



## Article

# Analyzing the Impact of Cyber Security Related Attributes for Intrusion Detection Systems

Abdullah Alharbi <sup>1</sup>, Adil Hussain Seh <sup>2</sup>, Wael Alosaimi <sup>1</sup>, Hashem Alyami <sup>3</sup>, Alka Agrawal <sup>2</sup>, Rajeev Kumar <sup>4,\*</sup> and Raees Ahmad Khan <sup>2</sup>

<sup>1</sup> Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; amharbi@tu.edu.sa (A.A.); w.osaimi@tu.edu.sa (W.A.)

<sup>2</sup> Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow 226025, India; aadil3316@gmail.com (A.H.S.); alka\_csjmu@yahoo.co.in (A.A.); khaanraees@yahoo.com (R.A.K.)

<sup>3</sup> Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; hyami@tu.edu.sa

<sup>4</sup> Department of Computer Science and Engineering, Babu Banarasi Das University, Lucknow 226028, India

\* Correspondence: rs0414@gmail.com

**Abstract:** Machine learning (ML) is one of the dominating technologies practiced in both the industrial and academic domains throughout the world. ML algorithms can examine the threats and respond to intrusions and security incidents swiftly in an instinctive way. It plays a critical function in providing a proactive security mechanism in the cybersecurity domain. Cybersecurity ensures the real time protection of information, information systems, and networks from intruders. Several security and privacy reports have cited that there has been a rapid increase in both the frequency and the number of cybersecurity breaches in the last decade. Information security has been compromised by intruders at an alarming rate. Anomaly detection, phishing page identification, software vulnerability diagnosis, malware identification, and denial of services attacks are the main cyber-security issues that demand effective solutions. Researchers and experts have been practicing different approaches to address the current cybersecurity issues and challenges. However, in this research endeavor, our objective is to make an idealness assessment of machine learning-based intrusion detection systems (IDS) under the hesitant fuzzy (HF) conditions, using a multi-criteria decision making (MCDM)-based analytical hierarchy process (AHP) and technique for order of preference by similarity to ideal-solutions (TOPSIS). Hesitant fuzzy sets are useful for addressing decision-making situations in which experts must overcome the reluctance to make a conclusion. The proposed research project would assist the machine learning practitioners and cybersecurity specialists in identifying, selecting, and prioritizing cybersecurity-related attributes for intrusion detection systems, and build more ideal and effective intrusion detection systems.

**Keywords:** machine learning; cybersecurity; hesitant fuzzy logic; AHP-TOPSIS; idealness assessment; IDS



**Citation:** Alharbi, A.; Seh, A.H.; Alosaimi, W.; Alyami, H.; Agrawal, A.; Kumar, R.; Khan, R.A. Analyzing the Impact of Cyber Security Related Attributes for Intrusion Detection Systems. *Sustainability* **2021**, *13*, 12337. <https://doi.org/10.3390/su132212337>

Academic Editors: Muhammad Shafiq, Jin-Ghoo Choi, Farman Ali and Amjad Ali

Received: 28 September 2021

Accepted: 2 November 2021

Published: 9 November 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

The progress in ICT is one of the most noticeable changes in the modern world. In the last few decades, the technological revolution has greatly influenced the whole world and changed the thinking of people and their lifestyles. One of the prominent and well-known technologies in this domain is machine learning. Machine learning, a sub-domain of artificial intelligence, was first proposed by Arthur Samuel 1959 [1,2]. After that, there was a significant increase in the use of ML techniques in various fields of life, and today, it is recognized as one of the most imminent and fast growing technologies, particularly for addressing issues such as future event prediction, disease diagnosis, market analysis, email filtering, intrusion detection, image and speech recognition, etc. [3]. ML algorithms have a strong ability to learn from both structured and unstructured data, and they may assist automated systems in a variety of real-life fields. Machine learning allows algorithms

to learn from previous (historical) data. As we all know, the digital world is driven by data. In such a scenario, with the use of data mining and machine learning techniques, the scientists and researchers find new and productive insights from these data. The existing data contain interesting patterns that help us to make future predictions about both the normal and abnormal events. Initially, data as a dataset are provided as input to the devised ML models to train itself accordingly. With the help of ML algorithms, these ML-based models learn from the data and improve their performance accordingly. After the completion of the training phase, the proposed model is to be tested and validated with new but relevant data so as to determine the efficiency and accuracy of the proposed ML model. Thus, with less human intervention and explicit programming, it would be possible to use the learning behavior and predict future events and activities [4]. At every correct decision, the input data program improves its performance measure. More formally, ML is defined as “A computer program is said to learn from experience  $E$  with respect to some class of tasks  $T$  and performance measure  $P$ , if its performance at tasks in  $T$ , as measured by  $P$ , improves with experience  $E$ ” [2]. Here, the main focus is on these three things: a set of tasks represented by  $T$ ; estimation of performance, which is denoted by  $P$ ; and  $E$ , which represents the source of experience for the program.

In recent times, ML has gained significant importance in the field of cyber security [5]. Generally, supervised and unsupervised techniques are two common classes of machine learning that are mostly focused on by researchers to design and build compact intrusion detection systems [6]. Intrusion detection systems provide proactive security mechanisms to detect different types of intrusions. Supervised ML-based intrusion detection systems as the name imply works under a supervised environment [7]. In it, labeled historical data is used to train and test the devised models. Supervised ML algorithms are implemented to build models that map the given inputs with the outputs based on the existing knowledge [8]. It infers the output class for an input object according to the knowledge perceived from labeled examples of training data. The input object is usually a vector of attributes of a most ideal class of which it has common characteristics. In supervised ML, the models are completely subjected to labeled data, and efficiency and accuracy of models are directly proportional to the quality of data, whereas unsupervised ML is a contrastive study against supervised ML, and in this, unsupervised ML algorithms are implemented to build intrusion detection systems. Data used in this context are completely unlabeled, and models are exclusively autonomous to compact internal representation of the given data according to their common characteristics [2]. Data are analyzed by the unsupervised ML models, and significant insights are found from this data to classify future data on the basis of these insights. ML makes deep insights into different real-life domains, and cybersecurity is one of them. On the basis of cybersecurity datasets, namely malware training data sets, spam identification data sets, intuition detention data sets, unified host and network datasets, malicious URLs, etc., ML-based models have to be trained first and then used to detect future cyber security threats. However, considering the idealness and prioritization of the idealness attributes at the initial stages of intrusion, detection system development has become a challenging and fascinating issue for cybersecurity experts and researchers. Attribute identification and prioritization is a decision-making problem and needs experts' views and deep research insights [8]. Moreover, idealness assessment of software security systems is a continuous process that must be performed periodically by the experts to test the proactive security preparedness, effectiveness, and accuracy of these products [9]. Hence, in this research endeavor, our focus is to analyze the impact of cyber security related attributes for intrusion detection systems and make an idealness assessment of ML-based intrusion detection systems owned by Indian hospitals under the hesitant fuzzy conditions through MCDM approaches. For this assessment, the identification and selection of the relevant attributes is based on the experts' views. This idealness assessment will help the researchers and cybersecurity experts to identify and prioritize the ideal cybersecurity attributes in the context of ML-based intrusion detection systems. Besides this, the study's findings will also help in building more robust and

