The Fuzzy AHP Approach to Evaluation of Criteria Related to Active Cyber Attacks

Dušan Simjanović[1,*], Luka Ristić[1], Andrija Milovanović[1] and Aleksandar Jovanović[1]

[1]Faculty of Information Technology, Belgrade Metropolitan University, Tadeuša Košćuška 63, 11000 Belgrade, Serbia

Abstract

Cybersecurity encompasses the practices, technologies, and processes designed to protect networks, devices, and data from unauthorized access, attacks, and damage. In today's digital world, where a significant amount of information is stored online, cybersecurity has become increasingly important. This paper employs the AHP (Analytic Hierarchy Process) and FAHP (Fuzzy Analytic Hierarchy Process) methods to determine the importance of criteria related to active cyberattacks. The study identifies Social Engineering and Masquerade Attacks as the most critical threats.

The research focuses on developing a systematic framework for prioritizing cyberattack prevention strategies by analyzing the relative significance of various attack types. Through an in-depth assessment of criteria such as attack frequency, potential damage, and mitigation complexity, the study highlights the utility of decision-making tools in cybersecurity planning. Using both qualitative and quantitative data, the findings emphasize the pressing need to address vulnerabilities associated with human error and identity exploitation. Furthermore, the paper outlines practical recommendations for integrating AHP and FAHP methodologies into organizational risk management processes, ensuring a proactive approach to cyber defense. By leveraging these analytical techniques, organizations can allocate resources more effectively and reinforce resilience against the most prevalent and damaging forms of cyberattacks.

Keywords

cyber security, criteria, active attack, AHP, FAHP.

1. Introduction

In our increasingly digital world, the importance of cybersecurity cannot be overstated. Cybersecurity is essential for protecting computer systems, networks, and data from theft, damage, or unauthorized access. By investing in security, companies can ensure they remain safe and competitive in the market. As businesses, governments, and individuals rely more on technology, safeguarding information and ensuring the integrity of systems becomes paramount [1].

Cybersecurity encompasses a wide range of technologies and strategies used to defend against cyber threats. These threats can take various forms, including malware, phishing attacks, data breaches, and other cybercrimes. The goal of cybersecurity is to create a defense infrastructure capable of identifying, preventing, and responding to threats effectively.

With the always-on connectivity and advancements in technology today, threats rapidly exploit different aspects of technology. Any device in use nowadays is vulnerable to cyberattacks. For instance, in October 2016, a series of Distributed Denial of Service (DDoS) attacks targeted DNS servers, causing major web services to experience significant disruptions.

The increasing trend of remote work has led to a growing number of remote workers utilizing their infrastructures to connect with company systems. As the remote workforce expands, employees rely on their setups and networks to access company resources, which, if poorly planned and architected, can lead to insecure implementations. Similarly, the growth in companies allowing employees to bring their devices (BYOD) to work can result in security issues if not properly managed.

BISEC'2024: 15th International Conference on Business Information Security, November 28-29, 2024, Niš, Serbia

*Corresponding author.

dusan.simjanovic@metropolitan.ac.rs (D. Simjanović); luka.ristic.6001@metropolitan.ac.rs (L. Ristić); andrija.milovanovic.6310@metropolitan.ac.rs (A. Milovanović); aleksandar.jovanovic@metropolitan.ac.rs (A. Jovanović)

0000-0002-1709-0765 (D. Simjanović); 0000-0002-9815-4344 (A. Jovanović)

As the landscape of cyber threats continues to evolve, organizations must adopt a proactive approach to security. Humans are often the weakest link in the security chain, making old threats like phishing emails still impactful due to their psychological manipulation of users.

The storage, access, and management of data by both companies and private users have been transformed by cloud computing. While this convenience brings many benefits, it also raises concerns related to cyber threats. Cloud computing involves storing and accessing data files or software online instead of using physical hard disks or local servers. Although providers offer strong security measures, it is equally important for individuals using these services to safeguard their files and operating devices [2].

In the present day, the widespread adoption of cloud computing by numerous companies is evident. Many begin their cloud journey in a hybrid environment, where Infrastructure as a Service (IaaS) takes center stage, while some organizations may leverage Software as a Service (SaaS) for specific solutions.

On-premise security remains vital as the foundation of any organization, where the majority of users access critical resources. When an organization expands its on-premise infrastructure by integrating with a cloud provider for IaaS, it must carefully assess potential threats and devise effective countermeasures through comprehensive risk assessments.

