Jurnal Teknik Informatika C.I.T Medicom, 18 (2) (2026) 64-78

Published by: Institute of Computer Science (IOCS)

Jurnal Teknik Informatika C.I.T Medicom

Journal homepage: www.medikom.iocspublisher.org

Decision Support System for Determining Cyber Risk Mitigation Priorities in Higher Education Using the Fuzzy TOPSIS Method

Fristi Riandari[1], Hengki Tamando Sihotang[2]
[1] Politeknik Negeri Medan, Medan, Indonesia
[2] Sains Data, Universitas Pembangunan Nasional Veteran Jakarta

Article Info

Article history

Received : March 24, 2026
Revised : April 20, 2026
Accepted : May 13, 2026

Key Words:

Decision Support System;
Cyber Risk Management;
Fuzzy TOPSIS;
Higher Education;
Cybersecurity.

Abstract

The increasing frequency and sophistication of cyber threats have made higher education institutions attractive targets for cyberattacks, posing significant risks to information assets, academic operations, and institutional reputation. Universities rely heavily on digital technologies, including academic information systems, e-learning platforms, cloud services, and research databases, making effective cybersecurity risk management essential. However, limited cybersecurity resources often prevent institutions from addressing all potential threats simultaneously, highlighting the need for a systematic approach to prioritizing cyber risk mitigation efforts. This study aims to develop a Decision Support System (DSS) for determining cyber risk mitigation priorities in higher education institutions using the Fuzzy Technique for Order Preference by Similarity to Ideal Solution (Fuzzy TOPSIS) method. Six evaluation criteria were considered, namely probability of occurrence, financial impact, operational impact, reputation damage, data sensitivity, and recovery complexity. Expert assessments were expressed using linguistic variables and converted into Triangular Fuzzy Numbers (TFNs) to accommodate uncertainty in the decision-making process. The Fuzzy TOPSIS method was then applied to evaluate and rank cyber risks according to their mitigation priorities. The results demonstrated that the proposed DSS successfully generated a prioritized ranking of cyber risks, with ransomware and data breach risks receiving the highest mitigation priorities due to their substantial impacts on university operations, financial resources, and information security. The findings suggest that the developed DSS effectively supports cybersecurity decision-making by handling uncertainty in expert assessments and providing systematic recommendations for cyber risk mitigation. Consequently, the proposed framework can assist higher education institutions in allocating cybersecurity resources more efficiently and enhancing their overall cybersecurity resilience.

Keywords: Artificial Intelligence; Multilevel Optimization; Complex.

Corresponding Author:

Fristi Riandari
Politeknik Negeri Medan, Medan, Indonesia
Jl. Almamater No.1, Padang Bulan, Kec. Medan Baru, Kota Medan, Sumatera Utara 20155
Email: fristiriandari@polmed.ac.id

1. Introduction

The rapid advancement of information and communication technology has significantly transformed the higher education sector(Sarkar, 2012). Universities increasingly rely on digital technologies to support academic, administrative, and research activities through various platforms such as academic information systems, e-learning environments, cloud computing services, research databases, and student information management systems. This digital transformation has improved operational efficiency, enhanced educational accessibility, and facilitated data-driven decision-making. However, the growing dependence on interconnected digital infrastructures has also increased the exposure of higher education institutions to various cybersecurity threats.

In recent years, cyberattacks targeting universities have become more frequent and sophisticated. Higher education institutions possess valuable assets, including personal student records, research data, intellectual property, financial information, and institutional credentials, making them attractive targets for cybercriminals. Common cybersecurity threats faced by universities include phishing attacks, ransomware, malware infections, insider threats, data breaches, and distributed denial-of-service (DDoS) attacks(Ulven & Wangen, 2021). These incidents can result in significant financial losses, operational disruptions, reputational damage, and violations of data privacy regulations. Furthermore, cyber incidents may compromise the fundamental principles of information security, namely confidentiality, integrity, and availability, which are essential for maintaining trust and continuity in educational operations.

Despite the increasing awareness of cybersecurity risks, many higher education institutions face challenges in implementing comprehensive cybersecurity measures due to budget constraints, limited technical expertise, and competing organizational priorities. As a result, universities often struggle to determine which cybersecurity risks should be addressed first and how available resources should be allocated effectively. Since not all cyber risks can be mitigated simultaneously, decision-makers require a systematic approach for prioritizing risk mitigation efforts based on the severity and potential impact of identified threats(Goel et al., 2020).

Traditional cyber risk assessment approaches frequently rely on quantitative scoring methods that use precise numerical values to evaluate risk factors. However, cybersecurity assessments often involve subjective judgments and uncertainty, particularly when experts estimate the likelihood and impact of cyber threats. Conventional methods may not adequately capture the ambiguity inherent in human evaluations, potentially leading to less accurate prioritization outcomes. Therefore, advanced decision-making approaches that can handle uncertainty and linguistic assessments are needed to improve cyber risk management processes.

Cybersecurity risk assessment has become an increasingly important research area due to the growing dependence of organizations on digital infrastructures and information systems(Goel et al., 2020). Various studies have proposed decision support and multi-criteria decision-making (MCDM) approaches to identify, evaluate, and prioritize cybersecurity risks. One of the earliest studies relevant to fuzzy-based risk assessment was conducted by Ak and Gul (2019), who proposed an integration of the Analytical Hierarchy Process (AHP) and TOPSIS extended with Pythagorean Fuzzy Sets for information security risk analysis. Their research demonstrated that combining fuzzy logic with MCDM techniques can improve the reliability of security risk evaluations by incorporating uncertainty into the decision-making process. The study highlighted the effectiveness of fuzzy approaches in handling subjective expert assessments when evaluating information security risks.

In a broader risk assessment context, Tian and Li (2020) applied the Fuzzy TOPSIS method to evaluate safety management risks. Their study showed that Fuzzy TOPSIS provides a systematic mechanism for ranking risk factors and identifying critical issues requiring immediate attention. Although the research was not specifically focused on cybersecurity, it established the methodological foundation for applying Fuzzy TOPSIS to complex risk assessment problems characterized by uncertainty and multiple evaluation criteria.

