, Lack of Privacy Controls, Risk of Insecure Software/Firmware, Risk of Weak Device Management, Device Integration Risk, Risk of Insecure Default Settings, Technology Risk. Output: System and Software Risks
13) Security Monitoring and Logging Risks. Inputs: Lack of Security Monitoring, Lack of Logging, Monitoring Security Events and Measuring Security Metrics, Testing Risk, Verification Risk, Likelihood Risk. Output: Security Monitoring and Logging Risks
14) Malware and Virus Risks. Inputs: Malware Risk, Viruses Risk. Output: Malware and Virus Risks
15) Human Risks. Inputs: Phishing Risk, Social Engineering Risk, Risk of Misuse, Risk of Fraud, Risk of Human Errors Leading to Security Breaches, Risk of Insider Threats, Risk of Error, Risk Appearing When Writing Code. Output: Human Risks
16) External Risks. Inputs: Environmental Risk, Climate Risk. Output: External Risks

The defuzzification outcomes for each fuzzy machine are visually represented in Figure 2, highlighted clearly in blue.

As an illustrative case, Astana International University employed the LMS Platonus v6.0[1] (build# 401) during the period 2006–2024. This example showcases the practical application of fuzzy logic in assessing IS risks within an educational institution's context.

4. Experiments and Discussions

The National Institute of Standards and Technology (NIST) Special Publication 800-30 provides guidance on risk assessment for information systems. The classic standard risk formula used in NIST 800-30 is based on the following formula [28]:

$$R = T \times V \times I \tag{1}$$

Threats (T) manifest in various forms, each potentially compromising the confidentiality, integrity, and availability of information systems.

Vulnerabilities (V) are weaknesses within a system, which may arise in software, hardware, personnel, or procedural elements.

Impact (I) refers to the consequences of IS incidents, which can affect different facets of an organization and even impact individuals.

The product of the three components (threats, vulnerabilities, impact) provides an idea of the overall IS risk. The risk assessment process involves assigning values or scores to each component. These scores are then multiplied to obtain a quantitative measure of risk. This quantitative assessment helps organizations effectively prioritize and manage risks. At the same time, resources will be allocated to mitigate the most significant threats.

It is necessary to normalize the computed formulas:

$$R_{norm} = (T–T_{min}) / T_{max}–T_{min}) * (V–V_{min}) / (V_{max}–V_{min}) * (I–I_{min}) / (I_{max}–I_{min}) \tag{2}$$

ISO standards typically provide guidance on the overall risk management process rather than prescribing specific formulas. A simplified representation of the IS risk formula aligned with common risk assessment principles looks like this:

$$R = (V \times T \times A) - C \tag{3}$$

Vulnerability (V). The weakness or flaw in the system that could be exploited by a threat.

Threat (T). The potential source of harm or danger to a system.

Asset (A). The value assigned to the information or system being protected.

Controls (C). The effectiveness of existing controls or countermeasures in place to mitigate the risk.

It is necessary to normalize the calculated formulas to establish correlations between different methods:

$$R_{norm} = ((V - V_{min}) / (V_{max} - V_{min}) * (T - T_{min}) / T_{max} - T_{min}) * (A - A_{min}) / (A_{max} - A_{min})) - (C - C_{min}) / (C_{max} - C_{min})) \tag{4}$$

BS 7799 served as a foundational standard that preceded ISO/IEC 27001. Originally, BS 7799 was subsequently split into two distinct parts: BS 7799-1, which focused on the code of practice for IS management, and BS 7799-2, which detailed the specification for an Information Security Management System. These divisions allowed for a more structured approach to addressing the various aspects of IS management, encapsulating both the strategic framework and the operational specifics needed to secure information assets effectively. This bifurcation not only streamlined the implementation of security measures but also provided a clear pathway for organizations seeking to adopt robust IS practices aligned with international standards:

$$Risk = Asset * Level(threat) * Level(vulnerability) \tag{5}$$

Asset. The value assigned to the information or system being protected.

Level of threat. Typically represents the likelihood or probability of a threat event occurring.

Level of vulnerability. Typically represents the likelihood or probability that a vulnerability will be exploited by a threat.

