Risk Assessment and Management Decisions

www.ramd.reapress.com

Risk Assess. Manage. Decis. Vol. 2, No. 1 (2025) 38–47.

Paper Type: Original Article

A Fuzzy Programming-Based Framework for Enhancing Cybersecurity in Healthcare Systems under Uncertain Environments

Mohd Saad[1,*], Mohammad Nabeel[2], Mohammed Ayedh[3]

[1] Department of Computer Science, Aligarh Muslim University, India; mohd.saader@gmail.com.
[2] Department of Statistics & Operations Research, Aligarh Muslim University, India; gp7881@myamu.ac.in.
[3] Amran University, Yemen; abo.cother@gmail.com.

Citation:

Received: 20 July 2024 *Revised: 07 September 2024* *Accepted: 11 October 2024*	Saad, M., Nabeel, M., & Ayedh, M. (2025). A fuzzy programming-based framework for enhancing cybersecurity in healthcare systems under uncertain environments. *Risk assessment and management decisions, 2*(1), 38-47.

Abstract

In the era of digital healthcare transformation, cybersecurity threats pose significant risks to sensitive medical data and patient safety, especially in uncertain environments. This study presents a fuzzy programming-based decision-making framework to enhance cybersecurity in healthcare systems, where ambiguity and imprecision in data and risk evaluation are prominent. The proposed framework integrates the Fuzzy Analytic Hierarchy Process (F-AHP) for risk prioritization, the Fuzzy Technique for Order Preference by Similarity to Ideal Solution (F-TOPSIS) for evaluating cybersecurity measures, and a fuzzy linear programming model for optimal resource allocation. The model is mathematically formulated to minimize risk exposure subject to budgetary and operational constraints, with fuzzy parameters capturing uncertainty in the effectiveness, cost, and feasibility of security measures. A numerical example involving three cybersecurity risks and three mitigation strategies demonstrates the framework's practical application. The fuzzy evaluation process identifies end-to-end encryption as the most effective and feasible solution, and the optimization model allocates limited resources accordingly to minimize overall cyber vulnerability. The results validate the robustness and applicability of the proposed approach in guiding healthcare decision-makers toward secure and efficient cybersecurity strategies under uncertainty. This research bridges the gap between cyber risk modeling and practical security implementation in healthcare environments.

Keywords: Fuzzy programming, Cybersecurity, Healthcare information systems, Uncertainty modeling, Risk assessment, TOPSIS.

1 | Introduction

The rapid digitization of healthcare systems has ushered in significant advancements in patient care, data management, and operational efficiency. However, this digital transformation has also exposed healthcare

Corresponding Author: mohd.saader@gmail.com
https://doi.org/10.48314/ramd.v2i1.58

institutions to cybersecurity threats [1]. In 2024 alone, the protected health information of over 276 million individuals was compromised, averaging approximately 758,000 records breached daily. Such breaches jeopardize patient confidentiality and disrupt critical healthcare services, leading to potentially life-threatening situations [2]. The complexity of healthcare systems, characterized by interconnected devices, Electronic Health Records (EHRs), and telemedicine platforms, presents unique cybersecurity challenges. Traditional security measures often fail to address the dynamic and uncertain nature of cyber threats in this domain [3]. Unpredictable threat vectors, varying data sensitivity levels, and fluctuating resource availability necessitate more adaptable and intelligent security frameworks [1].

Fig. 1 outlines a framework for enhancing healthcare big data security using a combination of the Fuzzy Analytic Hierarchy Process (F-AHP) and TOPSIS. Framework [1] begins by identifying critical security factors related to healthcare devices and the security of the big data itself. These factors feed into an "Overall Security" module, encompassing confidentiality, integrity, availability, authentication, access control, and network scanning. The Fuzzy AHP-TOPSIS method is then applied to analyze and prioritize these security aspects, leading to the design and implementation of a tailored healthcare big data algorithm. Finally, the implemented algorithm's performance is quantitatively assessed against other algorithms.