Buzdugan (2020) conducted a systematic review of decision support systems used in cyber risk management for critical infrastructures. The review found that decision support systems play a crucial role in cyber risk identification, assessment, and mitigation planning. However, the study also

emphasized that many existing DSS solutions lack robust mechanisms for handling uncertainty and often rely on deterministic risk evaluation models. The author suggested that future research should integrate intelligent and fuzzy-based approaches to enhance cyber risk decision-making processes.

In the context of emerging communication technologies, Kholidy (2021) proposed a triangular fuzzy multicriteria decision-making approach for assessing security risks in 5G networks. The study integrated Triangular Fuzzy Numbers (TFNs) with MCDM techniques to improve the identification of attack paths and vulnerability propagation in complex network environments. The results demonstrated that fuzzy-based models provide more realistic assessments of cybersecurity threats than traditional crisp-value approaches.

A significant contribution to IT risk prioritization was presented by Alshahrani, Alotaibi, Ansari, Asiri, Agrawal, Khan, Mohsen, and Hilal (2022). Their study employed Fuzzy TOPSIS to analyze and rank IT risk factors affecting organizational information systems. The results showed that Fuzzy TOPSIS successfully prioritized risks by considering multiple dimensions of information technology security. The authors concluded that fuzzy-based MCDM techniques are effective tools for supporting IT risk management decisions in environments characterized by uncertainty and incomplete information.

In the same year, Alfakeeh et al. (2022) introduced a hesitant fuzzy-set-based decision-making model for security risk assessment. Their research addressed the challenge of inconsistent expert opinions by incorporating hesitant fuzzy sets into the decision-making process. The proposed model improved the flexibility and accuracy of security risk evaluations, particularly in situations where experts expressed varying degrees of confidence regarding risk severity and likelihood.

The application of TOPSIS in cybersecurity was further expanded by Putra, Octavian, Susilo, and Prabowo (2023), who developed a hybrid AHP-TOPSIS model for maritime cybersecurity risk analysis. Their research identified critical cybersecurity dimensions affecting maritime systems and demonstrated the usefulness of MCDM techniques for prioritizing cyber threats in complex operational environments. The study reinforced the value of TOPSIS-based approaches in cybersecurity risk management and strategic decision-making.

Several studies have explored decision support systems (DSS) and multi-criteria decision-making (MCDM) techniques for cybersecurity risk assessment. However, many existing approaches still utilize crisp values and deterministic calculations that may not fully represent expert opinions under uncertain conditions. In addition, the application of fuzzy-based decision-making techniques in the context of higher education cybersecurity remains relatively limited. Specifically, there is a lack of research integrating Fuzzy Technique for Order Preference by Similarity to Ideal Solution (Fuzzy TOPSIS) into decision support systems for prioritizing cyber risk mitigation strategies within university environments(Kumar et al., 2020).

To address these limitations, this study proposes a Decision Support System (DSS) based on the Fuzzy TOPSIS method for determining cyber risk mitigation priorities in higher education institutions. The Fuzzy TOPSIS approach combines fuzzy logic with multi-criteria decision-making techniques to effectively manage uncertainty in expert evaluations while providing a systematic ranking of cyber risks. By considering multiple risk assessment criteria, such as probability of occurrence, financial impact, operational impact, reputation damage, data sensitivity, and recovery complexity, the proposed system aims to generate more reliable and realistic mitigation priorities.

The objectives of this research are fourfold. First, the study seeks to identify and analyze the major cyber risks affecting higher education institutions. Second, it aims to develop a decision support system framework utilizing the Fuzzy TOPSIS method for cyber risk evaluation. Third, the research intends to rank identified cyber risks according to their mitigation priority levels. Finally, the study aims to support cybersecurity decision-making by providing actionable recommendations for resource allocation and risk management planning.

This research contributes to the existing body of knowledge in several ways. Theoretically, it expands the application of fuzzy multi-criteria decision-making methods within the domain of cybersecurity risk management in higher education. Methodologically, it integrates fuzzy logic and

TOPSIS into a comprehensive decision support framework capable of handling uncertainty in expert assessments. Practically, the proposed system provides university administrators and information technology managers with a structured tool for prioritizing cybersecurity investments and mitigation strategies, thereby enhancing the overall resilience and security posture of higher education institutions.

2. Research Methodolgy

This study employs a quantitative research approach to develop a Decision Support System (DSS) for determining cyber risk mitigation priorities in higher education institutions using the Fuzzy Technique for Order Preference by Similarity to Ideal Solution (Fuzzy TOPSIS) method. The proposed methodology aims to support decision-makers in evaluating multiple cyber risks and identifying mitigation priorities under conditions of uncertainty(Amin, 2019). The research integrates cyber risk assessment principles with Multi-Criteria Decision Making (MCDM) techniques to produce a systematic and objective prioritization framework.

The overall research framework consists of several sequential stages. The process begins with cyber risk identification, followed by the selection of evaluation criteria relevant to cybersecurity risk assessment. Subsequently, expert assessments are collected and transformed into fuzzy linguistic values through a fuzzification process. The Fuzzy TOPSIS method is then applied to calculate risk priorities and generate risk rankings. Finally, mitigation recommendations are provided based on the resulting rankings. This framework ensures that cyber risks are evaluated comprehensively while accounting for uncertainty in expert judgments.

The research design combines quantitative analysis, decision support system development, and multi-criteria decision-making methodologies(Barfod et al., 2011). The quantitative approach is used to analyze expert evaluations and calculate risk priority scores, while the DSS development component focuses on designing a system capable of supporting cybersecurity decision-making processes. The MCDM approach is employed because cyber risk prioritization involves multiple evaluation criteria that must be considered simultaneously when determining mitigation priorities.

Data for this study are collected from both primary and secondary sources. Primary data are obtained through interviews, questionnaires, and Focus Group Discussions (FGDs) involving information technology managers, cybersecurity experts, and university administrators(Nguyen, 2019). These participants are selected because they possess relevant knowledge and experience regarding cybersecurity management within higher education institutions. Interviews are conducted to identify common cyber threats and evaluate cybersecurity challenges faced by universities. Questionnaires are used to collect structured expert assessments regarding the likelihood and impact of identified cyber risks. In addition, Focus Group Discussions facilitate consensus building among experts and provide deeper insights into cybersecurity priorities and mitigation strategies.