ideal intrusion detection systems. MCDM approaches have been used frequently by the researchers in several studies for various project assessments and evaluations. However, we did not find any research study that used the hesitant fuzzy-based MCDM techniques to make idealness assessment of intrusion detection systems. Thus, this work aims at using a novel approach to assess the ML based intrusion detection systems by practicing AHP-TOPSIS approaches under the hesitant fuzzy conditions.

AHP, an MCDM approach, offers a lot of potential when it comes to solving hierarchical decision-making problems. T.L. Saaty initially suggested the proposed approach in 1970 [8]. The method has undergone numerous improvements since then. It offers a practical method for calculating the weight of criteria (attributes). Instead of merely affixing a particular value, it assists the specialists in finding the decision that best matches their objective and understanding of the situation [10]. Furthermore, including hesitant fuzzy in this approach improves its efficiency and aids in the elicitation of more accurate findings [11]. Experts frequently experience a hesitation when making a decision in AHP and are unable to settle on a specific value, because they want to go above or below the values. These values, however, are not accessible [12,13]. In this case, the hesitant fuzzy sets are quite important. Reluctant fuzzy Sets are used to reflect the hesitant preferences of decision-makers. HF-logic can be used to eliminate hesitations that may arise during the decision-making process, especially when determining an element's membership in a fixed set is challenging. Such issues are beyond the scope of conventional fuzzy logic [14]. Since its introduction, the hesitant fuzzy collection has garnered a lot of attention from academics both at home and abroad. Furthermore, the TOPSIS method is well known for its ability to provide the greatest possible alternative ranking [8]. As a result, combining hesitant fuzzy logic with the AHP-TOPSIS technique improves the efficiency of this study and makes it suitable for evaluating the performance of ML-based intrusion detection systems.

Hesitant fuzzy based AHP-TOPSIS has a substantial capacity to solve MCDM problems caused by imprecise and uncertain data [11,14]. AHP under hesitant fuzzy conditions provides more accurate attribute weights, resulting in more effective outcomes [15], [16]. A more familiar technique for ranking options in MCDM problem solving is TOPSIS under hesitant fuzzy conditions [13]. Eight cybersecurity features are used as criteria in this study, while 10 machine learning-based intrusion detection systems are used as alternatives. The experts' views and well-known research works are used to identify and choose the characteristics. Here, the domain experts were consulted by our research team. Our team had also undertaken various research studies using different MCDM approaches. With knowledge and experience in this domain, the experts identified and chooses the suitable attribute sets for the specified problem that needed to be solved using the MCDM approaches. Consultation with the domain experts helped us to remove the redundancy, inconsistency, and ambiguity from the data (attribute set).

Furthermore, the study has been detailed in the following order: Section 2 presents the review of the existing relevant studies; Section 3 describes the framework of cybersecurity attributes related to the ML-based intrusion detection systems; Section 4 elaborates upon the implemented methodology; Section 5 describes the mathematical calculations and results; Section 6 incorporates the discussion; and Section 7 concludes the study.

## 2. Review of Existing Relevant Studies

Review of the existing relevant research works is an effective tool that provides ways to identify the actual research gap and establish the objectives for the current work. The few eminent and pertinent research studies that we found relevant to our proposed research endeavor are briefly discussed here:

- S. Bekesiene and colleagues (2021) organized a research endeavor to evaluate distance learning modules through integrated AHP TOPSIS approach under the fuzzy based environment [17]. In this study, three distance learning courses have been evaluated at three level stage assessment namely course structure, quality of information tools,

and student opinion. The fuzzy TOPSIS technique was found to be a practical method that delivered an excellent value analysis and ranking, according to the survey data.

- Almotiri (2021) proposed a study to assess the effectiveness of malicious traffic detention systems. In this study, he used AHP-TOPSIS under fuzzy environment to evaluate six malicious traffic detention systems [18]. The Host-based malicious traffic detection strategy (MTD4) was shown to be the most successful and long-lasting malicious traffic detection mechanism among the six alternatives in this investigation.
- Sahu and Colleagues (2020) presented a novel framework for software durability assessment using AHP-TOPOSIS under the hesitant fuzzy conditions [15]. They discovered that trustworthiness and maintainability are two essential and vital qualities for preserving the software durability.
- Agarwal and Colleagues (2020) used well-known patterns, sometimes known as design strategies, to create a fuzzy ANP-TOPSIS evaluation of the university's various software systems [8]. To analyze the university's software security, a unique set of security qualities in terms of security techniques was identified and selected.
- Alharbe (2020) conducted a research study for usable-security evaluation of information software systems [12]. For that, he used the MCDM approaches and enunciated guidelines that would help the practitioners in recognizing and prioritizing usable-security attributes while designing and developing the software.
- Kaur and colleagues (2020) worked on the detection and assessment of security risk-factors during web application development; the suggested study employs an adaptive neural fuzzy inference system [19]. This study offers practitioners suggestions for analyzing and prioritizing security concerns in healthcare web apps throughout the early phases of development in order to create safe software solutions.
- Solangi and colleagues (2019) created a system for evaluating the best renewable energy resource for electricity production [10]. Fuzzy-based TOPSIS and Delphi-AHP algorithms were used to conduct this experiment. In this study, wind energy was considered to be the greatest option for generating electricity in Pakistan.
- Goutam and colleagues (2019) proposed a tactic for calculating the vulnerability of online applications [20]. Penetration testing is a technique for identifying software flaws. To establish their security, financial web apps have been submitted to both manual and automated testing. Throughout the study, the results of both vulnerability assessment approaches are nearly identical.
- Sengul and colleagues (2015) developed a fuzzy-TOPSIS-based model to assess Turkey's renewable energy systems [13]. Shannon's entropy approach was used to compute the weights of the qualities. In this study, the hydro-power plant was found to be the best renewable energy supply system.
- The significance of hesitant fuzzy sets in MCDM systems was investigated by Qian and colleagues (2013) [14]. According to the findings, generalised HF sets are the best fit for cases when decision makers are confused which membership to choose due to a number of possible memberships with unknown probability.
- Buyukozkan and colleagues (2012) the authors used the integrated AHP-TOPSIS approach under fuzzy conditions to conduct an analytical research on healthcare electronic service quality [21]. Specialization, interactivity, service correctness, dependability, and responsiveness were determined to be the most important characteristics in providing satisfying and effective healthcare web services, according to the study.