The overall risk within the IS framework is calculated by multiplying the asset value by the corresponding threat and vulnerability levels. This calculation offers a simple method for quantifying the potential risk for IS. In this way, the impact of various variables on the security status of the organization is assessed. It is necessary to

[1] https://platonus.aiu.kz/index

normalize the calculated formulas to establish correlations between different methods:

$$\begin{aligned} Risk_{norm} = {} & (Asset - Asset_{min}) / (Asset_{max} - Asset_{min}) \\ & * \left(Level\,(threat) - Level\,(threat)_{min}\right) / \\ & \left(Level\,(threat)_{max} - Level\,(threat)_{min}\right) \\ & * \left(Level\,(vulnerability) - Level\,(vulnerability)_{min}\right) / \\ & \left(Level\,(vulnerability)_{max} - Level\,(vulnerability)_{min}\right) \end{aligned} \quad (6)$$

We performed an empirical investigation aimed at assessing the IS risk associated with the LMS utilized by selected universities. Furthermore, a comprehensive evaluation of these six software applications was conducted by an expert specializing in LMS quality evaluation. The outcomes of this evaluation are succinctly presented in Table 1. The enumerated LMS applications under scrutiny are as follows:

1) Learning Management System Platonus v6.0 (build# 414)[2].
2) Learning Management System SmartENU[3].
3) Document flow Directum[4].
4) Online course platform MOOCENU[5].
5) Automated KPI Information System[6].
6) University web site[7].

In accordance with established standards, such as NIST 800-30, ISO/IEC 27001, BS 7799, and a proposed model, the evaluation was executed by individuals without specialized expertise in LMS IS. These inspectors systematically scrutinized the attributes and sub-attributes inherent in the methodologies governing IS risk evaluation. Notably, the inspectors adhered rigorously to the prescribed rules delineated within each respective methodology during the assessment process.

The 5th column in Table 1 of the results was populated by a specialist in cryptography and software architecture, who is also certified in relevant fields. When evaluating the quality of the six programs, the expert relied on their experience rather than a specific method. The specialist, however, didn't utilize the outlined methods. Furthermore, having extensive experience working with these software applications, he possesses the knowledge to select the most suitable one. Consequently, the evaluation by the expert is more objective as it is based on their personal familiarity with the six programs and their proficiency in creating secure software. Moving forward, we will undertake a correlation analysis. This analysis will provide us with an insight into the efficacy of our approach. The analysis results are displayed in Table 2.

Table 2 presents a matrix of paired correlation coefficients depicting the relationships between different standards and an expert-assessed proposed model for IS risk assessment. The coefficients quantify the degree of correlation between pairs of variables, ranging from 0 (indicating no correlation) to 1 (indicating a perfect positive correlation). The diagonal elements of the matrix represent the correlation of each standard or model with itself, resulting in a perfect correlation (correlation coefficient = 1), as expected. Notably, high correlation coefficients are observed between NIST 800-30, ISO/IEC 27001, BS 7799, and the proposed model, indicating strong positive associations in their assessments. Specifically, the correlation between NIST 800-30 and ISO/IEC 27001 is 0.985739, between NIST 800-30 and BS 7799 is 0.986092, and between ISO/IEC 27001 and BS 7799 is 0.999175. These values suggest a high level of consistency and similarity in the IS risk assessments derived from these standards. Moreover, the correlation coefficients involving the "Expert" and each standard or model are also notably high, ranging from 0.985053 to 0.998418. This indicates a strong alignment between the expert-assessed evaluations and those derived from established standards, as well as the proposed model.

The proposed model demonstrated the most robust positive correlation with established standards, including NIST 800-30, ISO/IEC 27001, BS 7799, and expert assessments. In contrast, the alternative assessment methodologies exhibited a single high correlation, exceeding 0.99, only when the proposed model was excluded from the dataset. This suggests that the proposed model not only aligns closely with these standards but also significantly influences the correlation dynamics within the dataset.

A statistical hypothesis test was conducted to analyze the data presented in Table 3. The objective of this test is to facilitate a robust inference regarding a specific attribute of the overall population based on the provided sample data. In this context, a robust inference is defined as a conclusion supported by a probability approaching unity, which confers a high degree of confidence in the inference made. For the purpose of this analysis, consider the null hypothesis that posits the equality between the population mean and the value associated with the proposed model.

The following parameters are defined for the analysis:

μ – Represents the general average, equated to the value associated with the proposed model.

n – Denotes the number of techniques, excluding the proposed model, equaling 4, namely, NIST 800-30, ISO/IEC 27001, BS 7799, and Expert.

X_{avg} – Signifies the arithmetic mean.

s – Represents the root mean square deviation.

t_{fact} – Refers to the t-criterion.