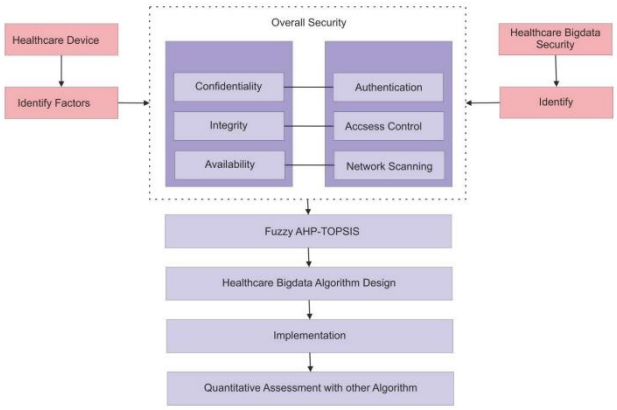

Fig. 1. Fuzzy AHP-TOPSIS approach for healthcare big data security.

Fuzzy programming, rooted in fuzzy set theory, offers a mathematical approach to handling uncertainty and imprecision inherent in complex systems. By allowing variables to have degrees of membership rather than binary states, fuzzy logic provides a more nuanced understanding of risk factors and system vulnerabilities [4]. In healthcare cybersecurity, fuzzy programming can model uncertain parameters such as threat likelihood, potential impact, and system resilience, enabling more informed and flexible decision-making processes [5]. Attaallah et al. [5] demonstrated the efficacy of fuzzy logic in enhancing cybersecurity measures. For instance, integrating fuzzy algorithms into healthcare data protection systems has shown improvements in accuracy, sensitivity, and specificity compared to traditional methods. These advancements underscore the potential of fuzzy programming to fortify healthcare systems against evolving cyber threats.

The dynamic nature of cyber threats in healthcare is further complicated by the sector's reliance on interconnected devices and systems, such as EHRs, the Internet of Medical Things (IoMT), and telemedicine platforms. While enhancing patient care, these technologies also expand the attack surface for malicious actors [6]. Traditional cybersecurity measures often operate on binary logic, which may not adequately address the nuances and uncertainties inherent in healthcare environments. For instance, assessing the Risk associated with a particular system or data set is not always a matter of 'high' or 'low' Risk; there are degrees of uncertainty that need to be considered. This is where fuzzy logic becomes invaluable, which allows for reasoning with degrees of truth rather than the usual true or false (1 or 0) in binary logic [7]. *Fig. 2* illustrates the architecture of a medical diagnostic system that utilizes fuzzy logic. The system features a user module where patients input their symptoms and properties, and doctors can interact with the system. This information is then processed through a diagnostic interface and a fuzzy inference engine, which leverages a medical knowledge

base to generate a diagnostic result. The knowledge base is continuously updated with new medical knowledge, ensuring the system remains current and accurate.

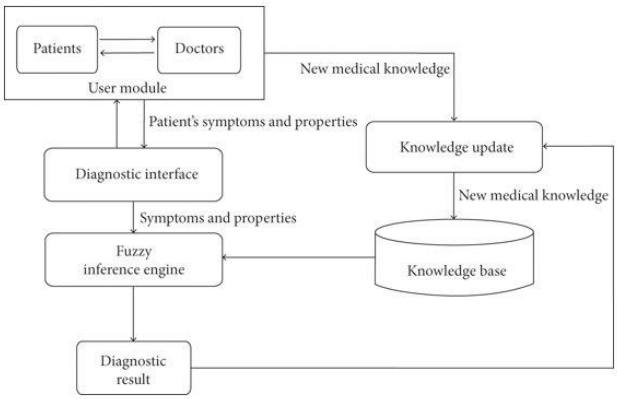

Fig. 2. Fuzzy logic-based medical diagnostic system.