Personal devices, although not directly connected to on-premise resources, can still compromise company data if users access corrupted SaaS applications, click on suspicious email links, or if former employees or unauthorized users gain access to company data stored on personal devices. Using the same passwords across multiple emails and sites can also lead to compromised accounts.

2. Data security

Data security involves safeguarding digital information from unauthorized access, corruption, or theft at every stage of its existence. This comprehensive concept spans various aspects of information security [3, 4]:

- *Physical Security:* Hardware storage devices and physical infrastructure are protected.
- *Administrative Controls:* Policies, guidelines, and procedures are implemented.
- *Logical Security:* Software applications, databases, and networks are secured.

Properly implemented, robust data security strategies ensure that an organization's information assets are protected against cybercriminal activities, insider threats, and human error, which are among the leading causes of data breaches today. Tools and technologies that enhance the organization's visibility into the location and usage of its critical data are deployed. Protections such as encryption, data masking, and redacting sensitive files are applied. Additionally, reporting is automated to streamline audits and help adhere to regulatory requirements.

To ensure the integrity and availability of sensitive information, these four data security measures can be implemented:

- *Encryption:* Algorithms are utilized to transform regular text characters into an unreadable format. These keys play a crucial role in scrambling data, ensuring that only authorized users can access it. File and database encryption software act as a protective barrier, obscuring sensitive information through encryption or tokenization. Additionally, many encryption tools incorporate security key management features.
- *Data Erasure:* Software is employed to thoroughly overwrite data on any storage device, ensuring it is more secure than conventional data wiping. It is confirmed that the data cannot be recovered. Data Masking: Real data is used for application development or training while protecting personally identifiable information (PII). This ensures that development can occur in compliance with privacy regulations.
- *Data Masking:* Real data is used for application development or training while protecting personally identifiable information (PII). This ensures that development can occur in compliance with privacy regulations.

- *Data Resiliency:* An organization's ability to withstand and recover from various failures, including hardware issues, power outages, and other events that affect data availability, is ensured. Rapid recovery is essential to minimize impact.

3. Cyber Attacks

A cyberattack is a malicious and deliberate attempt by an individual or organization to breach another individual's information system. Usually, the attacker seeks some type of benefit from disrupting the victim's network. Cyberattacks can be categorized into two categories: active and passive. The primary distinction lies in their impact on the target system's resources. Passive cyberattacks involve attempts to gain access to the target's system without directly affecting its system resources. In contrast, active cyberattacks can cause damage to the target's system, such as data breaches or ransomware attacks. One common byproduct of a cyber attack is a data breach, where personal data or other sensitive information is exposed. An active attack is an activity in which a hacker attempts to make changes to data on the target or data route to the target. There are several different types of active attacks. However, in all cases, the threat actor takes some sort of action on the data in the system or the devices the data resides on. Attackers may attempt to insert data into the system or change or control data that is already in the system. In the sequel, some types of cyber attack will be emphasized [1, 2, 3, 4, 5].

- CA1: *Social Engineering.* Social engineering attacks manipulate individuals into disclosing sensitive information, downloading potentially harmful software, accessing questionable websites, transferring funds to malicious actors, or making other security-compromising errors. These actions can have significant repercussions for both personal and organizational security.
- CA2: *Masquerade attack.* A masquerade attack is a detrimental and misleading cyber intrusion strategy, utilized by malicious actors to gain unauthorized access to networks, systems, or devices through the exploitation of stolen credentials or login data. By circumventing the existing digital infrastructure and deceiving authorization protocols to pose as legitimate system users, these threat actors can manipulate business transactions, perpetrate financial offenses, and disrupt operational processes. Unlike numerous other cyberattacks, masquerade attacks are primarily centered on human-related system vulnerabilities. The acquisition of stolen login credentials or the utilization of phishing emails to gather sufficient user information for unauthorized network entry is merely the initial stage of a masquerade attack. Once the target systems are breached, the potential for inflicting damage is virtually unbounded.
- CA3: *3. DoS attack.* A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. DoS attack can occur in two ways:
  1. Flooding. The attacker floods the target computer with internet traffic to the point that the traffic overwhelms the target system. The target system is unable to respond to any requests or process any data, making it unavailable to legitimate users.
  2. Malformed data. Rather than overloading a system with requests, an attacker may strategically send data that a victim's system cannot handle. For example, a DoS attack could corrupt system memory, manipulate fields in the network protocol packets, or exploit servers.
  A DoS attack is characterized by using a single computer to launch the attack.
  On the other hand, a distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.
- CA4: *Session hijacking attack.* A session hijacking attack is also called a session replay attack. In it, the attacker takes advantage of a vulnerability in a network or computer system and replays the session information of a previously authorized system or user. The attacker steals an authorized user's session ID to get that user's login information. The attacker can then use that information to impersonate the authorized user.