From the analysis of the studies mentioned above, it was found that different MCDM techniques have been endorsed in various approaches/ methods such as F-AHP, TOPSIS, and F-ANP to find out the solutions for MCDM problems. However, we did not find any research study that used the integration of hesitant fuzzy logic with AHP-TOPSIS to make an idealness assessment of ML-based intrusion detection systems. Further, our identified criteria set are ideal to assess the effective characteristics of ML-based intrusion detection systems. This depicts the significance of our proposed research work.

### 3. Machine Learning in Cybersecurity

Machine learning as an emerging technology provides great flexibility to make insights into big data. This in turn helps researchers to analyze the existing huge amounts of data and find interesting patterns from it [4]. The insights examined from historical data through machine learning provide enormous benefits to modern industries and business organizations. Additionally, one of the interesting characteristics of machine learning techniques is to provide proactive security mechanism in the cybersecurity domain [5]. ML-based intrusion detection systems provide an effective security approach for addressing cybersecurity issues, examining threats and responding to intrusions and security incidents swiftly in an instinctive way. Cybersecurity experts and researchers have practiced different ML algorithms to address various cybersecurity issues [22]. The most commonly used machine learning algorithms are decision trees, support vector machine, naïve Bayes classifier, artificial neural networks, k-means clustering, convolutional neural networks, k-nearest neighbor, recurrent neural network, restricted Boltzmann machine, and fuzzy c-means clustering to design and develop intrusion detection systems [23,24]. These algorithms are practiced by researchers in different working scenarios to address cybersecurity issues. However, here, our aim is to make an idealness assessment of these ML-based intrusion detection systems with respect to the identified cybersecurity attributes.

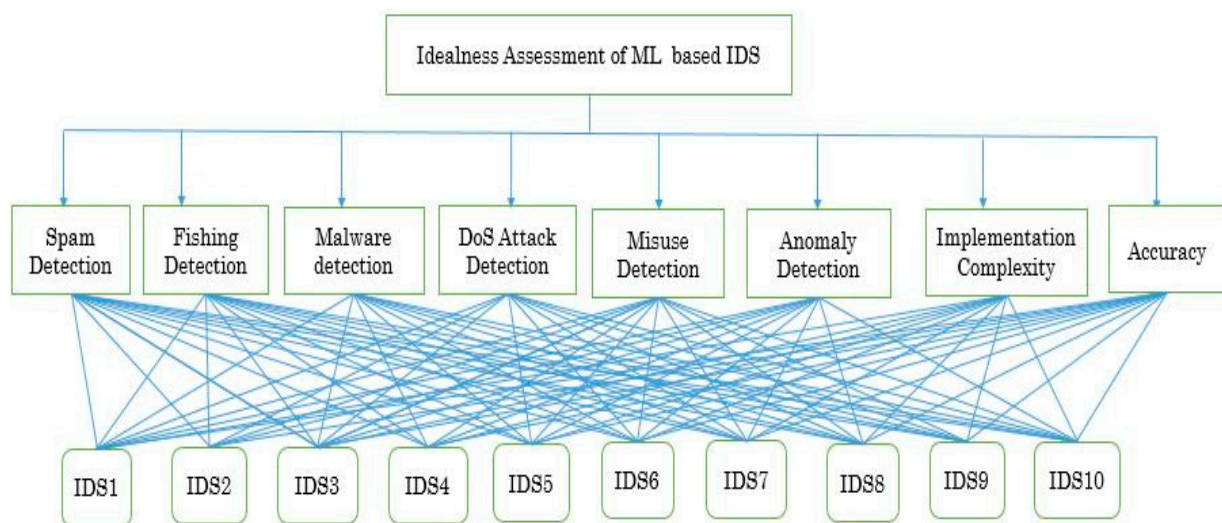
To improve the efficiency of intrusion detection systems and to prioritize the cybersecurity attributes concerning the ML-based intrusion detection systems, a case study was performed on ten ML-based intrusion detection systems installed in the hospitals of UP, India. The identification and selection of the attributes for the assessment of machine learning algorithms is a consensual decision based on the expert viewpoints and experience of authors. For this work, eight cybersecurity attributes concerning machine learning with 10 different alternatives for the idealness assessment of intrusion detection systems have been considered. These ten alternatives (intrusion detection systems) are symbolized as IDS-1, IDS-2, IDS-3, IDS-4, IDS-5, IDS-6, IDS-7, IDS-8, IDS-9, and IDS-10. The process of alternative selection is a result of collective decision of domain experts and owners of intrusion detection systems of different Indian hospitals for their comparative cyber-security assessment. The 10 selected intrusion detection systems have been installed at different hospitals for the detection of various cyber-security attacks. These detection systems have used different machine learning algorithms from basic to complex level of algorithm integration and hybridization. Each of the IDS uses more than one ML algorithm to detect different types of attacks. Additionally, with respect to our identified attribute set each intrusion detection system has gained a value between 0 and 1 for each attribute, as authors of the study have practiced hesitant fuzzy logic for this assessment. Moreover, the subjective cognition results of evaluators in linguistic terms for each intrusion detection system are based on the scale and experts' opinion, which is discussed in the methodology section. On the basis of the identified attribute set, the process of evaluation and quantitative results about the 10 different intrusion detection systems have been presented in Section 5 of this work. Figure 1 represents the identified attributes and alternatives. The subsection description and significance of the identified attributes are discussed in the figure below:

- (1) *Spam Detection*: Spam detection is a significant feature of ML-based intrusion detection systems that are used to identify spams. Spam, as a technical term, is mostly related to electronic mails and is known by some other names, such as junk mail or unsolicited bulk mail. It is unwanted and unwelcomed digital content that is used by spammers through different messaging systems [25]. Mostly, it comes in the form of unwanted and unnecessary mails through internet. Most of the times spams are used for commercial purposes and are just unpleasant in nature. However, sometimes, spam messages can be catastrophic for the system and system's user. In this scenario, the intention of spammers is to send malicious codes, execute phishing scams, and to earn money.

- (2) *Phishing Identification:* Cyber intrusions are very common at present, and there has been a rampant increase in their occurrence. Phishing is one of the common and interesting social engineering attacks used by intruders to steal confidential data. The targeted data often include credit card details and login credentials. In phishing, cyber criminals use the concept of spoofing, which helps them to masquerade as a legitimate and known source to the victim [24]. Mostly, they use it to spoof the websites of reputed organizations so that the victims can easily trust and share their confidential data. In addition, phishing attacks are also used to spread malware for system cookie stealing and keystroke capturing. Thus, detection of phishing attacks has become one of the significant features of ML-based intrusion detection systems.
- (3) *Malware Identification:* Malware, as a collective suit of various malicious software mainly, compromises viruses, spyware, key loggers, and ransomware. Malware is a code designed by cyber-attackers with the intention to cause severe damage in the victim's system or to acquire illegitimate network access. Generally, it is a coded file that is spread by cyber-attackers through different messaging systems such as e-mail and requires the victim to execute the malware. Different types of malware programs are designed for different purposes by the intruders and are often used to compromise the financial data of organizations and enterprises [24]. Machine learning algorithms have been produced by researchers for both malware detection and malware classification into different classes or families. Hence, detection of malware is also one of the key characteristics of ML-based intrusion detection systems.
- (4) *DoS Attacks Detection:* The three main components of security or cyber-security are confidentiality, integrity, and availability (CIA). These are commonly known as CIA triad and are considered the basic components for the security of any system or network. Among the three, one of the vital components is availability. Availability literally defines the character that is to be used or obtained, but in information security, it ensures that, whenever information and other resources are needed by the authentic users, there should be timely and reliable access to them [26]. To interrupt the functioning of the system and system resource access for its users, the cyber intruders use the DOS attacks. Denial of service (DoS) attacks are used to make online system resources unavailable to its users by flooding a server with traffic. The different types of DoS attack are teardrop attack, flooding attack, IP fragmentation attack, protocol attack, and application-based attack [24]. Researchers have practiced different ML algorithms to detect DoS attacks. Thus, detection of these attacks is also a key characteristic of ML-based intrusion detection models.
- (5) *Misuse Detection:* Misuse detection is a significant characteristic of ML-based intrusion detection systems. Misuse detection ensures the identification of those cybersecurity attacks that are familiar to an intrusion detection system [27]. The intrusion detection system already knows the nature of these attacks and has signatures of these attacks in their supporting database. Analysis and detection of new attacks are based on these existing signatures. Therefore, detection systems merely having this characteristic are very poor in detecting the unknown attacks whose signatures are not present in the supporting database.
- (6) *Anomaly Detection:* Identification or detection of zero-day attacks (unknown attacks) is a challenging issue and one of the important characteristics addressed by the ML-based approaches. The behavior of zero-day attack types is not recorded in the model's supporting database. An intelligent model based on machine learning analyzes these types of attacks and attempts to forecast their class based on its knowledge and experience [27]. Thus, identification of zero-day attacks is an essential attribute for an ML-based intrusion detection system. It plays a crucial role in making an ML-based intrusion detection model ideal for installation environment.
- (7) *Implementation Complexity:* As the name implies, it specifies all those complications that are considered during the whole implementation process of a system. Here, it defines all those complexity parameters that are considered by researchers, scientists,

and other stockholders to build an ML-based intrusion detection system. It includes processing power, amount of training data, working complexity of model, implementation complexity of an algorithm, overall cost of model and other required resources, etc. Thus, implementation complexity is also an essential attribute for evaluating an ML-based intrusion detection system and has been considered for this assessment.

- (8) *Accuracy*: This defines the measure of degree of correctness and precision of any computation or process corresponding to the right standard. It is one of the most notable features of ML algorithms. In machine learning, accuracy is determined by how well the proposed ML-based models generate the required results [27]. It is measured using precision, sensitivity, specificity, area under the curve, and other measures. It describes how accurate a machine learning-based model is when compared to the other models or techniques.



**Figure 1.** Idealness assessment attribute tree for ML-based intrusion detection systems.

All the above discussed attributes are relevant to the ML-based intrusion detection systems in some way. Moreover, all the identified attributes, by their implicit specifications, have a significant role in the overall idealness of ML-based intrusion detection systems. The authors of the study first identified a set of 20 attributes relevant to this study. After that, the domain experts' team was approached to finalize the attribute set. Experts made a group discussion about all the identified attributes and removed redundant and inconsistent attributes. Individual conflicts of experts regarding attribute selection were minimized, and finally, a set of eight cyber security attributes were selected in this expert group discussion. Hence, each of these attributes were considered for this assessment.