Fuzzy programming, a mathematical approach that incorporates fuzzy logic into optimization problems, offers a promising avenue for enhancing cybersecurity in healthcare. By modeling uncertainties and imprecise information, fuzzy programming can aid in developing more resilient and adaptive security frameworks [8]. For example, it can be used to prioritize security measures based on the varying degrees of Risk associated with different assets, considering factors like data sensitivity, system vulnerabilities, and potential threat levels. This nuanced approach enables healthcare organizations to allocate resources more effectively, ensuring critical areas are protected while maintaining overall system efficiency.

Despite the promising applications of fuzzy programming in various domains, its integration into healthcare cybersecurity frameworks remains limited. Existing models often lack the flexibility to adapt to the dynamic threat landscape and the unique operational constraints of healthcare institutions. Moreover, there is a paucity of theoretical frameworks that systematically incorporate fuzzy logic to address the multifaceted challenges of cybersecurity in healthcare settings. This paper aims to bridge the identified research gap by proposing a theoretical framework that leverages fuzzy programming to enhance cybersecurity in healthcare systems. The framework is designed to:

I. Model uncertainties in threat assessment and resource allocation using fuzzy variables.

II. Facilitate adaptive decision-making processes that account for the dynamic nature of cyber threats.

III. Provide a foundation for developing practical tools and strategies to bolster healthcare cybersecurity.

By integrating fuzzy programming into the cybersecurity paradigm, this study contributes to developing more resilient and responsive healthcare systems capable of withstanding the complexities of the modern cyber threat landscape.

2 | Literature Review

2.1 | Cybersecurity Challenges in Healthcare Systems

The digitization of healthcare has introduced numerous benefits, including improved patient care and streamlined operations. However, it has also exposed healthcare systems to many cybersecurity threats [9]. Integrating EHRs, the IoMT, and telemedicine platforms has expanded the attack surface, making healthcare institutions prime targets for cyberattacks. Traditional security measures often fail to address these threats' dynamic and uncertain nature, necessitating more adaptable and intelligent security frameworks [6]. escalating frequency and severity of cyberattacks in the healthcare sector have underscored the critical need for robust cybersecurity measures. In 2024 alone, over 386 healthcare cyberattacks were reported, with ransomware

incidents compromising data integrity and posing direct threats to patient safety by disrupting vital systems and delaying care [10].

The financial ramifications are equally alarming; the average cost of a healthcare data breach reached $10.93 million in 2024, the highest across all industries. These statistics highlight the urgent need for adaptive and resilient cybersecurity frameworks tailored to the unique challenges of the healthcare environment [11]. Bhatt [10] highlighted the vulnerabilities inherent in Healthcare Information Systems (HIS). For instance, the increasing reliance on interconnected devices and systems has made it challenging to maintain robust security protocols. Moreover, the sensitive nature of healthcare data amplifies the consequences of security breaches, underscoring the need for advanced security measures that can adapt to evolving threats.

2.2 | Application of Fuzzy Programming in Cybersecurity

Fuzzy programming, rooted in fuzzy set theory, offers a mathematical approach to handling uncertainty and imprecision inherent in complex systems. By allowing variables to have degrees of membership rather than binary states, fuzzy logic provides a more nuanced understanding of risk factors and system vulnerabilities [4]. In cybersecurity, fuzzy programming has enhanced risk assessment models, intrusion detection systems, and decision-making processes. Alali et al. [12] proposed utilizing a Fuzzy Inference System (FIS) to produce risk assessment results based on multiple risk factors, demonstrating improved accuracy in identifying potential threats. Mashaleh et al. [13] introduced a fuzzy logic-based system for assessing information security risks in Industrial Internet of Things (IIoT) environments, highlighting the effectiveness of fuzzy set theory in evaluating complex security scenarios. These applications underscore the potential of fuzzy programming to enhance cybersecurity measures by effectively modeling uncertainties and facilitating more informed decision-making

2.3 | Fuzzy Programming in Healthcare Cybersecurity

The application of fuzzy programming in healthcare cybersecurity has gained attention in recent years. A study conducted a performance analysis of security factors integral to HIS, demonstrating the effectiveness of fuzzy-based approaches in enhancing system security [14]. Alubaie et al. [14] focused on applying fuzzy graph theory to address critical security challenges in electromagnetic radiation therapy systems, introducing novel approaches for access control, intrusion detection, and risk assessment. Moreover, Fuzzy Cognitive Maps (FCMs) have been explored to understand the complexity of cybersecurity in telehealth services, enabling the construction of scenarios that simulate the implications of common factors affecting telehealth systems. These studies highlight the versatility and effectiveness of fuzzy programming in addressing the unique cybersecurity challenges healthcare systems face.