A session hijacking attack commonly occurs over web applications and software that use cookies for authentication. With the use of the session ID, the attacker can access any site and any data that is available to the system or the user being impersonated.

- CA5: *Message modification attack.* In a message modification attack, an intruder alters packet header addresses to direct a message to a different destination or to modify the data on a target machine. Message modification attacks are commonly email-based attacks. The attacker takes advantage of security weaknesses in email protocols to inject malicious content into the email message. The attacker may insert malicious content into the message body or header fields.

3.0.1. Preventing Cyber Attacks

To prevent cyber attacks, it's important to analyze the cybersecurity challenges that companies, governments, and individual users face today. It is necessary to obtain accurate data and research the state of the market. Not all companies use the same versions of operating systems or dedicated software, and this makes cybersecurity challenges harder. In other words, the most appropriate approaches to cybersecurity techniques are not specialized in certain industries. According to the Kaspersky Global IT Risk Report 2016, the main aspects of most data breaches are listed in the following order [6]

- Viruses, malware, and trojans
- Lack of diligence and untrained employees
- Phishing and social engineering
- Targeted attack
- Crypto and ransomware

The cybersecurity community has been practicing these three aspects for quite some time. Because they are old and well-known suspects in cybersecurity. The biggest problem is not an insufficient investment in securing systems, but rather human error. The reason can be when someone clicks on a phishing link and downloads a malicious file, such as a virus, malware, or trojan, onto their computer. This approach is known as social engineering. When an attacker has planned what is a specific target that will be attacked in their minds, we're talking about a targeted attack. Before attacking the systems, attackers spend time researching resources to perform public reconnaissance and gather important pieces of data. Attackers intend to steal and sell data on the dark web. Crypto and ransomware are creating a new level of challenge for cybersecurity analysts and organizations. In May 2017, the world faced the biggest ransomware attack in history. This ransomware is called WannaCry and exploits a known vulnerability in Windows SMBv1. Attackers used an exploit called EternalBlue, which was released in April 2017. The hacking group Shadow Brokers created this exploit. Some of the important works regarding the cyber securita criteria can be seen in [6, 7, 8, 9].

4. Methodology

Let all fuzzy sets defined on the set of real numbers $\mathbb{R}$ be represented as $F(\mathbb{R})$. The number $A \in F(\mathbb{R})$ is a fuzzy number if there exists $x_0 \in \mathbb{R}$ so condition $\mu_A(x_0) = 1$ holds, and $A_\lambda = \left[x, \mu_{A_\lambda}(x) \geq \lambda\right]$ is a closed interval for every $\lambda \in [0, 1]$. The membership function, a component of a triangular fuzzy number (TFN) A, is a function $\mu_A : \mathbb{R} \to [0, 1]$, defined as [5, 10]

$$\mu_A(x) = \begin{cases} (x-l)/(m-l), & l \leq x \leq m, \\ (u-x)/(u-m), & m \leq x \leq u, \\ 0, & \text{otherwise}, \end{cases} \tag{1}$$

where inequality $l \leq m \leq u$ holds. Variables l, m, and u are the lower, middle, and upper value, respectively, and when $l = m = u$, TFN becomes a crisp number. In the sequel, the triangular fuzzy number will be denoted by $\tilde{A} = (l, m, u)$.