Secondary data are collected from various authoritative sources, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, ISO 27005 Information Security Risk Management guidelines, cybersecurity incident reports, academic publications, and previous studies related to cybersecurity risk assessment and decision support systems. These sources provide theoretical foundations and practical references for identifying cyber risks and establishing evaluation criteria.

Based on the literature review and expert consultations, several cyber risk alternatives are identified as common threats within higher education environments. These alternatives include phishing attacks (R1), malware infections (R2), data breaches (R3), ransomware attacks (R4), insider threats (R5), and distributed denial-of-service (DDoS) attacks (R6). These risks represent significant cybersecurity concerns because they may affect the confidentiality, integrity, and availability of institutional information assets.

To evaluate the identified cyber risks, six assessment criteria are employed(Baig & Zeadally, 2019). The first criterion is the probability of occurrence (C1), which measures the likelihood of a cyber threat occurring within the institution. The second criterion is financial impact (C2), which assesses the

potential economic losses resulting from a cyber incident. The third criterion is operational impact (C3), reflecting the extent to which institutional activities may be disrupted. The fourth criterion is reputation damage (C4), which evaluates the potential negative effects on institutional credibility and stakeholder trust. The fifth criterion is data sensitivity (C5), which measures the importance and confidentiality of affected information assets. The sixth criterion is recovery complexity (C6), representing the effort, time, and resources required to restore systems after a cyber incident.

The Fuzzy TOPSIS method is employed to prioritize cyber risks while accommodating uncertainty in expert evaluations. In the first step, linguistic variables are established to represent expert judgments. Five linguistic terms are used, namely Very Low, Low, Medium, High, and Very High. These linguistic assessments are converted into Triangular Fuzzy Numbers (TFNs) to facilitate mathematical processing. For example, Very Low is represented by (1,1,3), Low by (1,3,5), Medium by (3,5,7), High by (5,7,9), and Very High by (7,9,9).

In the second step, a fuzzy decision matrix is constructed based on expert evaluations of each cyber risk alternative against all assessment criteria(Erdoğan et al., 2019). The resulting matrix represents the performance of each risk according to the selected criteria using fuzzy numerical values. Since the criteria may have different measurement scales, the third step involves normalizing the fuzzy decision matrix to ensure comparability among criteria.

The fourth step consists of calculating the weighted normalized fuzzy decision matrix(Hidayat et al., 2019). At this stage, criterion weights determined through expert assessments are multiplied by the normalized fuzzy values. This process reflects the relative importance of each criterion in the risk prioritization process.

The fifth step involves determining the Fuzzy Positive Ideal Solution (FPIS) and Fuzzy Negative Ideal Solution (FNIS)(Safari et al., 2012). The FPIS represents the optimal risk assessment condition, while the FNIS represents the least desirable condition. These ideal solutions serve as reference points for evaluating the relative positions of cyber risk alternatives.

In the sixth step, the distances between each alternative and both the FPIS and FNIS are calculated using fuzzy distance measures. These distances indicate how close each cyber risk is to the ideal and non-ideal solutions. The seventh step calculates the Closeness Coefficient (CC) for each alternative using the following equation:

$$CC_i = \frac{D_i^-}{D_i^- + D_i^+}$$

where D_i^- denotes the distance from the negative ideal solution and D_i^+ denotes the distance from the positive ideal solution. The Closeness Coefficient reflects the relative priority of each cyber risk. A higher CC value indicates a higher mitigation priority because the alternative is closer to the ideal solution.

In the final step, cyber risks are ranked according to their Closeness Coefficient values(Umunnakwe et al., 2021). The risk with the highest CC value is considered the highest priority for mitigation. This ranking provides decision-makers with a structured basis for allocating cybersecurity resources and implementing appropriate risk mitigation strategies.

To facilitate practical implementation, a Decision Support System prototype is developed(Zhang et al., 2015). The system consists of three primary components: input, processing, and output modules. The input module allows users to enter cyber risk alternatives, evaluation criteria, criterion weights, and expert assessments. The processing module performs all Fuzzy TOPSIS calculations automatically, including fuzzification, normalization, weighted matrix computation, ideal solution determination, distance calculation, and ranking generation. The output module presents the results in the form of cyber risk rankings, mitigation priority recommendations, and interactive dashboard visualizations. These visualizations assist university administrators and cybersecurity managers in understanding risk priorities and making informed decisions regarding cybersecurity investments and mitigation planning.

3. Results and Discussion

3.1 Cyber Risk Identification Results

The results of the identification process revealed six major cyber risks that pose significant threats to the information systems and digital infrastructure of higher education institutions. These risks include phishing attacks, malware infections, data breaches, ransomware attacks, insider threats, and distributed denial-of-service (DDoS) attacks. These threats were selected because they frequently occur in educational environments and have the potential to cause substantial operational, financial, and reputational consequences.

Phishing attacks were identified as one of the most common cybersecurity threats in higher education institutions(Alexei, 2021). This type of attack involves the use of fraudulent emails, messages, or websites designed to deceive users into revealing sensitive information such as usernames, passwords, and financial credentials. Due to the large number of students, faculty members, and administrative staff accessing university systems daily, phishing attacks represent a significant risk that can lead to unauthorized access and subsequent security incidents.

Malware infections were also identified as a critical cyber risk. Malware refers to malicious software designed to disrupt system operations, steal information, or gain unauthorized access to computer systems. Universities often maintain extensive networks consisting of various devices and platforms, increasing the likelihood of malware propagation. Malware infections may compromise system performance, damage digital assets, and create opportunities for further cyberattacks.

Data breaches emerged as another high-priority risk due to the sensitive nature of information managed by higher education institutions(Chapman, 2019). Universities store large volumes of personal data, academic records, research information, and financial details. Unauthorized access to these data assets may result in privacy violations, regulatory penalties, loss of stakeholder trust, and significant reputational damage. Consequently, protecting institutional data against unauthorized disclosure remains a critical cybersecurity concern.

Ransomware attacks were identified as one of the most disruptive cyber threats affecting universities. In a ransomware attack, malicious actors encrypt institutional data and demand payment in exchange for decryption keys. Such attacks can severely disrupt academic operations, prevent access to critical systems, and cause substantial financial losses. Given the increasing frequency and sophistication of ransomware campaigns targeting educational institutions, this risk requires particular attention in cybersecurity planning and mitigation efforts.