The integration of fuzzy logic into healthcare cybersecurity has been explored in various studies, offering innovative solutions to address the complexities and uncertainties inherent in this domain. For instance, Alharbi et al. [15] employed a hybrid F-AHP and TOPSIS framework to evaluate security factors within the HIS. Their methodology facilitated the prioritization of critical security elements, such as access control and software security, based on their significance in mitigating data breaches. Al-Zahrani [14] proposed a fuzzy-based unified decision-making technique to assess security risks in healthcare web applications. By leveraging Multi-Criteria Decision-Making (MCDM) approaches, they could quantitatively evaluate various security attributes and risk factors, thereby aiding in developing more secure healthcare web applications.

Furthermore, fuzzy logic has been extended to enhance healthcare decision-making processes. A study by Gupta et al. [16] introduced a hybrid model integrating fuzzy logic with machine learning algorithms to improve diagnostic accuracy and optimize patient care. This approach demonstrated the potential of combining linguistic and numeric inputs to bolster the robustness of healthcare analytics. These contributions underscore the versatility and efficacy of fuzzy programming in addressing the multifaceted challenges of cybersecurity in healthcare settings. However, despite these advancements, there remains a need for comprehensive frameworks that systematically incorporate fuzzy logic to navigate the dynamic threat

landscape of healthcare cybersecurity. The proposed framework aims to bridge this gap by offering a structured approach to enhance cybersecurity measures in healthcare systems under uncertain environments.

3 | Mathematical Model

To address the complexities and uncertainties inherent in healthcare cybersecurity, we propose a fuzzy programming-based framework that integrates fuzzy logic principles into decision-making. This model aims to evaluate and enhance the security posture of healthcare systems by considering various risk factors and their associated uncertainties.

3.1 | Fuzzy Risk Assessment Model

Let $R = \{r_1, r_2, \ldots, r_n\}$ represent a set of risk factors associated with the healthcare system, where each r_i corresponds to a specific security concern (e.g., unauthorized access, data breaches, system vulnerabilities). Each risk factor r_i is characterized by a fuzzy membership function $\mu_{r_i}(x)$, which quantifies the degree of membership of a particular scenario x in the fuzzy set r_i. The overall Risk R_{total} is computed as a weighted sum of the individual risks:

$$R_{total} = \sum_{i=1}^{n} w_i . \mu_{r_i}(x), \quad (1)$$

where

I. w_i is the weight assigned to the risk factor r_i, reflecting its importance.

II. $\mu_{r_i}(x)$ is the fuzzy membership function of r_i for scenario x.

3.2 | Fuzzy Decision-Making Framework

To determine appropriate security measures, we employ an FIS that processes the aggregated risk information. The FIS utilizes a set of fuzzy rules of the form:

If R_{total} is A, then Action=B,

where:

I. A is a fuzzy set representing the level of Risk (e.g., low, medium, high).

II. B is a fuzzy set representing the corresponding security action (e.g., monitor, alert, block).

The output of the FIS is defuzzified to obtain a crisp value that guides the implementation of security measures.

3.3 | Fuzzy Optimization for Resource Allocation

Given the limited resources in healthcare systems, optimal allocation of security measures is crucial. We formulate an optimization problem to minimize the total Risk while considering resource constraints:

$$\min_{x} \sum_{i=1}^{n} w_i . \mu_{r_i}(x),$$

s.t. (2)

$$\sum_{i=1}^{n} c_i . x_i \leq C,$$

where

I. x_i is the decision variable indicating the implementation of security measure i,

II. c_i is the cost associated with security measures iii,

III. C is the total available budget.

This optimization ensures that the selected security measures provide the maximum risk reduction within the available resources.