#### 4. Adopted Methodology

The methodology for our proposed work lays out a sequential approach for machine learning-based intrusion detection systems in the cyber security perspective. In order to complete this task, reluctant AHP and TOPSIS were used under fuzzy conditions. This technique helped us to obtain more accurate findings. In sectors where the solution to a problem could be anything from definitely true to absolutely false, hesitant fuzzy logic has acquired a lot of momentum as an improved variant of classical logic. It might be entirely *true*, *half true*, *half false*, or *entirely false*. It comes with the capacity to deal with information ambiguity [10]. The most appropriate approach for tackling issues that might yield numerous hierarchical solutions is the AHP. It does a hierarchical analysis of the problem. When it comes to the subjective and objective values of characteristics, AHP delivers reliable calculations [8]. TOPSIS is well recognized in the MCDM problem space for alternative ranking and examines the best alternative in the specified alternative set [8].

In this work, the weights of attributes are determined using AHP under fuzzy conditions, and then TOPSIS is used to rank the alternatives. The sequential working process for this study's analysis is shown in Figure 2. Numerical equations are presented in the next part to assist researchers in performing a numerical analysis of this work.

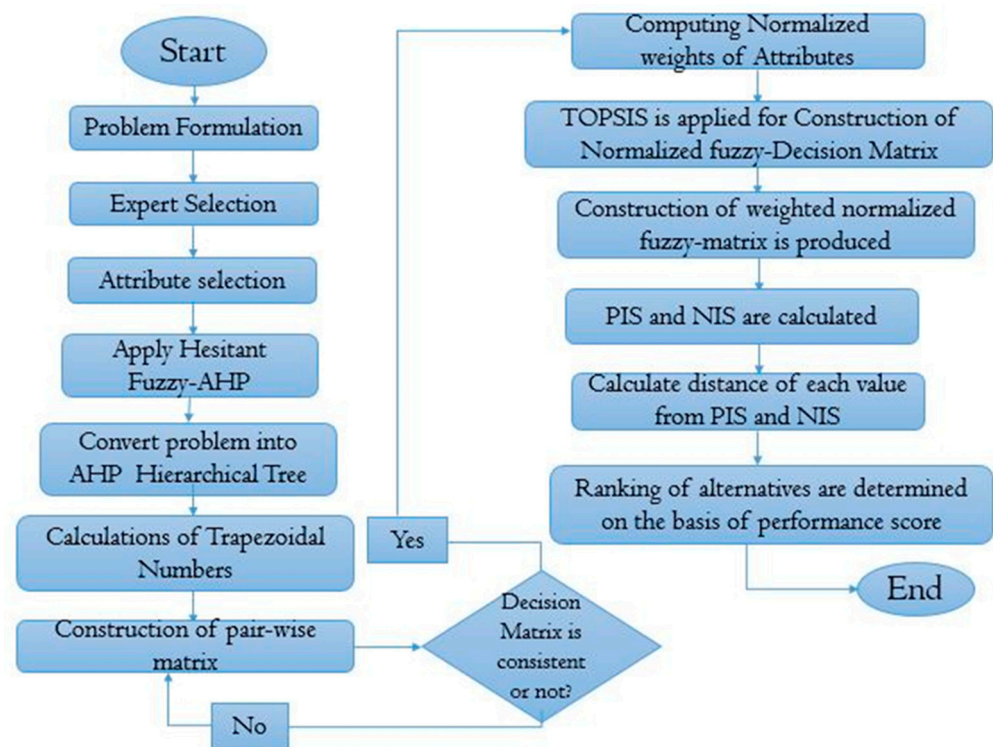


Figure 2. Sequential working procedure of AHP-TOPSIS under fuzzy conditions.

In this study, we presented hesitant fuzzy-AHP techniques to evaluate the priority of ML-based cybersecurity attributes, and then we calculated their testing and influence on alternatives (10 intrusion detection systems) for similar characteristics. The following is a detailed description of the approached methodology:

Point\_1: The suggested methodology's first step was to create hierarchical models for various attributes.

Point\_2: Using linguistic words and pair-wise comparisons between those attributes, decision makers used Table 1 as a guide.

Table 1. HF-AHP standard scale.

Rank	Abbreviation	Linguistic Term	Triangular Fuzzy Number
10	AHI	Absolutely High Importance	(7.0000, 9.0000, 9.0000)
9	VHI	Very High Importance	(5.0000, 7.0000, 9.0000)
8	ESHI	Essentially High Importance	(3.0000, 5.0000, 7.0000)
7	WHI	Weakly High Importance	(1.0000, 3.0000, 5.0000)
6	EHI	Equally High Importance	(1.0000, 1.0000, 3.0000)
5	EE	Exactly Equal	(1.0000, 1.0000, 1.0000)
4	ELI	Equally Low Importance	(0.3300, 1.0000, 1.0000)
3	WLI	Weakly Low Important	(0.2000, 0.3300, 1.0000)
2	ESLI	Essentially Low Importance	(0.1400, 0.2000, 0.3300)
1	VLI	Very Low Importance	(0.1100, 0.1400, 0.2000)
0	ALI	Absolutely Low Importance	(0.1100, 0.1100, 0.1400)

Point\_3: Fuzzy wrappers [27] were applied to modified outcomes. In the stated linguistic scale, it was assumed that  $T_0$  had the smallest priority and  $T_g$  has the greatest.



The evaluations were between  $T_i$  and  $T_j$ , such that  $T_0 \leq T_i \leq T_j \leq T_g$ , and an ordered weighted average of the attribute was performed as in Equation (1).

$$OWA(a_1, a_2, \dots, a_n) = \sum_{j=1}^n W_j b_j. \tag{1}$$

$W$  indicates the weight of attributes, while  $OWA$  describes the technique for ordered weighted averaging. Similarly, professionals use Equation (2) to obtain the trapezoidal numbers  $C = (l, m, n, o)$  after using Equations (1) and (5).

$$l = \min\{a_L^i, a_M^i, a_M^{i+1}, \dots, a_M^j, a_R^j\} = a_L^i \tag{2}$$

$$o = \max\{a_L^i, a_M^i, a_M^{i+1}, \dots, a_M^j, a_R^j\} = a_R^j \tag{3}$$

$$m = \left\{ \begin{array}{l} a_M^i, \text{ if } i + 1 = j \\ OWA_{w^{2(a_m^j, \dots, a_m^{\frac{i+j}{2}})}, \text{ if } i+j \text{ is even}} \\ OWA_{w^{2(a_m^j, \dots, a_m^{\frac{i+j+1}{2}})}, \text{ if } i+j \text{ is odd}} \end{array} \right\} \tag{4}$$

$$n = \left\{ \begin{array}{l} a_M^{i+1}, \text{ if } i + 1 = j \\ OWA_{w^{2(a_m^j, a_m^{j-1}, \dots, a_m^{\frac{(i+j)}{2}})}, \text{ if } i+j \text{ is even}} \\ OWA_{w^{2(a_m^j, a_m^{j-1}, \dots, a_m^{\frac{(i+j+1)}{2}})}, \text{ if } i+j \text{ is odd}} \end{array} \right\} \tag{5}$$

The 1st and 2nd type weights were calculated with the aid of Equations (6) and (7), using  $\eta$ . This is a number inside the unit interval  $[0, 1]$ , which experts obtain using Equations (6) and (7).