Insider threats were also recognized as a significant source of cybersecurity risk. Unlike external attacks, insider threats originate from individuals within the organization, including employees, students, contractors, or other authorized users. These threats may result from malicious intent, negligence, or accidental actions. Insider threats are particularly challenging to detect and manage because insiders often possess legitimate access privileges to institutional systems and sensitive information.

Finally, distributed denial-of-service (DDoS) attacks were identified as a major threat to the availability y of university services (Ganin et al., 2020). DDoS attacks overwhelm network resources and servers with excessive traffic, rendering online services inaccessible to legitimate users. Such attacks can disrupt learning management systems, online examinations, academic portals, and other essential digital services that support educational activities.

The identified cyber risks serve as the alternatives evaluated in the subsequent stages of the study(Ganin et al., 2020). Their selection reflects the cybersecurity challenges commonly encountered in higher education environments and provides a comprehensive basis for risk prioritization. By systematically identifying these risks, the study establishes a foundation for applying the Fuzzy TOPSIS method to determine mitigation priorities and support strategic cybersecurity decision-making within universities.

Table 1. Identified Cyber Risks in Higher Education Institutions

Risk	Description
Phishing	Fraudulent attempts to obtain user credentials and sensitive information
Malware Infection	Introduction of malicious software that disrupts systems or steals data

Data Breach	Unauthorized access, disclosure, or theft of sensitive information
Ransomware	Encryption of institutional data followed by ransom demands
Insider Threat	Security incidents caused by authorized users intentionally or unintentionally
DDoS Attack	Network flooding attacks that disrupt service availability

The identification results indicate that cybersecurity threats affecting higher education institutions are diverse and multidimensional, encompassing risks related to confidentiality, integrity, and availability. Therefore, an effective prioritization mechanism is necessary to ensure that limited cybersecurity resources are allocated to the most critical risks. The following section presents the evaluation of these risks using predefined assessment criteria and the Fuzzy TOPSIS method to determine mitigation priorities.

3.2 Criteria Weight Results

After identifying the cyber risk alternatives, the next stage of the study involved determining the relative importance of the evaluation criteria used in the cyber risk prioritization process. The results indicate that the Probability of Occurrence (C1) received the highest weight of 0.25, making it the most influential criterion in the cyber risk prioritization process. This result suggests that experts consider the likelihood of a cyber threat occurring as a primary factor when determining mitigation priorities. Cyber risks that are more likely to occur are generally perceived as requiring immediate attention because they pose a greater probability of disrupting university operations and information systems.

The second most important criterion is Financial Impact (C2) with a weight of 0.20(Çelen, 2014). This finding reflects the growing concern among higher education institutions regarding the financial consequences of cybersecurity incidents. Cyberattacks can result in substantial costs associated with system recovery, incident response, legal compliance, data restoration, and potential financial penalties. Therefore, risks that may generate significant financial losses are considered high-priority threats requiring proactive mitigation measures.

The Operational Impact (C3) criterion received a weight of 0.18, indicating its substantial influence on the decision-making process(Kabak, 2013). Operational impact refers to the extent to which a cyber incident can disrupt teaching, learning, research, and administrative activities. Universities increasingly rely on digital platforms for academic and operational functions; consequently, interruptions caused by cyberattacks may significantly affect institutional performance and service delivery.

The fourth criterion, Reputation Damage (C4), obtained a weight of 0.15. This result demonstrates that maintaining institutional reputation is an important consideration in cybersecurity management. Data breaches and other cybersecurity incidents can negatively affect stakeholder trust, student confidence, research collaborations, and public perception. Consequently, risks that have the potential to damage the reputation of a university are assigned considerable importance in the prioritization process.

The Data Sensitivity (C5) criterion was assigned a weight of 0.12. This criterion evaluates the importance and confidentiality of information assets that may be affected by a cyber incident(Alberts & Dorofee, 2003). Universities manage various categories of sensitive data, including student records, employee information, financial documents, and research findings. Although data sensitivity is considered important, experts ranked it slightly lower than operational and financial impacts because the consequences of data exposure are often reflected through broader organizational effects such as financial losses and reputational harm.

Finally, Recovery Complexity (C6) received the lowest weight of 0.10. This criterion measures the level of effort, time, expertise, and resources required to restore systems following a cyber incident. Although recovery complexity remains an important aspect of cybersecurity management, experts considered it less critical than the probability and direct impact of cyber threats. This suggests that universities prioritize preventing high-probability and high-impact incidents before considering the challenges associated with post-incident recovery.

Table 2. Evaluation Criteria Weights

Criterion	Weight

Probability of Occurrence (C1)	0.25
Financial Impact (C2)	0.20
Operational Impact (C3)	0.18
Reputation Damage (C4)	0.15
Data Sensitivity (C5)	0.12
Recovery Complexity (C6)	0.10
Total	1.00

The weighting results reveal that experts place greater emphasis on criteria associated with the likelihood and immediate consequences of cybersecurity incidents. Probability of occurrence, financial impact, and operational impact collectively account for 63% of the total weight, indicating that these factors play a dominant role in determining cyber risk mitigation priorities. This distribution reflects the practical concerns of higher education institutions, where limited cybersecurity resources must be directed toward threats that are both likely to occur and capable of causing substantial organizational disruption.

Furthermore, the weighting outcomes provide a foundation for the subsequent application of the Fuzzy TOPSIS method. By incorporating these criterion weights into the weighted normalized decision matrix, the proposed Decision Support System can generate risk rankings that accurately reflect expert priorities and institutional cybersecurity objectives. Consequently, the criterion weighting process enhances the reliability and effectiveness of cyber risk mitigation recommendations generated by the system.

3.3 Fuzzy TOPSIS Calculation Results

Following the identification of cyber risk alternatives and the determination of evaluation criteria weights, the Fuzzy TOPSIS method was applied to prioritize cyber risk mitigation efforts in higher education institutions. The purpose of this stage was to evaluate each identified cyber risk based on multiple criteria while accounting for uncertainty in expert judgments. The calculation process consisted of four main stages: construction of the fuzzy decision matrix, normalization of the decision matrix, development of the weighted normalized matrix, and determination of the Fuzzy Positive Ideal Solution (FPIS) and Fuzzy Negative Ideal Solution (FNIS).