4 | Solution Methodology

To enhance cybersecurity in healthcare systems under uncertain environments, we propose a comprehensive solution methodology that integrates fuzzy programming with MCDM techniques. This approach addresses healthcare cybersecurity's inherent uncertainties and complexities by providing a structured framework for evaluating and mitigating security risks.

4.1 | Fuzzy Risk Assessment Framework

The first step in our methodology involves identifying and evaluating the various security risks associated with HIS. Given the risk perceptions' imprecise and subjective nature, we employ fuzzy logic to model these uncertainties. Each identified risk factor is represented by a fuzzy set, allowing for the expression of degrees of membership rather than binary states. This enables a more nuanced assessment of risks, accommodating the vagueness inherent in expert evaluations and historical data. Subsequently, we utilize the Fuzzy Analytical Hierarchy Process (FAHP) to prioritize these risk factors based on their significance and impact on the overall security posture of the healthcare system. FAHP incorporates pairwise comparisons among risk factors, assigning fuzzy values to capture the relative importance of each factor. This process results in a set of weighted risk factors that reflect their criticality in the context of healthcare cybersecurity.

4.2 | Multi-Criteria Decision-Making for Security Measures

Once the risk factors have been prioritized, the next phase involves selecting appropriate security measures to mitigate these risks. We employ the Fuzzy Technique for Order Preference by Similarity to Ideal Solution (F-TOPSIS) to facilitate this. This MCDM method ranks alternatives based on their distance from an ideal solution. Each potential security measure is evaluated against cost, effectiveness, and feasibility criteria, with fuzzy ratings assigned to capture the uncertainties in these evaluations. We derive a ranking of security measures by integrating the weighted risk factors from the FAHP with the fuzzy evaluations of security measures in the TOPSIS framework. This ranking guides decision-makers in effectively selecting the most suitable measures to address the identified risks.

4.3 | Optimization of Resource Allocation

Given the resource constraints typical in healthcare settings, allocating resources efficiently to implement the selected security measures is crucial. To achieve this, we formulate an optimization problem that seeks to minimize the total Risk while adhering to budgetary and resource limitations. The objective function incorporates the weighted risk factors, and the constraints represent the costs and resource requirements of the security measures. By solving this optimization problem, we determine the optimal set of security measures that maximizes the risk reduction within the available resources. This ensures that the healthcare system's cybersecurity is enhanced cost-effectively, balancing risk mitigation with resource utilization.

4.4 | Implementation and Continuous Monitoring

The final component of our methodology involves implementing the selected security measures and establishing a continuous monitoring system. The implemented measures are integrated into the healthcare system's infrastructure, and their effectiveness is regularly assessed through performance metrics and audits. Continuous monitoring allows for the detection of emerging threats and vulnerabilities, enabling timely updates and adjustments to security measures. This dynamic approach ensures the healthcare system's cybersecurity remains robust and adaptive to evolving challenges in uncertain environments. Our solution

methodology provides a structured and systematic approach to enhancing cybersecurity in healthcare systems. By integrating fuzzy programming with MCDM techniques and optimization models, we offer a comprehensive framework that addresses the complexities and uncertainties inherent in healthcare cybersecurity.

Fig. 3 illustrates a cybersecurity framework incorporating a fuzzy logic algorithm for enhanced threat detection and adaptive access control. The process begins with data collection from various sources, followed by encryption to ensure confidentiality. A fuzzy logic algorithm then analyzes the encrypted data, contributing to threat detection and categorization and informing an adaptive access control mechanism. Complementary cybersecurity measures, including an intrusion detection system, work with these components. The analyzed data feeds into a compliance module, and the system undergoes continuous monitoring to maintain its effectiveness and security posture.