Assume two TFNs, $\tilde{A}_1 = (l_1, m_1, u_1)$, $\tilde{A}_2 = (l_2, m_2, u_2)$, and scalar $k > 0$, $k \in \mathbb{R}$. The basic arithmetic operations (addition, subtraction, multiplication, scalar multiplication, and inverse element) are respectively defined as follows [11]:

$$\begin{aligned}
&\tilde{A}_1 \oplus \tilde{A}_2 = (l_1 + l_2, m_1 + m_2, u_1 + u_2),\\
&\tilde{A}_1 \ominus \tilde{A}_2 = (l_1 - u_2, m_1 - m_2, u_1 - l_2),\\
&\tilde{A}_1 \otimes \tilde{A}_2 = (l_1 \cdot l_2, m_1 \cdot m_2, u_1 \cdot u_2),\\
&k \cdot \tilde{A}_1 = (k \cdot l_1, k \cdot m_1, k \cdot u_1),\\
&\tilde{A}_1^{-1} = (1/u_1, 1/m_1, 1/l_1).
\end{aligned} \tag{2}$$

For a given triangular number $\tilde{A} = (l, m, u)$ the left side of the membership function $\mu_{\tilde{A}}$ and it's inverse are given as

$$\begin{aligned}
\mu^l_{\tilde{A}} &= (x - l)/(m - l);\\
(\mu^l_{\tilde{A}})^{-1} &= l + (m - l)y, y \in [0, 1],
\end{aligned} \tag{3}$$

and the right side of the membership function $\mu_{\tilde{A}}$ and it's inverse are given as

$$\begin{aligned}
\mu^r_{\tilde{A}} &= (u - x)/(u - m);\\
(\mu^r_{\tilde{A}})^{-1} &= u + (m - u)y, y \in [0, 1].
\end{aligned} \tag{4}$$

The total integral value, according to [12] as a combination of left and right integral values $I_L(\tilde{A})$ and $I_R(\tilde{A})$, is

$$\begin{aligned}
I^{\lambda}_T(\tilde{A}) &= \lambda I_R(\tilde{A}) + (1 - \lambda) I_L(\tilde{A})\\
&= \lambda \int_0^1 (\mu^r_{\tilde{A}})^{-1} dy + (1 - \lambda) \int_0^1 (\mu^l_{\tilde{A}})^{-1} dy\\
&= \frac{1}{2} (\lambda u + m + (1 - \lambda) l) .
\end{aligned} \tag{5}$$

where λ represents an optimism index. The optimistic ($\lambda = 1$), balanced ($\lambda = 0.5$) and pessimistic ($\lambda = 0$) point of view are significant to obtain and rank criteria, while semi-pessimistic ($\lambda = 0.25$) and semi-optimistic ($\lambda = 0.75$) point of view are used when additional opinion is needed or more accurate results required [13].

In the sequel, the steps of the FAHP will be presented.

Step I: Establishing the hierarchy

In general, the hierarchical structure has been organized vertically: the main goal is, as the most important component, at the top; the criteria that contribute to the goal are at the intermediate levels; and the sub-criteria are at the lowest level.

Step II: Matrix comparison

Determining the pairwise comparison matrix $\widetilde{D}$ in terms of TFNs. In this step, a positive fuzzy reciprocal comparison matrix $\widetilde{D} = (\tilde{d}_{ij})_{n \times n}$ with a total of $n(n-1)/2$ comparisons of elements from a higher level with elements from a lower level is developed. The fuzzy value $\tilde{d}_{ij}$ represents the degree of relative importance between criteria; $i = j$, $\tilde{d}_{ij} = (1, 1, 1)$, and $\tilde{d}_{ij} = 1/\tilde{d}_{ji}$, otherwise.

The fuzzy scale for constructing pairwise comparisons can be seen in [10].

The graphic representation of the used FAHP scale with all three values (lower, median, and upper) is presented in Figure 1.

Step III: Matrix consistency review

For a matrix $D = (d_{ij})_{n \times n}$, the consistency index CI and consistency ratio CR are calculated using equations