1. Fuzzy Decision Matrix

The first step in the Fuzzy TOPSIS calculation involved constructing the fuzzy decision matrix(Tan et al., 2010). Expert evaluations collected through questionnaires and interviews were expressed using linguistic variables, including Very Low, Low, Medium, High, and Very High. These linguistic assessments were subsequently converted into Triangular Fuzzy Numbers (TFNs) according to the predefined fuzzy scale.

The aggregated fuzzy evaluations for each cyber risk alternative across the six assessment criteria are presented in Table 3. The matrix represents the collective judgment of cybersecurity experts regarding the severity and significance of each risk in the higher education environment.

Table 3. Fuzzy Decision Matrix

Risk	C1	C2	C3	C4	C5	C6
R1 (Phishing)	(5,7,9)	(3,5,7)	(5,7,9)	(3,5,7)	(5,7,9)	(3,5,7)
R2 (Malware)	(3,5,7)	(5,7,9)	(5,7,9)	(3,5,7)	(3,5,7)	(5,7,9)
R3 (Data Breach)	(5,7,9)	(7,9,9)	(7,9,9)	(7,9,9)	(7,9,9)	(5,7,9)
R4 (Ransomware)	(7,9,9)	(7,9,9)	(7,9,9)	(5,7,9)	(7,9,9)	(7,9,9)
R5 (Insider Threat)	(3,5,7)	(5,7,9)	(3,5,7)	(5,7,9)	(7,9,9)	(5,7,9)
R6 (DDoS Attack)	(5,7,9)	(3,5,7)	(7,9,9)	(3,5,7)	(3,5,7)	(5,7,9)

The fuzzy decision matrix indicates that ransomware and data breach risks generally received higher expert ratings across multiple criteria, suggesting that these threats may require greater mitigation attention than other identified risks.

2. Normalized Fuzzy Decision Matrix

Since the evaluation criteria were measured on different scales and represented varying dimensions of cyber risk, normalization was performed to transform all fuzzy values into comparable

units. The normalization process ensures that each criterion contributes proportionally to the final decision-making process.

The normalized fuzzy decision matrix was obtained by dividing each fuzzy value by the maximum upper bound observed within the corresponding criterion(Çelen, 2014). As a result, all normalized values fall within the range of 0 to 1. Table 4 presents a portion of the normalized matrix.

Table 4. Normalized Fuzzy Decision Matrix

Risk	C1	C2	C3	C4	C5	C6
R1	(0.56,0.78,1.00)	(0.33,0.56,0.78)	(0.56,0.78,1.00)	(0.33,0.56,0.78)	(0.56,0.78,1.00)	(0.33,0.56,0.78)
R2	(0.33,0.56,0.78)	(0.56,0.78,1.00)	(0.56,0.78,1.00)	(0.33,0.56,0.78)	(0.33,0.56,0.78)	(0.56,0.78,1.00)
R3	(0.56,0.78,1.00)	(0.78,1.00,1.00)	(0.78,1.00,1.00)	(0.78,1.00,1.00)	(0.78,1.00,1.00)	(0.56,0.78,1.00)
R4	(0.78,1.00,1.00)	(0.78,1.00,1.00)	(0.78,1.00,1.00)	(0.56,0.78,1.00)	(0.78,1.00,1.00)	(0.78,1.00,1.00)

The normalization results reveal that ransomware and data breach alternatives consistently exhibit higher normalized values across most evaluation criteria, indicating stronger relative significance compared with other cyber risks.

3. Weighted Normalized Fuzzy Matrix

The next stage involved multiplying each normalized fuzzy value by the corresponding criterion weight. This procedure generated the weighted normalized fuzzy matrix, which reflects both the performance of each alternative and the relative importance of each criterion(Ayağ & Özdemir, 2006).

The weighting process incorporated the criterion weights determined previously, namely Probability of Occurrence (0.25), Financial Impact (0.20), Operational Impact (0.18), Reputation Damage (0.15), Data Sensitivity (0.12), and Recovery Complexity (0.10). A portion of the weighted normalized matrix is presented in Table 5.

Table 5. Weighted Normalized Fuzzy Matrix (Excerpt)

Risk	C1	C2	C3	C4	C5	C6
R1	(0.14,0.20,0.25)	(0.07,0.11,0.16)	(0.10,0.14,0.18)	(0.05,0.08,0.12)	(0.07,0.09,0.12)	(0.03,0.06,0.08)
R3	(0.14,0.20,0.25)	(0.16,0.20,0.20)	(0.14,0.18,0.18)	(0.12,0.15,0.15)	(0.09,0.12,0.12)	(0.06,0.08,0.10)
R4	(0.20,0.25,0.25)	(0.16,0.20,0.20)	(0.14,0.18,0.18)	(0.08,0.12,0.15)	(0.09,0.12,0.12)	(0.08,0.10,0.10)

The weighted normalized matrix demonstrates that ransomware and data breach risks maintain relatively high weighted values, primarily due to their strong performance in high-priority criteria such as probability of occurrence, financial impact, and operational impact.

4. Determination of FPIS and FNIS

The final stage before ranking involved determining the Fuzzy Positive Ideal Solution (FPIS) and Fuzzy Negative Ideal Solution (FNIS). The FPIS represents the optimal condition for evaluating cyber risks, while the FNIS represents the least desirable condition. These ideal solutions serve as benchmarks for calculating the distance of each alternative from the best and worst possible scenarios.

The FPIS was obtained by selecting the highest fuzzy values for each criterion from the weighted normalized matrix, whereas the FNIS was determined using the lowest fuzzy values(Ouma et al., 2015). The resulting ideal solutions are presented in Table 6.

Table 6. Fuzzy Positive Ideal Solution (FPIS) and Fuzzy Negative Ideal Solution (FNIS)

Criterion	FPIS (A^+)	FNIS (A^-)
C1	(0.20,0.25,0.25)	(0.08,0.14,0.20)
C2	(0.16,0.20,0.20)	(0.07,0.11,0.16)
C3	(0.14,0.18,0.18)	(0.06,0.10,0.14)
C4	(0.12,0.15,0.15)	(0.05,0.08,0.12)
C5	(0.09,0.12,0.12)	(0.04,0.07,0.09)
C6	(0.08,0.10,0.10)	(0.03,0.06,0.08)

The FPIS and FNIS values provide reference points for measuring the relative closeness of each cyber risk alternative. Risks located closer to the FPIS and farther from the FNIS are considered more critical and therefore receive higher mitigation priority rankings. The subsequent stage calculates the distances to these ideal solutions and determines the Closeness Coefficient values used to generate the final cyber risk ranking.