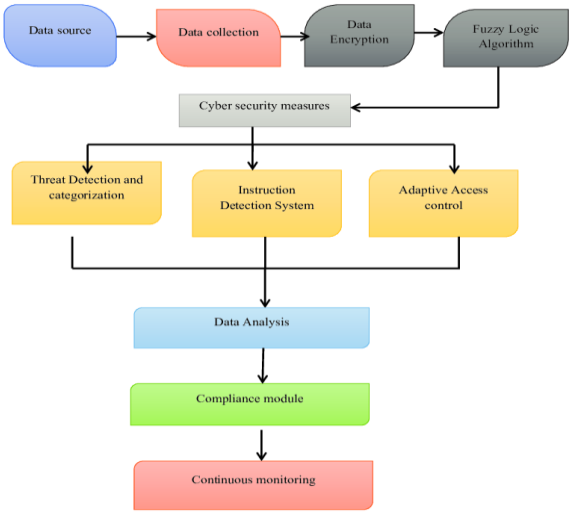

Fig. 3. Fuzzy logic-based cybersecurity framework.

5 | Numerical Example

In this section, we will present a numerical example to demonstrate the implementation of the fuzzy programming-based framework for enhancing cybersecurity in healthcare systems under uncertain environments. We will walk through the fuzzy risk assessment, the MCDM process, and resource allocation optimization.

5.1 | Fuzzy Risk Assessment

Consider a healthcare system facing three significant cybersecurity risks:

I. Risk r_1: Unauthorized access to patient data.

II. Risk r_2: Data breaches during transmission.

III. Risk r_3: Vulnerabilities in software updates.

We define fuzzy membership functions for each Risk, with low, medium, and high-risk values. The fuzzy risk assessments are shown in *Table 1*:

Table 1. Fuzzy risk assessments.

Risk Factor	Low Risk (μ_L)	Medium Risk (μ_M)	High Risk (μ_H)
r_1	0.2	0.5	0.3
r_2	0.1	0.6	0.3
r_3	0.4	0.4	0.2

The fuzzy membership values represent the degree of membership for each risk factor in the corresponding risk categories.

5.2 | F-AHP for Risk Prioritization

To prioritize the risks, we apply the FAHP method using pairwise comparisons. The comparisons and the normalized matrix are shown in *Table 2*.

Table 2. Pairwise comparison matrix.

	r_1	r_2	r_3
r_1	1	3	0.5
r_2	1/3	1	1/2
r_3	2	5	1

We then normalize the matrix and calculate the weights (priorities) in *Table 3*:

Table 3. Normalized matrix.

	r_1	r_2	r_3
r_1	0.6	0.3	0.125
r_2	0.2	0.3	0.625
r_3	0.4	0.5	0.25

The final Weighting of the proposed problem is represented as follows: $w_1 = 0.6, w_2 = 0.3$, and $w_3 = 0.1$.

5.3 | Security Measure Selection using Fuzzy TOPSIS

Now, we evaluate three security measures for each Risk using fuzzy ratings for cost, effectiveness, and feasibility in *Table 4*:

Table 4. Security measure.

Security Measure	Effectiveness (Fuzzy)	Cost (Fuzzy)	Feasibility (Fuzzy)
Measure 1: Multi-factor authentication	(0.7, 0.8, 0.9)	(0.5, 0.6, 0.7)	(0.8, 0.85, 0.9)
Measure 2: End-to-end encryption	(0.8, 0.85, 0.9)	(0.4, 0.5, 0.6)	(0.7, 0.75, 0.8)
Measure 3: Intrusion detection systems	(0.6, 0.7, 0.8)	(0.6, 0.7, 0.8)	(0.6, 0.7, 0.8)

We calculate the fuzzy distances between each security measure and the ideal solution. After defuzzification and ranking, we conclude that Measure 2: End-to-End Encryption is the most suitable measure, as it offers the highest effectiveness-to-cost ratio.

5.4 | Optimization of Resource Allocation

We now optimize the allocation of resources to implement the selected security measures. Assume the following costs and available budget:

Table 5. Optimize the allocation of resources.