1st weight types ( $W1 = (w_1^1, w_2^1, \dots, w_n^1)$ ):

$$w_1^1 = \eta_2, w_2^1 = \eta_2(1 - \eta_2), \dots, w_n^1 \eta_2(1 - \eta_2)^{n-2} \tag{6}$$

2nd weight types ( $W2 = (w_1^2, w_2^2, \dots, w_n^2)$ ):

$$w_1^2 = \eta_1^{n-1}, w_2^2 = (1 - \eta_1)\eta_1^{n-1} \tag{7}$$

The formula depicts  $\eta_1 = \frac{u-(j-1)}{u-1}s$  and  $\eta_2 = \frac{l-(j-1)}{u-1}$ , where  $u$  specifies the upper assessment (see in Table 1  $u = 10$ ), and  $i$  and  $j$  specifies the attribute assessment ranks as low and high, respectively.

Point\_4: Approaching Equations (8) and (9), pair-wise comparison matrix ( $\tilde{A}$ ) has been computed by experts as

$$\tilde{A} = \begin{bmatrix} 1 & \dots & \tilde{c}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{c}_{n1} & \dots & 1 \end{bmatrix} \tag{8}$$

$$\tilde{c}_{ji} = \left( \frac{1}{c_{ij_u}}, \frac{1}{c_{ij_{m2}}}, \frac{1}{c_{ij_{m1}}}, \frac{1}{c_{ij_1}} \right) \tag{9}$$

Point\_5: Approaching Equation (10), to identify a comparison matrix, experts use it for defuzzification of the matrix.

$$\mu_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{10}$$

In Equation (10),  $l, m_1, m_2$ , and  $h$  depict four components of a trapezoidal number, that is, lower bound, upper middle bound, lower middle bound, and higher bound.

Experts approached Equations (11) and (12) to determine the consistency ratio of those values [7,28].

$$CI = \frac{\gamma_{max} - n}{n - 1}, \tag{11}$$

$$CR = \frac{CI}{RI}, \tag{12}$$

where *CI* stands for consistency index and *RI* stands for random index, which is established by Saaty [29] and changes for different *n* numbers. If the value of consistency ration was less than 0.1, our calculated matrix was consistent; otherwise, we returned to Point\_2 and updated our evaluation.

Point\_6: The geometric mean for row values was computed using Equation (13) by the domain experts.

$$\tilde{r}_i = (\tilde{c}_{i1} \otimes \tilde{c}_{i2} \dots \otimes \tilde{c}_{in})^{\frac{1}{n}} \tag{13}$$

Point\_7: Experts analyzed the weight of the most significant qualities by approaching Equation (14) to find the most important attributes.

$$\tilde{w}_i = \tilde{r}_1 \otimes (\tilde{r}_1 \oplus \tilde{r}_2 \dots \oplus \tilde{r}_n)^{-1} \tag{14}$$

Point\_8: Experts approached Equation (15) to the defuzzified values and conducted an analysis on them.

$$\mu_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{15}$$

Point\_9: By approaching Equation (16), experts defuzzified values and turned them into normalized weights.

$$\frac{\tilde{w}_i}{\sum_i \sum_j \tilde{w}_j} \tag{16}$$

Then, among the various alternatives, TOPSIS under hesitant fuzzy is utilized to choose the optimal alternative. TOPSIS has been shown to be one of the finest approaches for selecting the best option and assisting specialists in dealing with real-world situations as a widely used MCDM methodology [8]. The solutions created by TOPSIS are the furthest from the negative ideal solution and the closest to the positive ideal solution [8]. The suggested method is based on using envelopes to measure the distance between H1s and H2s, for example. Given the envelopes  $envp(H1s) = [T_p, T_q]$  and  $envp(H2s) = [T_p^*, T_q^*]$ , the distance is defined as Equation (17).

$$d(H1s, H2s) = |q^* - q| + |p^* - p| \tag{17}$$

Further, the procedure can be defined as:

Point\_10: Here, we assumed for the beginning step that the concerned problem had *E* alternatives ( $C = \{C_1, C_2, \dots, C_E\}$ ) and *n* criteria ( $C = \{C_1, C_2, \dots, C_n\}$ )

Here, *ex* represents the practitioners and *k* depicts the numeric count of experts in TOPSIS approach.

$\tilde{X}^l = [H_{S_{ij}}^l]_{E \times n}$  in TOPSIS technique is used to present a hesitant fuzzy decision matrix, where  $H_{S_{ij}}^l$  represents an alternative *i*(*C<sub>i</sub>*) estimated score against criteria (attribute) *j*(*A<sub>j</sub>*) specified by practitioners *e<sub>x</sub>*.