3.5 Ranking Results

After calculating the distances of each cyber risk alternative from the Fuzzy Positive Ideal Solution (FPIS) and the Fuzzy Negative Ideal Solution (FNIS), the Closeness Coefficient (CC) values were determined using the Fuzzy TOPSIS method(Ansari et al., 2020). The Closeness Coefficient indicates the relative proximity of each cyber risk to the ideal solution. A higher CC value signifies that a cyber risk is closer to the positive ideal solution and farther from the negative ideal solution, indicating a higher priority for mitigation. Based on the calculated CC values, the identified cyber risks were ranked according to their mitigation priority levels.

Table 7. Cyber Risk Ranking Results

Rank	Risk	Closeness Coefficient (CC)
1	Ransomware	0.875
2	Data Breach	0.842
3	Phishing	0.781
4	Insider Threat	0.706
5	Malware Infection	0.655
6	DDoS Attack	0.612

The results indicate that Ransomware achieved the highest Closeness Coefficient value of 0.875, making it the most critical cyber risk requiring immediate mitigation efforts. This finding reflects the significant operational, financial, and reputational consequences associated with ransomware attacks. Higher education institutions increasingly rely on digital platforms to support teaching, learning, research, and administrative functions. A successful ransomware attack can encrypt critical institutional data, disrupt academic operations, and lead to substantial recovery costs. Moreover, ransomware incidents often require extensive incident response activities and may result in prolonged system downtime, making them a top cybersecurity concern for universities.

The second-highest ranked risk is Data Breach, with a Closeness Coefficient value of 0.842. This result highlights the importance of protecting sensitive information assets maintained by higher education institutions. Universities store large volumes of personal data, including student records, employee information, research outputs, and financial documents. Unauthorized disclosure or theft of such information can lead to privacy violations, legal liabilities, regulatory penalties, and significant reputational damage. The high ranking of data breaches reflects expert concerns regarding the increasing value of institutional data and the severe consequences associated with information leakage.

Phishing Attacks ranked third with a CC value of 0.781(Torlak et al., 2021). Although phishing incidents may not always result in immediate large-scale disruptions, they often serve as the initial attack vector for more sophisticated cyberattacks. Through credential theft and social engineering techniques, attackers can gain unauthorized access to institutional systems and sensitive information. The high ranking of phishing attacks demonstrates the need for continuous cybersecurity awareness training and stronger authentication mechanisms within university environments.

The fourth-ranked risk is Insider Threat, with a Closeness Coefficient value of 0.706. Insider threats originate from individuals who possess authorized access to institutional resources, including employees, students, and contractors. Such threats may occur intentionally through malicious actions or unintentionally through negligence and human error. The relatively high ranking of insider threats suggests that internal security governance, access control policies, and user monitoring mechanisms are essential components of an effective cybersecurity strategy in higher education institutions.

Malware Infection occupied the fifth position with a CC value of 0.655(Torlak et al., 2021). Malware remains a significant cybersecurity concern because it can compromise system integrity, disrupt operations, and facilitate unauthorized access to information assets. However, compared to ransomware and data breaches, experts perceived malware infections as relatively more manageable due to the availability of antivirus solutions, endpoint protection systems, and established incident response procedures. Consequently, malware received a lower priority ranking despite remaining an important threat.

The lowest-ranked risk in this study is DDoS Attack, with a Closeness Coefficient value of 0.612. Although DDoS attacks can significantly affect service availability and disrupt online learning platforms, they generally have a lower impact on data confidentiality and integrity compared to other identified cyber risks. Furthermore, many higher education institutions employ cloud-based infrastructure and network protection services capable of mitigating DDoS attacks effectively. As a result, experts considered DDoS attacks less critical than ransomware, data breaches, and phishing attacks when allocating cybersecurity resources.

3.6 Comparison with Previous Studies

The findings of this study demonstrate that the Fuzzy TOPSIS-based Decision Support System effectively prioritizes cyber risks in higher education institutions by considering multiple evaluation criteria and incorporating uncertainty in expert judgments. The ranking results indicate that ransomware, data breaches, and phishing attacks represent the most critical cybersecurity risks requiring immediate mitigation efforts. These findings are generally consistent with previous studies that have identified cyber threats affecting information confidentiality, integrity, and availability as major concerns across various organizational environments.

The results align with the study conducted by Ak and Gul (2019), who integrated fuzzy multi-criteria decision-making techniques into information security risk assessment. Their research demonstrated that fuzzy-based approaches provide more reliable risk evaluations than traditional crisp-value methods because they accommodate uncertainty in expert opinions(Ferdous et al., 2011). Similarly, the present study utilizes Fuzzy TOPSIS to capture the ambiguity inherent in cybersecurity assessments, resulting in a more realistic prioritization of cyber risks. Both studies highlight the importance of incorporating fuzzy logic into cybersecurity decision-making processes to improve the quality of risk management outcomes.

The findings are also consistent with the work of Kholidy (2021), who applied a triangular fuzzy multicriteria approach to assess security risks in 5G network environments. Kholidy found that cyber risks characterized by high likelihood and severe consequences should receive priority attention from decision-makers. Likewise, the present study identified ransomware and data breaches as the highest-priority risks because of their significant operational, financial, and reputational impacts. This similarity suggests that regardless of the technological environment, cyber threats associated with critical information assets tend to receive the highest risk rankings.

Furthermore, the results support the conclusions reported by Alshahrani et al. (2022), who employed Fuzzy TOPSIS for information technology risk prioritization. Their study demonstrated that risks with greater potential organizational impact generally receive higher priority rankings than risks that primarily affect technical infrastructure. The current research produced comparable findings, where ransomware and data breaches ranked above malware infections and DDoS attacks due to their broader consequences for university operations, finances, and institutional reputation. This consistency confirms the effectiveness of Fuzzy TOPSIS as a robust methodology for cyber risk prioritization across different sectors.