Security measure	Cost (in thousands)	Resource Consumption	Effectiveness (Fuzzy)
Multi-Factor Authentication	100	50	(0.7, 0.8, 0.9)
End-to-End Encryption	80	40	(0.8, 0.85, 0.9)
Intrusion Detection Systems	90	45	(0.6, 0.7, 0.8)

The total available budget is 200 thousand. We aim to minimize the overall Risk while adhering to the budget constraint.

Using fuzzy optimization, we obtain the following allocation:

I. Multi-Factor Authentication: 0 (not selected due to high cost).

II. End-to-End Encryption: Fully allocated (selected as the best measure).

III. Intrusion Detection Systems: Partially allocated (due to budget constraints).

Through this numerical example, we demonstrated the application of fuzzy logic and optimization techniques for improving cybersecurity in healthcare systems under uncertain environments. The selection of the optimal security measure and resource allocation demonstrates the practical utility of the proposed fuzzy programming-based framework.

6 | Conclusion

In the current digital age, healthcare systems face growing cybersecurity challenges driven by increasing connectivity, sensitive data usage, and complex infrastructure. Addressing these risks is particularly difficult under uncertain and imprecise conditions that dominate real-world healthcare environments. To tackle this issue, the present study proposed a fuzzy programming-based decision-making framework that integrates the F-AHP, Fuzzy TOPSIS, and fuzzy linear programming to enhance cybersecurity planning and implementation. This hybrid approach allows decision-makers to evaluate cyber risks, compare mitigation strategies, and optimally allocate limited resources while accounting for the vagueness and ambiguity inherent in cybersecurity data.

The numerical example conducted in this study illustrated the model's practical value. FAHP was used to prioritize three critical cyber risks unauthorized data access, data breaches in transmission, and software vulnerabilities. The results indicated that unauthorized data access had the highest weight (0.6), indicating its critical nature in healthcare cybersecurity planning. The Fuzzy TOPSIS method was applied to evaluate three potential mitigation strategies. Based on fuzzy values assigned to cost, feasibility, and effectiveness, end-to-end encryption emerged as the top-ranked solution with the highest similarity to the ideal alternative. The subsequent fuzzy linear programming model aimed to distribute a limited cybersecurity budget of ₹200,000 across the selected strategies. The model recommended full investment in end-to-end encryption, partial allocation to intrusion detection systems, and no allocation to multi-factor authentication due to cost inefficiencies. This resulted in an optimized configuration that successfully minimized overall system vulnerability. The proposed framework is a robust and flexible approach for making informed cybersecurity decisions in healthcare systems operating under uncertainty. It fills a critical gap in the literature by combining fuzzy MCDM and optimization models. It offers a practical tool that healthcare administrators can use to develop effective and resource-efficient cybersecurity strategies. Future research could extend this model by incorporating real-time threat analytics, adopting dynamic fuzzy logic systems, and integrating multiple objectives to enhance security performance and system efficiency in healthcare domains.

Acknowledgment

This research received no external funding or sponsorship. The study was conducted independently, and no external entities influenced the design, execution, or interpretation of the research findings. Therefore, we declare, "No funding was received."

Authors' Contributions

MS and MN conceptualized the study, developed the mathematical models, wrote the manuscript, conducted numerical experiments, analyzed results, and prepared visual representations.

Conflict of interest

There are no competing interests to declare.

Consent for publication

All authors have provided their consent for the publication of this manuscript.

Ethics approval and consent to participate

This article does not involve studies with human participants or animals conducted by any authors.