The HF-TOPSIS standard for evaluating criteria and the impact of outcomes is described as and falls between the extremely bad and highly good scale:

- $r_1^1$  = between medium and good (bt M&G)
- $r_2^1$  = at most medium (am M)
- $r_1^2$  = at least good (al G)
- $r_2^2$  = between very bad and medium (bt VB&M)

The comparative fuzzy envelope has been computed for each linguistic phrase as follows [14]:

$$envp_F(\text{EGH (btM\&G)}) = T (0.3300, 0.5000, 0.6700, 0.8300)$$

$$envp_F(\text{EGH (amM)}) = T (0.0000, 0.0000, 0.3500, 0.6700)$$

$$envp_F(\text{EGH (alG)}) = T (0.5000, 0.8500, 1.0000, 1.0000)$$

$$envp_F(\text{EGH (btVB\&M)}) = T (0.0000, 0.3000, 0.3700, 0.6700)$$

Point\_11: The aggregation of practitioners' individual assessments ( $\tilde{X}^1, \tilde{X}^2, \dots, \tilde{X}^K$ ) was taken, and construction of summarized decision matrix  $X = [x_{ij}]$  was completed with the help of Equation (18).

$$\begin{aligned} T_{pij} &= \min \left\{ \min_{i=1}^K \left( \max H_{t_{ij}}^x \right), \max_{i=1}^K \left( \min H_{t_{ij}}^x \right) \right\} \\ T_{qij} &= \max \left\{ \min_{i=1}^K \left( \max H_{t_{ij}}^x \right), \max_{i=1}^K \left( \min H_{t_{ij}}^x \right) \right\} \end{aligned} \tag{18}$$

Point\_12: In TOPSIS evaluation, the effective factor is denoted by  $b$ , whereas the most effective factor is denoted by  $A_j$ , and the cost characteristic is denoted by  $c$ . Furthermore, the lowest relative alternatives for cost-related preferences necessitate a high level of precision. Equations (19) and (22) were calculated to make a cost estimation and identify effective attributes [28]:

$$\begin{aligned} \tilde{V}_{pj}^+ &= \max_{i=1}^K \left( \max_i \left( \min H_{S_{ij}}^x \right) \right) j \in \alpha_b \\ &\text{and } \min_{i=1}^K \left( \min_i \left( \min H_{S_{ij}}^x \right) \right) j \in \alpha_c \end{aligned} \tag{19}$$

$$\begin{aligned} \tilde{V}_{qj}^+ &= \max_{i=1}^K \left( \max_i \left( \min H_{S_{ij}}^x \right) \right) j \in \alpha_b \\ &\text{and } \min_{i=1}^K \left( \min_i \left( \min H_{S_{ij}}^x \right) \right) j \in \alpha_c \end{aligned} \tag{20}$$

$$\begin{aligned} \tilde{V}_{pj}^- &= \max_{i=1}^K \left( \max_i \left( \min H_{S_{ij}}^x \right) \right) j \in \alpha_c \\ &\text{and } \min_{i=1}^K \left( \min_i \left( \min H_{S_{ij}}^x \right) \right) j \in \alpha_b \end{aligned} \tag{21}$$

$$\begin{aligned} \tilde{V}_{qj}^- &= \max_{i=1}^K \left( \max_i \left( \min H_{S_{ij}}^x \right) \right) j \in \alpha_c \\ &\text{and } \min_{i=1}^K \left( \min_i \left( \min H_{S_{ij}}^x \right) \right) j \in \alpha_b \end{aligned} \tag{22}$$

Point\_13: By approaching Equations (23) and (24), the positive and negative ideal matrixes ( $M^+$  and  $M^-$ ) were computed, respectively.

$$M^+ = \begin{bmatrix} d(x_{11}, \tilde{V}_1^+) + d(x_{12}, \tilde{V}_2^+) + \dots + d(x_{1n}, \tilde{V}_n^+) \\ d(x_{21}, \tilde{V}_1^+) + d(x_{22}, \tilde{V}_2^+) + \dots + d(x_{2n}, \tilde{V}_n^+) \\ d(x_{m1}, \tilde{V}_1^+) + d(x_{m2}, \tilde{V}_2^+) + \dots + d(x_{mn}, \tilde{V}_n^+) \end{bmatrix} \tag{23}$$

$$M^- = \begin{bmatrix} d(x_{11}, \tilde{V}_1^-) + d(x_{12}, \tilde{V}_2^-) + \dots + d(x_{1n}, \tilde{V}_n^-) \\ d(x_{21}, \tilde{V}_1^-) + d(x_{22}, \tilde{V}_2^-) + \dots + d(x_{2n}, \tilde{V}_n^-) \\ d(x_{m1}, \tilde{V}_1^-) + d(x_{m2}, \tilde{V}_2^-) + \dots + d(x_{mn}, \tilde{V}_n^-) \end{bmatrix} \tag{24}$$

Point\_14: Relative closeness score for each alternative was determined by approaching Equations (25) and (26).

$$CS(A_i) = \frac{M_i^+}{M_i^+ + M_i^-}, \quad i = 1, 2, \dots, m, \tag{25}$$

where

$$M_i^+ = \sum_{j=1}^n d(x_{ij}, V_j^+) \text{ and } M_i^- = \sum_{j=1}^n d(x_{ij}, V_j^-) \quad (26)$$

Point\_15: Based on the related relative proximity ratings, an ordered ranking of the options was given.

This work will use the above-mentioned systematic step-by-step methodology to conduct a case study on machine learning-based intrusion detection systems for the idealness evaluation in the cybersecurity perspective. The numerical computations for this investigation are detailed in the following part of this paper.

## 5. Numerical Calculations and Results

Evaluating the quality attribute of any software-based system, including cybersecurity, is a difficult process [8], since quantitative measurement of a qualitative characteristic is a complicated operation. This work's numerical analysis will give a quantitative assessment of machine learning-based intrusion detection systems. For this reason, this paper conducts a case study on ten different machine learning-based intrusion detection systems in order to assess their idealness characteristic from the cybersecurity perspective. Ten different intrusion detection systems have been selected as alternatives for this work. The alternative identification and their ranking evaluation is an integral part of the methodology chosen for our study. Further, these 10 different intrusion detection systems have been selected as alternatives on the basis of collective decision of domain experts and owners of intrusion detection systems for their comparative cyber-security assessment. AHP-TOPSIS under hesitant fuzzy conditions have been approached to make this task more corroborative and efficient. To determine the idealness assessment of ML-based intrusion detection system, eight attributes, namely spam detection, phishing detection, malware detection, DoS attack detection, misuse detection, anomaly detection, implementation complexity, and accuracy were considered for this experiment. The identified attributes have been represented as: CSA1, CSA2, CSA3, CSA4, CSA5, CSA6, CSA7, and CSA8, respectively, in the further study. Approaching Equations (1)–(26) described in Section 4 of this work, idealness assessment of ML-based intrusion detection systems have been performed using AHP-TOPSIS under hesitant fuzzy conditions as follows.