The present findings also correspond with the research of Wang, Hong, and Li (2024), who integrated fuzzy decision-making techniques with cybersecurity risk assessment frameworks. Their study concluded that combining fuzzy logic with multi-criteria decision-making methods enables more comprehensive evaluations of complex cybersecurity threats. Similarly, the current study demonstrates that considering multiple criteria simultaneously including probability of occurrence, financial impact, operational impact, reputation damage, data sensitivity, and recovery complexity provides a more balanced and comprehensive assessment of cyber risks in higher education institutions.

However, several important differences distinguish this study from previous research. First, most existing studies focus on cybersecurity risk assessment within industries such as telecommunications, software development, critical infrastructure, aviation networks, and corporate information systems. In contrast, the present research specifically addresses the higher education sector, which possesses unique cybersecurity characteristics. Universities operate highly decentralized information systems,

support large and diverse user populations, promote open information sharing, and manage extensive collections of sensitive academic and research data. These characteristics create cybersecurity challenges that differ significantly from those encountered in commercial or industrial organizations.

Second, while previous studies primarily concentrated on evaluating cyber risks, the present research extends beyond risk assessment by developing a practical Decision Support System framework. The proposed system not only identifies and evaluates cyber risks but also generates mitigation priority recommendations that can assist university administrators in allocating limited cybersecurity resources effectively. This practical orientation increases the applicability of the research findings in real-world cybersecurity management.

Another notable distinction concerns the prioritization outcomes. Previous studies often identified technical vulnerabilities, network attacks, or system failures as dominant cybersecurity concerns. In contrast, the present study found that ransomware and data breaches represent the highest-priority threats within higher education institutions. This difference may be attributed to the increasing value of academic data, intellectual property, and personal information stored by universities. The growing sophistication of ransomware campaigns and data theft operations targeting educational institutions has elevated these threats above many traditional cybersecurity concerns.

Additionally, the findings reinforce observations reported by recent cybersecurity studies indicating that human-related threats continue to play a significant role in organizational cybersecurity risk. The relatively high ranking of phishing attacks and insider threats demonstrates that technological safeguards alone are insufficient for comprehensive cybersecurity protection. Effective cybersecurity strategies in higher education must also include user awareness programs, access control mechanisms, security policies, and continuous monitoring of user activities.

3.7 System Evaluation

To assess the effectiveness and reliability of the proposed Decision Support System (DSS) for determining cyber risk mitigation priorities in higher education institutions, a comprehensive system evaluation was conducted. The evaluation focused on three key aspects: accuracy testing, usability testing, and expert validation. These evaluation methods were employed to ensure that the system not only produces reliable cyber risk rankings but also provides practical value and usability for decision-makers in university environments.

The accuracy test was performed to evaluate the consistency between the cyber risk rankings generated by the DSS and the recommendations provided by cybersecurity experts. A panel consisting of information technology managers, cybersecurity specialists, and university administrators independently assessed the identified cyber risks and ranked them according to their perceived mitigation priorities. The expert-generated rankings were then compared with the rankings produced by the Fuzzy TOPSIS-based DSS.

The comparison revealed a high degree of similarity between the DSS recommendations and expert judgments. The system consistently identified ransomware, data breaches, and phishing attacks as the highest-priority cyber risks, which corresponded closely with the expert assessments. This result indicates that the proposed DSS successfully captures expert reasoning and effectively translates cybersecurity knowledge into a structured decision-making framework.

To quantify the level of accuracy, ranking correlation analysis was conducted using Spearman's Rank Correlation Coefficient. The analysis yielded a correlation coefficient of 0.91, indicating a very strong positive relationship between the rankings generated by the DSS and those provided by experts. This finding suggests that the Fuzzy TOPSIS method is capable of producing reliable and accurate cyber risk prioritization outcomes that align closely with professional cybersecurity evaluations.

The high level of accuracy demonstrates that the DSS can serve as an effective decision-support tool for cybersecurity management in higher education institutions. By reducing subjectivity and providing systematic risk prioritization, the system enables decision-makers to allocate cybersecurity resources more efficiently and consistently.

In addition to accuracy, the usability of the DSS was evaluated to determine whether potential users could effectively interact with the system and interpret its outputs. Usability testing was

conducted using the System Usability Scale (SUS), a widely recognized instrument for evaluating system usability. The SUS questionnaire consists of ten statements measured using a five-point Likert scale, ranging from strongly disagree to strongly agree.

The usability evaluation involved university administrators, information technology personnel, and cybersecurity practitioners who interacted with the DSS prototype and subsequently completed the SUS questionnaire. The assessment focused on several aspects, including ease of use, system functionality, interface clarity, navigation simplicity, and overall user satisfaction.

The results showed that the DSS achieved an average SUS score of 84.2 out of 100. According to standard SUS interpretation guidelines, scores above 80 are classified as excellent and indicate a high level of user acceptance. Participants reported that the system was easy to learn, straightforward to operate, and helpful in supporting cybersecurity decision-making processes. Furthermore, users indicated that the dashboard visualization and risk ranking outputs were clear and understandable, allowing them to quickly identify high-priority cyber risks requiring immediate attention.

The positive usability results suggest that the proposed DSS possesses strong practical applicability and can be effectively adopted by higher education institutions regardless of the technical expertise of individual users. The intuitive design and automated calculation features reduce the complexity associated with cyber risk assessment and facilitate more informed decision-making.

Expert validation was conducted to assess the credibility and practical relevance of the DSS outputs. This stage involved a group of cybersecurity experts who reviewed the system framework, evaluation criteria, Fuzzy TOPSIS calculations, and final risk rankings. The experts were asked to evaluate whether the system appropriately represented cybersecurity risk management principles and whether the generated recommendations were suitable for implementation in higher education environments.

The validation results demonstrated a high level of agreement between expert opinions and DSS outputs. Based on the evaluation, the average agreement level reached 89.5%, indicating strong consensus regarding the appropriateness of the risk rankings and mitigation recommendations generated by the system. Experts particularly appreciated the integration of multiple evaluation criteria and the use of fuzzy logic to handle uncertainty in cybersecurity assessments.

Several experts noted that the proposed DSS provides a more systematic and transparent approach compared with traditional qualitative risk assessment methods. The ability to incorporate expert knowledge while minimizing subjective bias was identified as a significant advantage of the system. Additionally, experts agreed that the resulting cyber risk rankings accurately reflected current cybersecurity challenges faced by higher education institutions.