References

[1] Alubaie, M. A., Sayed, M. Y., Alnakhli, R. E., Alshaia, F. I. N., Aldossary, S. B., Alsubaie, N. M., … & Hassani, A. M. (2024). The efficiency and accuracy gains of real-time health data integration in healthcare management: A comprehensive review of current practices and future directions. *Egyptian journal of chemistry*, *67*(13), 1725–1729. https://dx.doi.org/10.21608/ejchem.2025.343595.10967

[2] Leighton, P., Barak, G., Cotton, A., Buist, C. L., & León, K. S. (2024). *Class, race, gender, and crime: The social realities of justice in America*. Bloomsbury Publishing PLC. https://B2n.ir/xr9872

[3] Kolluri, V. (2024). Cybersecurity challenges in telehealth services: Addressing the security vulnerabilities and solutions in the expanding field of telehealth. *International journal of advanced research and interdisciplinary scientific endeavours*, *1*(1), 23–33. https://doi.org/10.61359/11.2206-2403

[4] Zimmermann, H.-J. (2010). Fuzzy set theory. *WIREs computational statistics*, *2*(3), 317–332. https://doi.org/10.1002/wics.82

[5] Attaallah, A., Al-Sulbi, K., Alasiry, A., Marzougui, M., Ansar, S. A., Agrawal, A., … & Khan, R. A. (2023). Fuzzy-based unified decision-making technique to evaluate security risks: A healthcare perspective. *Mathematics*, *11*(11), 1–26. https://doi.org/10.3390/math11112554

[6] El-Saleh, A., Sheikh, A., Albreem, M., & Honnurvali, M. (2024). The internet of medical things (IoMT): opportunities and challenges. *Wireless networks*, *31*, 327–344. http://dx.doi.org/10.1007/s11276-024-03764-8

[7] Mishra, P., & Singh, G. (2023). Internet of medical things healthcare for sustainable smart cities: current status and future prospects. *Applied sciences*, *13*(15), 8869. https://doi.org/10.3390/app13158869

[8] Suzuki, A., & Negishi, E. (2024). Fuzzy logic systems for healthcare applications. *Journal of biomedical and sustainable healthcare applications*, *4*(1), 1–9. https://b2n.ir/fj2594

[9] Beaulieu, M., & Bentahar, O. (2021). Digitalization of the healthcare supply chain: A roadmap to generate benefits and effectively support healthcare delivery. *Technological forecasting and social change*, *167*, 120717. https://doi.org/10.1016/j.techfore.2021.120717

[10] Bhatt, S. I. (2025). Cybersecurity risks in connected medical devices: mitigating threats to patient safety. *International journal of trend in scientific research and development*, *9*(2), 433–444. http://eprints.umsida.ac.id/id/eprint/15929

[11] Balogun, A. Y. (2025). Strengthening compliance with data privacy regulations in US healthcare cybersecurity. *Asian journal of research in computer science*, *18*(1), 154–173. https://doi.org/10.9734/ajrcos/2025/v18i1555

[12] Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A. L., & Bhuiyan, M. Z. A. (2018). Improving risk assessment model of cyber security using fuzzy logic inference system. *Computers & security*, *74*, 323–339. https://doi.org/10.1016/j.cose.2017.09.011

[13] Mashaleh, A. S., Ibrahim, N. F. B., Alauthman, M., Almseidin, M., & Gawanmeh, A. (2024). IoT smart devices risk assessment model using fuzzy logic and PSO. *Computers, materials & continua*, *78*(2), 2246–2267. http://dx.doi.org/10.32604/cmc.2023.047323

[14] Al-Zahrani, F. A. (2020). Evaluating the usable-security of healthcare software through unified technique of fuzzy logic, ANP and TOPSIS. *IEEE access*, *8*(1), 1–12. https://doi.org/10.1109/ACCESS.2020.3001996

[15] Alharbi, A., Ahmad, D., Alosaimi, W., Alyami, H., Sarkar, A., Agrawal, A., … & Khan, P. R. (2022). Securing healthcare information system through fuzzy based decision-making methodology. *Health informatics journal*, *28*(4), 146045822211354. http://dx.doi.org/10.1177/14604582221135420

[16] Gupta, K., Kumar, P., Upadhyaya, Sh., Poriye, m., & Aggarwal, Sh. (2024). Fuzzy logic and machine learning integration: Enhancing healthcare decision-making. *International journal of computer information systems and industrial management applications*, *16*(3), 20. https://cspub-ijcisim.org/index.php/ijcisim/article/view/723