[2] https://edu.enu.kz/

[3] https://smart.enu.kz/

[4] https://directum.enu.kz/

[5] https://mooc.enu.kz/

[6] https://kpi.enu.kz/

[7] www.enu.kz

Table 1
Results of evaluating six software applications

Software	NIST 800-30	ISO/IEC 27001	BS 7799	Expert	Proposed model
Platonus	0.546	0.749	0.738	0.536	0.646
Smart ENU	0.843	0.985	0.951	0.885	0.928
Directum	0.914	0.998	0.992	0.910	0.954
MOOC ENU	0.407	0.484	0.482	0.394	0.441
KPI	0.225	0.315	0.295	0.205	0.219
Web site	0.371	0.453	0.431	0.353	0.401

Table 2
Results of evaluating six software applications

Standards	NIST 800-30	ISO/IEC 27001	BS 7799	Expert	Proposed model
NIST 800-30	1	0.985	0.986	0.998	0.994
ISO/IEC 27001	0.985	1	0.999	0.986	0.996
BS 7799	0.986	0.999	1	0.985	0.996
Expert	0.998	0.986	0.985	1	0.994
Proposed model	0.994	0.996	0.996	0.994	1

Table 3
Statistical analysis for comparing the means in software evaluations

Parameters	Platonus	Smart ENU	Directum	Mooc ENU	KPI	Web site
μ	0.64	0.92	0.95	0.44	0.21	0.4
X_{avg}	0.64	0.91	0.95	0.44	0.26	0.4
n	4	4	4	4	4	4
s	0.09	0.04	0.03	0.03	0.04	0.03
t_{fact}	–0.08	–0.48	–0.02	0.04	1.84	0.05
α	0.5	0.5	0.5	0.5	0.5	0.5
d.f.	3	3	3	3	3	3
t_{crit}	3.18	3.18	3.18	3.18	3.18	3.18
p-value	0.93	0.66	0.98	0.97	0.16	0.96

α – Denotes the significance level, set at 0.05, representing a 5% probability of error.

d.f. – Represents the quantity of freedom degrees, equating to 3.

t_{crit} – Signifies the critical value of the *t*-criterion, derived from the two-way inverse Student's *t*-distribution.

p-value – Serves as a metric quantifying the likelihood that the observed discrepancy is solely due to random variability, determined from the bilateral Student's *t*-distribution.

Table 3 presents the results of a statistical hypothesis test comparing the means of software evaluations. The *t*-criterion (t_{fact}) ranges from −0.08269 to 1.847972, indicating varying degrees of deviation from the proposed model's mean. Notably, for each software, the *p*-values exceed the significance level α of 0.05, suggesting that observed differences in means are likely due to random chance, and thus, we fail to reject the null hypothesis. These findings imply that, within the sample data, the general mean of the evaluated software does not significantly differ from the value associated with the proposed model.

The proposed fuzzy expert system offers a significant advantage over traditional statistical methods. The advantage is achieved due to the ability to manage uncertainties and dynamic changes in cybersecurity. Using fuzzy logic, the system skillfully imitates human decision-making processes, effectively integrating both qualitative and quantitative data. Traditional models often fail in such conditions. They are either too slow to adapt or do not capture subtle gradations of threat levels. In contrast, the fuzzy expert system is able to adapt to rapid changes and subtle differences in security threats. This improves the effectiveness and efficiency of IS risk management strategies.

5. Conclusion

This study makes a significant contribution to the existing body of knowledge in IS risk assessment. Traditional models often fail in dynamic and ambiguous environments. The proposed fuzzy model excels in capturing the nuances and complexities of cyber threats. This study expands the scope of fuzzy logic applications. The results demonstrate the effectiveness of integrating qualitative and quantitative data for comprehensive risk analysis. The proposed model addresses a critical gap in methodologies for handling the fluid nature of IS risks by combining fuzzy logic with MCDM.

The fuzzy model is distinguished by its ability to manage uncertainty and ambiguity in IS risk assessment. IS risks are often unpredictable and evolve rapidly. The use of linguistic variables and fuzzy rule sets allows it to more accurately approximate human reasoning. Fuzzy functions are essential for effective risk assessment. Fuzzy logic offers a more adaptive and nuanced approach that traditional models do not provide.

Looking ahead, our future research will focus on further refining the fuzzy model. This will be aimed at expanding its application to various industries outside of education, including healthcare and finance. In these industries, data sensitivity and security are critical. We also plan to extend the model's capabilities using advanced AI techniques to automate the interpretation of fuzzy logic outputs. Also, integrating real-time data streams into the fuzzy evaluation framework will be a focus of our future research.

Funding Support

This research was funded by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (grant no. AP19174390).

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data available on request from the corresponding author upon reasonable request.