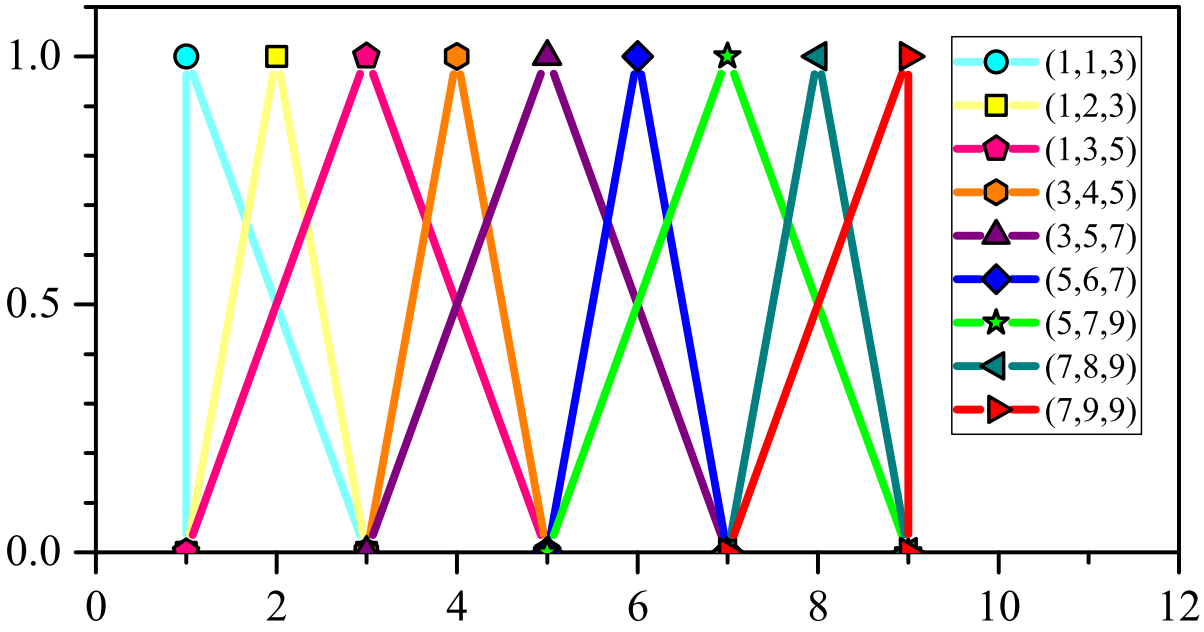

Figure 1: Graphic representation of triangular fuzzy numbers

$$CI = \frac{\lambda_{max} - n}{n-1}, \quad CR = \frac{CI}{RI}, \tag{6}$$

where $\lambda_{\max}$ corresponds to a maximal eigenvalue of matrices D and RI is a random index.

The value $CR < 0.1$ confirms the comparison matrix consistency, while otherwise the reason for inconsistency should be found and calculations repeated.

Step IV: The fuzzification phase

Using the triangular fuzzy numbers from the comparison matrix $\widetilde{D} = \left(\tilde{d}_{ij}\right)_{n\times n}$, applying

$$A = \sum_{i=1}^{n}\sum_{j=1}^{n}\tilde{d}_{ij} = \sum_{i=1}^{n}\sum_{j=1}^{n}\left(l_{ij}, m_{ij}, u_{ij}\right), \tag{7}$$

and

$$\begin{aligned} A^{-1} &= \left(\sum_{i=1}^{n}\sum_{j=1}^{n}\tilde{d}_{ij}\right)^{-1} \\ &= \left(\left(\sum_{i=1}^{n}\sum_{j=1}^{n}l_{ij}\right)^{-1}, \left(\sum_{i=1}^{n}\sum_{j=1}^{n}m_{ij}\right)^{-1}, \left(\sum_{i=1}^{n}\sum_{j=1}^{n}u_{ij}\right)^{-1}\right) \end{aligned} \tag{8}$$

the value of the fuzzy synthetic extent is obtained as follows [11]:

$$\begin{aligned} \widetilde{S}_i &= \sum_{j=1}^{n}\tilde{d}_{ij} \otimes A^{-1} \\ &= \sum_{j=1}^{n}\left(l_{ij}, m_{ij}, u_{ij}\right) \otimes A^{-1}, \quad i = \overline{1,n}. \end{aligned} \tag{9}$$

Step V: The defuzzification phase

The defuzzification phase starts with the weighted vector w_i in order to obtain the total integral value

for the TFNs, $\widetilde{S}_i$

$$w_i = I_T^{\lambda}(\widetilde{S}_i) = \frac{1}{2}\big(\lambda u_i + m_i + (1-\lambda)m_i\big),\ \lambda \in [0,1], i = \overline{1,n}, \tag{10}$$

Step VI: Normalization phase

In the normalization phase, the weight vectors w_i^* for criteria are obtained.

$$w_i^* = \frac{w_i}{\sum_{i=1}^{n} w_i} \tag{11}$$

Step VII: Ranking phase

The weights for each sub-criterion are obtained by multiplying the weights of the criteria and sub-criteria. Then, arranging the obtained weights, the sub-criteria ranking is received.

5. Results

We firstly discuss the criteria ranking using the previously described FAHP algorithm.