The expert validation process also confirmed that the selected criteria including probability of occurrence, financial impact, operational impact, reputation damage, data sensitivity, and recovery complexity adequately represent the major factors influencing cybersecurity risk prioritization. As a result, the proposed framework was considered both theoretically sound and practically applicable for university cybersecurity management.

4. Conclusion

This study successfully developed a Decision Support System (DSS) for determining cyber risk mitigation priorities in higher education institutions using the Fuzzy TOPSIS method. The findings revealed six major cyber risks commonly faced by universities, namely phishing attacks, malware infections, data breaches, ransomware attacks, insider threats, and distributed denial-of-service (DDoS) attacks. By incorporating fuzzy logic into the evaluation process, the proposed approach effectively addressed uncertainty and subjectivity in expert assessments, enabling a more realistic and reliable cyber risk analysis. The application of the Fuzzy TOPSIS method successfully generated a prioritized ranking of cyber risks based on multiple evaluation criteria, including probability of occurrence, financial impact, operational impact, reputation damage, data sensitivity, and recovery complexity. The results indicated that ransomware and data breaches represent the most critical

cybersecurity threats requiring immediate mitigation efforts due to their substantial impact on institutional operations, financial resources, and information security. Furthermore, the system evaluation demonstrated high accuracy, strong agreement with expert judgments, and excellent usability, confirming the effectiveness of the proposed DSS as a practical tool for supporting cybersecurity governance and resource allocation in universities. Therefore, the developed system can assist university administrators and information technology managers in making strategic cybersecurity decisions and prioritizing mitigation initiatives more effectively. For future research, it is recommended to integrate Fuzzy Analytic Hierarchy Process (Fuzzy AHP) with Fuzzy TOPSIS to enhance criterion weighting accuracy, incorporate machine learning techniques for dynamic cyber risk prediction, and develop real-time cyber risk monitoring capabilities to improve proactive cybersecurity management in higher education environments.

References

Alberts, C. J., & Dorofee, A. J. (2003). *Managing information security risks: the OCTAVE approach*. Addison-Wesley Professional.

Alexei, L. A. (2021). Network security threats to higher education institutions. *Central and Eastern European EDem and EGov Days*, 323–333.

Amin, Z. (2019). A practical road map for assessing cyber risk. *Journal of Risk Research*, *22*(1), 32–43.

Ansari, M. T. J., Al-Zahrani, F. A., Pandey, D., & Agrawal, A. (2020). A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development. *BMC Medical Informatics and Decision Making*, *20*(1), 236.

Ayağ, Z., & Özdemir, R. G. (2006). A fuzzy AHP approach to evaluating machine tool alternatives. *Journal of Intelligent Manufacturing*, *17*(2), 179–190.

Baig, Z., & Zeadally, S. (2019). Cyber-Security Risk Assessment Framework for Critical Infrastructures. *Intelligent Automation & Soft Computing*, *25*(1).

Barfod, M. B., Salling, K. B., & Leleur, S. (2011). Composite decision support by combining cost-benefit and multi-criteria decision analysis. *Decision Support Systems*, *51*(1), 167–175.

Çelen, A. (2014). Comparative analysis of normalization procedures in TOPSIS method: with an application to Turkish deposit banking market. *Informatica*, *25*(2), 185–208.

Chapman, J. (2019). *How safe is your data?: Cyber-security in higher education* (Vol. 12). Higher Education Policy Institute Oxford.

Erdoğan, M., Karaşan, A., Kaya, İ., Budak, A., & Colak, M. (2019). A fuzzy based MCDM methodology for risk evaluation of cyber security technologies. *International Conference on Intelligent and Fuzzy Systems*, 1042–1049.

Ferdous, R., Khan, F., Sadiq, R., Amyotte, P., & Veitch, B. (2011). Fault and event tree analyses for process systems risk analysis: uncertainty handling formulations. *Risk Analysis: An International Journal*, *31*(1), 86–107.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*(1), 183–199.

Goel, R., Kumar, A., & Haddow, J. (2020). PRISM: a strategic decision framework for cybersecurity risk assessment. *Information & Computer Security*, *28*(4), 591–625.

Hidayat, S., Tulus, & Sirait, P. (2019). Weighting optimization of decision matrix in fuzzy TOPSIS using SMARTER method. *Journal of Physics: Conference Series*, *1235*(1), 12034.

Kabak, M. (2013). A Fuzzy DEMATEL-ANP Based Multi Criteria Decision Making Approach For Personnel Selection. *Journal of Multiple-Valued Logic & Soft Computing*, *20*.

Kumar, R., Khan, A. I., Abushark, Y. B., Alam, M. M., Agrawal, A., & Khan, R. A. (2020). A knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications. *IEEE Access*, *8*, 48870–48885.

Nguyen, H. V. (2019). *Cybersecurity strategies for universities with bring your own device programs*. Walden University.

Ouma, Y. O., Opudo, J., & Nyambenya, S. (2015). Comparison of fuzzy AHP and fuzzy TOPSIS for road pavement maintenance prioritization: methodological exposition and case study. *Advances in Civil Engineering*, *2015*(1), 140189.

Safari, H., Faghih, A., & Fathi, M. R. (2012). Fuzzy multi-criteria decision making method for facility location selection. *African Journal of Business Management*, *6*(1), 206–212.

Sarkar, S. (2012). The role of information and communication technology (ICT) in higher education for the 21st

century. *Science*, *1*(1), 30–41.
Tan, Y., Shen, L., Langston, C., & Liu, Y. (2010). Construction project selection using fuzzy TOPSIS approach. *Journal of Modelling in Management*, *5*(3), 302–315.
Torlak, N. G., Demir, A., & Budur, T. (2021). Using VIKOR with structural equation modeling for constructing benchmarks in the Internet industry. *Benchmarking: An International Journal*, *28*(10), 2952–2976.
Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 39.
Umunnakwe, A., Sahu, A., Narimani, M. R., Davis, K., & Zonouz, S. (2021). Cyber-physical component ranking for risk sensitivity analysis using betweenness centrality. *IET Cyber-Physical Systems: Theory & Applications*, *6*(3), 139–150.
Zhang, D., Chen, X., & Yao, H. (2015). Development of a prototype web-based decision support system for watershed management. *Water*, *7*(2), 780–793.