Author Contribution Statement

Alibek Barlybayev: Conceptualization, Methodology, Validation, Formal analysis, Investigation, Resources, Data curation, Writing – original draft, Writing – review & editing, Supervision, Project administration, Funding acquisition. **Alua Turginbayeva:** Methodology, Software, Validation, Resources, Data curation, Visualization.

References

[1] Chai, J., Liu, J. N. K., & Ngai, E. W. T. (2013). Application of decision-making techniques in supplier selection: A systematic review of literature. *Expert Systems with Applications*, *40*(10), 3872–3885. https://doi.org/10.1016/j.eswa.2012.12.040

[2] Paelinck, J. H. P. (1978). Qualiflex: A flexible multiple-criteria method. *Economics Letters*, *1*(3), 193–197. https://doi.org/10.1016/0165-1765(78)90023-X

[3] Edwards, W., & Barron, F. H. (1994). SMARTS and SMARTER: Improved simple methods for multiattribute utility measurement. *Organizational Behavior and Human Decision Processes*, *60*(3), 306–325. https://doi.org/10.1006/obhd.1994.1087

[4] Abdullah, L., & Adawiyah, C. R. (2014). Simple additive weighting methods of multi criteria decision making and applications: A decade review. *International Journal of Information Processing and Management*, *5*(1), 39–49.

[5] Abdymanapov, S. A., Muratbekov, M., Altynbek, S., & Barlybayev, A. (2021). Fuzzy expert system of information security risk assessment on the example of analysis learning management systems. *IEEE Access*, *9*, 156556–156565. https://doi.org/10.1109/ACCESS.2021.3129488

[6] Kerimkhulle, S., Dildebayeva, Z., Tokhmetov, A., Amirova, A., Tussupov, J., Makhazhanova, U., ...,& Salykbayeva, A. (2023). Fuzzy logic and its application in the assessment of information security risk of Industrial Internet of Things. *Symmetry*, *15*(10), 1958. https://doi.org/10.3390/sym15101958

[7] Alonge, C. Y., Arogundade, O. T., Adesemowo, K., Ibrahalu, F. T., Adeniran, O. J., & Mustapha, A. M. (2020). Information asset classification and labelling model using fuzzy approach for effective security risk assessment. In *2020 International Conference in Mathematics, Computer Engineering and Computer Science*, 1–7. https://doi.org/10.1109/ICMCECS47690.2020.240911

[8] Ershadi, M. J., & Forouzandeh, M. (2019). Information security risk management of research information systems: A hybrid approach of fuzzy FMEA, AHP, TOPSIS and Shannon entropy. *Journal of Digital Information Management*, *17*(6), 321–336. https://doi.org/10.6025/jdim/2019/17/6/321-336

[9] Peisheng, L., Yunping, H., Xiaole, Z., Shunshun, W., & Zhenglin, L. (2020). Research on information system risk assessment based on improved AHP-fuzzy theory. *Journal of Physics: Conference Series*, *1693*(1), 012046. https://doi.org/10.1088/1742-6596/1693/1/012046

[10] Kumar, R., Pandey, A. K., Baz, A., Alhakami, H., Alhakami, W., Agrawal, A., & Khan, R. A. (2020). Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security. *Symmetry*, *12*(4), 664. http://doi.org/10.3390/sym12040664

[11] Yang, L., Cao, X., & Geng, X. (2019). A novel intelligent assessment method for SCADA information security risk based on causality analysis. *Cluster Computing*, *22*(3), 5491–5503. https://doi.org/10.1007/s10586-017-1315-4

[12] Erdoğan, M., Karaşan, A., Kaya, İ., Budak, A., & Çolak, M. (2020). A fuzzy based MCDM methodology for risk evaluation of cyber security technologies. In *Intelligent and Fuzzy Techniques in Big Data Analytics and Decision Making: Proceedings of the INFUS 2019 Conference*, 1042–1049. https://doi.org/10.1007/978-3-030-23756-1_123

[13] Kotenko, I., & Parashchuk, I. (2021). Evaluation of information security of industrial automation systems using fuzzy algorithms and predicates. In *2021 International Russian Automation Conference*, 261–266. https://doi.org/10.1109/RusAutoCon52004.2021.9537332

[14] Hart, S., Ferrara, A. L., & Paci, F. (2020). Fuzzy-based approach to assess and prioritize privacy risks. *Soft Computing*, *24*(3), 1553–1563. https://doi.org/10.1007/s00500-019-03986-5