The comparison matrix is consistent since $CI = 0.017$, and $CR = 0.015$. In the sequel, Tables 1 and 2 present the comparison matrix and corresponding weights. In all cases, the criteria $CA1$ named Social engineering is on the top of the ladder with the weight 0.416 in the AHP, and 0.378 in the balanced FAHP case.

Next place, with the highest weight 0.271 in the pessimistic FAHP case takes the criteria Masquerade attack. Being 1.59 times smaller than the leading one in the AHP, and 1.41 times in the optimistic FAHP case, criteria $CA2$ justifies the second place [14]. Moderately important in the process of determining significant active cyber attacks is $CA3$=DoS attack. At the bottom of the ladder, being 6.67 times less important than the leading one (AHP case), is criteria Message modification attack.

In the case of semi-pessimistic ($\lambda = 0.25$) and semi-optimistic ($\lambda = 0.75$) point of view, $CA5$ has respectively 5.93 and 5.96 times smaller weight than $CA1$. The graphical presentation of criteria ranking can be seen in Figure 2.

6. Conclusion

The internet has indeed transformed computing, expanding opportunities while also increasing vulnerabilities. This dual nature has made computer security more critical than ever, focusing on protecting

Table 1
Comparison matrix for the criteria.

	CA1	CA2	CA3	CA4	CA5
CA1	1	2	3	4	5
CA2	1/2	1	2	3	4
CA3	1/3	1/2	1	2	3
CA4	1/4	1/3	1/2	1	2
CA5	1/5	1/4	1/3	1/2	1

Table 2
Weights for the criteria in the AHP and FAHP case.

	AHP	FAHP		
		$\lambda = 0$	$\lambda = 0.5$	$\lambda = 1$
CA1	0.416212445	0.386363011	0.377617079	0.374014953
CA2	0.261787988	0.270868309	0.267093133	0.265538278
CA3	0.161050407	0.168968396	0.182586463	0.188195241
CA4	0.098572773	0.108697307	0.109250191	0.109477904
CA5	0.062376387	0.065102977	0.063453133	0.062773624

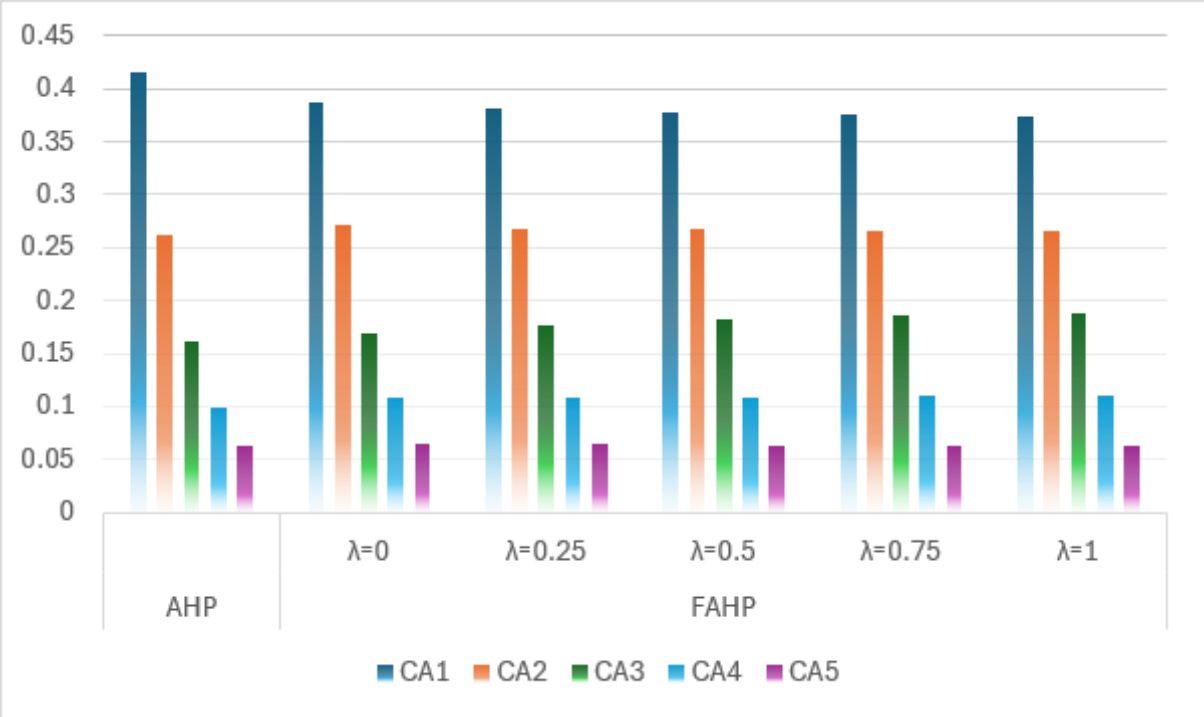

Figure 2: Graphic representation of criteria ranking

valuable data across various devices and networks. AHP and its generalizations in multi-criteria decision-making are particularly useful in navigating the complexities of security decision-making. Since its introduction by Saaty, AHP has provided a structured approach to quantify criteria weights, enabling more informed choices in security strategies. This methodology helps organizations prioritize risks and allocate resources effectively, ensuring that the most critical vulnerabilities are addressed. By applying AHP in security contexts, decision-makers can evaluate multiple factors—such as potential impact, likelihood of occurrence, and mitigation costs—systematically. This structured decision-making process is essential in today's landscape, where the stakes are high and the threats are constantly evolving. As the most important criteria in this work, Social engineering, and Masquerade attacks stand out. With the constant increase in threats in the cyber world, the idea like the one presented in this paper could be used in the improvement of protocols deployed, for instance, smart cities security platforms, in machine learning security, and lightweight cryptography. The findings in this paper present a starting point for our continual research in the cyber security area. We also plan to add or remove certain factors or sub-factors. Furthermore, an extension to this research could focus on the practical application for the ranking of the alternatives.

Acknowledgment

This paper was supported by the Blockchain Technology Laboratory at Belgrade Metropolitan University, Belgrade, Serbia.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Y. Diogenes, E. Ozkaya, Cybersecurity–attack and defense strategies, Small 622 (2021) 622.

[2] K. Thakur, A.-S. K. Pathan, Cybersecurity fundamentals: a real-world perspective, CRC Press, 2020.

[3] S. Alam, Cybersecurity: Past, present and future, arXiv preprint arXiv:2207.01227 (2022).

[4] M. Hasib, Cybersecurity leadership: powering the modern organization, volume 1, Tomorrow's Strategy Today, 2022.

[5] D. Simjanović, N. Vesić, B. Ranđelović, Đ. Vujadinović, Cyber security criteria: Fuzzy ahp approach (2023).

[6] A. Alharbi, A. H. Seh, W. Alosaimi, H. Alyami, A. Agrawal, R. Kumar, R. A. Khan, Analyzing the impact of cyber security related attributes for intrusion detection systems, Sustainability 13 (2021) 12337.

[7] M. Abdel-Basset, A. Gamal, K. M. Sallam, I. Elgendi, K. Munasinghe, A. Jamalipour, An optimization model for appraising intrusion-detection systems for network security communications: Applications, challenges, and solutions, Sensors 22 (2022) 4123.

[8] A. Agrawal, A. H. Seh, A. Baz, H. Alhakami, W. Alhakami, M. Baz, R. Kumar, R. A. Khan, Software security estimation using the hybrid fuzzy anp-topsis approach: Design tactics perspective, Symmetry 12 (2020) 598.

[9] S. G. Bhol, J. Mohanty, P. K. Pattnaik, Cyber security metrics evaluation using multi-criteria decision-making approach, in: Smart Intelligent Computing and Applications: Proceedings of the Third International Conference on Smart Computing and Informatics, Volume 2, Springer, 2020, pp. 665–675.

[10] D. M. Milošević, M. R. Milošević, D. J. Simjanović, Implementation of adjusted fuzzy ahp method in the assessment for reuse of industrial buildings, Mathematics 8 (2020) 1697.

[11] D.-Y. Chang, Applications of the extent analysis method on fuzzy ahp, European journal of operational research 95 (1996) 649–655.

[12] O. Kulak, M. B. Durmuşoğlu, C. Kahraman, Fuzzy multi-attribute equipment selection based on information axiom, Journal of materials processing technology 169 (2005) 337–345.

[13] D. J. Simjanović, N. Zdravković, N. O. Vesić, On the factors of successful e-commerce platform design during and after covid-19 pandemic using extended fuzzy ahp method, Axioms 11 (2022) 105.

[14] S. Seo, D. Kim, Study on inside threats based on analytic hierarchy process, Symmetry 12 (2020) 1255.