[15] Alfakeeh, A. S., Almalawi, A., Alsolami, F. J., Abushark, Y. B., Khan, A. I., Bahaddad, A. A. S., ...,& Khan, R. A. (2022). Hesitant fuzzy-sets based decision-making model for security risk assessment. *Computers, Materials & Continua*, *70*(2), 2297–2317. http://doi.org/10.32604/cmc.2022.020146

[16] Kumar, R., Baz, A., Alhakami, H., Alhakami, W., Agrawal, A., & Khan, R. A. (2021). A hybrid fuzzy rule-based multi-criteria framework for sustainable-security assessment of web application. *Ain Shams Engineering Journal*, *12*(2), 2227–2240. https://doi.org/10.1016/j.asej.2021.01.003

[17] Buldakova, T. I., & Mikov, D. A. (2019). Matlab application for information security risk analysis. *AIP Conference Proceedings: International Scientific and Practical Conference "Modeling in Education 2019"*, *2195*(1), 020004. https://doi.org/10.1063/1.5140104

[18] Vaczi, D., Toth-Laufer, E., & Szadeczky, T. (2020). Fuzzy-based cybersecurity risk analysis of the human factor from the perspective of classified information leakage. In *2020 IEEE 18th International Symposium on Intelligent Systems and Informatics*, 000113–000118. https://doi.org/10.1109/SISY50555.2020.9217053

[19] Komazec, N., Janković, K., Mladenović, M., Mijatović, M., & Lapčević, Z. (2024). Ranking of risk using the application of the AHP method in the risk assessment process on the Piraeus-Belgrade-Budapest railway corridor. *Journal of Decision Analytics and Intelligent Computing*, *4*(1), 176–186. https://doi.org/10.31181/jdaic10002122024k

[20] Kushwaha, D. K., Panchal, D., & Sachdeva, A. (2023). A modified FMEA approach based integrated decision framework for overcoming the problems of sudden failure and accidental hazards in turbine and alternator unit. *Facta Universitatis, Series: Mechanical Engineering*, Advance online publication. https://doi.org/10.22190/FUME221126010K

[21] Švadlenka, L., Bajec, P., Pivtorak, H., Bošković, S., Jovčić, S., & Dobrodolac, M. (2024). Risk prioritization from the crowdshipping provider's perspective using the CIMAS method. *Spectrum of Engineering and Management Sciences*, *2*(1), 234–246.

[22] Barlybayev, A., Sharipbay, A., Shakhmetova, G., & Zhumadillayeva, A. (2024). Development of a flexible information security risk model using machine learning methods and

ontologies. *Applied Sciences*, *14*(21), 9858. https://doi.org/10.3390/app14219858

[23] Tariq, M. I., Ahmed, S., Memon, N. A., Tayyaba, S., Ashraf, M. W., Nazir, M., ...,& Balas, M. M. (2020). Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks. *Sensors*, *20*(5), 1310. https://doi.org/10.3390/s20051310

[24] Markovic-Petrovic, J. D., Stojanovic, M. D., & Rakas, S. V. B. (2019). A fuzzy AHP approach for security risk assessment in SCADA networks. *Advances in Electrical and Computer Engineering*, *19*(3), 69–74. https://doi.org/10.4316/AECE.2019.03008

[25] Tariq, M. I. (2019). Agent based information security framework for hybrid cloud computing. *KSII Transactions on Internet and Information Systems*, *13*(1), 406–434. http://doi.org/10.3837/tiis.2019.01.023

[26] Kececioglu, O. F., Gani, A., & Sekkeli, M. (2020). Design and hardware implementation based on hybrid structure for MPPT of PV system using an interval type-2 TSK fuzzy logic controller. *Energies*, *13*(7), 1842. https://doi.org/10.3390/en13071842

[27] Acikgoz, H., Kececioglu, O. F., Gani, A., Tekin, M., & Sekkeli, M. (2017). Robust control of shunt active power filter using interval type-2 fuzzy logic controller for power quality improvement. *Tehnicki Vjesnik-Technical Gazette*, *24*, 363–368. https://doi.org/10.17559/TV-20161213004749

[28] Khambhammettu, H., Boulares, S., Adi, K., & Logrippo, L. (2013). A framework for risk assessment in access control systems. *Computers & Security*, *39*, 86–103. https://doi.org/10.1016/j.cose.2013.03.010

How to Cite: Barlybayev, A., & Turginbayeva, A. (2025). Development and Implementation of an Advanced Fuzzy Expert System for the Assessment of Information Security Risks. *Journal of Computational and Cognitive Engineering*. https://doi.org/10.47852/bonviewJCCE52024683