Initially, approaching Equations (1)–(9), and as a standard scale involving Table 1, the linguistic terms were transformed to the numeric values and later into HF-based crisp numeric values. Then, numerical calculations were carried out to create a pair-wise comparison matrix, and the concluding results are shown in Table 2. To obtain the final results for Table 2, the procedure experienced the implementation of fuzzy wrappers by approaching Equation (1); approaching Equations (2)–(5), estimation of trapezoidal numbers  $C = (l, m, n, o)$ ; and by approaching Equations (6) and (7), and considering  $\eta$ , which represents a number between (0–1), 1st and 2nd weight types have been found. At the end, the experts used Equations (8) and (9) to calculate the pair-wise comparison matrix. We have not represented the intermediately operations here due to the least significance.

With the use of Equations (10)–(16), the level 1 attributes' defuzzified values and normalized weights were computed, and the final findings are shown in Table 3. The following intermediate procedures were used in the whole process of calculating Table 3: first, Equation (10) was approached for defuzzification process to convert the pair-wise comparison matrixes into combined defuzzified values. Then, to check matrix consistency, Equations (11) and (12) were approached to determine both the consistency index and consistency ratio (CR) and our determined CR = 0.03485540 for this work, that is <0.1 that depicts our evaluated matrix is consistent. Afterwards, approaching Equations (13) and (14), numerical calculations have been carried out for the determination of geometric mean for row values and the most important attributes. Then, Equations (15) and (16) have been used to analyze defuzzified data and convert them to normalized weights, accordingly.

**Table 2.** Trapezoidal fuzzy pair-wise comparison matrix at level 1.

	CSA1	CSA2	CSA3	CSA4	CSA5	CSA6	CSA7	CSA8
CSA1	1.00000, 1.00000, 1.00000, 1.00000	0.02440, 0.07540, 0.23620, 0.88810	0.01402, 0.04390, 0.12750, 0.46970	0.01270, 0.03480, 0.09340, 0.34300	0.00930, 0.03480, 0.08710, 0.29360	0.00440, 0.01710, 0.06610, 0.21010	0.00068, 0.03405, 0.12320, 0.33240	0.01009, 0.04701, 0.15506, 0.16903
CSA2	-	1.00000, 1.00000, 1.00000, 1.00000	0.02607, 0.06102, 0.36090, 0.69100	0.30090, 0.41403, 0.89800, 1.54501	0.13082, 0.23080, 0.63051, 0.69100	0.06600, 0.12400, 0.40300, 0.49010	0.1340, 0.2570, 0.5810, 0.8400	0.00303, 0.01094, 0.13072, 0.74060
CSA3	-	-	1.00000, 1.00000, 1.00000, 1.00000	0.20400, 0.29100, 0.53500, 1.00000	0.00500, 0.02109, 0.12604, 0.88801	0.14100, 0.29100, 0.37100, 0.68700	0.00200, 0.01208, 0.04703, 0.32027	0.00016, 0.00093, 0.09052, 0.43061
CSA4	-	-	-	1.00000, 1.00000, 1.00000, 1.00000	0.20040, 0.29010, 0.53500, 1.00000	0.00500, 0.02190, 0.12604, 0.88081	0.14100, 0.29010, 0.37010, 0.68070	0.00200, 0.01208, 0.04703, 0.32207
CSA5	-	-	-	-	1.00000, 1.00000, 1.00000, 1.00000	0.08030, 0.20100, 0.37100, 0.47600	0.00102, 0.00808, 0.04703, 0.22306	0.00004, 0.00301, 0.01701, 0.11703
CSA6	-	-	-	-	-	1.00000, 1.00000, 1.00000, 1.00000	0.03050, 0.08800, 0.18300, 0.34200	0.00101, 0.00600, 0.02905, 0.23102
CSA7	-	-	-	-	-	-	1.00000, 1.00000, 1.00000, 1.00000	0.08600, 0.17200, 0.31060, 0.67040
CSA8	-	-	-	-	-	-	-	1.00000, 1.00000, 1.00000, 1.00000

**Table 3.** Defuzzification and normalized weights.

	CSA1	CSA2	CSA3	CSA4	CSA5	CSA6	CSA7	CSA8	Normalized Weights
CSA1	1.00000	0.29255	0.98708	0.38203	0.64130	0.24960	0.99330	0.19990	0.052354
CSA2	3.41822	1.00000	0.16210	0.16220	0.13920	0.19340	0.19220	0.39350	0.038937
CSA3	1.55933	7.18391	3.88651	1.07949	1.00000	0.71272	0.12028	0.91150	0.10973
CSA4	2.6176	6.16523	8.96861	1.00000	0.92636	0.10224	0.35211	0.76270	0.122505
CSA5	5.0025	2.5413	2.03004	1.31113	1.09709	0.99949	0.81552	1.00000	0.127306
CSA6	1.00675	5.20291	2.94811	2.84002	8.31393	0.99481	1.00000	1.22621	0.222015
CSA7	1.01309	6.16903	1.00000	0.11150	0.25730	0.11120	0.33920	0.49260	0.053217
CSA8	4.00641	5.17063	8.99281	9.78091	1.40308	1.00000	1.00522	1.00051	0.273937
C.R. = 0.03485540									

Hereafter, this part of the work presents a realistic assessment of the evaluated results on highly sensitive ML-based intrusion detection systems of Indian hospitals. After obtaining the defuzzified and normalized weights of attributes using an AHP approach under HF conditions, the global ranking of competing alternatives was generated using TOPSIS

under HF conditions. Next, we took the inputs on the technological data of 10 ML-based intrusion detection systems, and the summarized results shown in Table 4 were calculated by incorporating the standard scale specified in the Methodology sub-section in point\_10 and Equation (17). The attributes' weights that were obtained by AHP are provided to the TOPSIS method under HF conditions to achieve the ranking order for the alternatives. The normalized fuzzy decision-matrix for 8 attributes and 10 competitive alternatives was determined through some intermediary operations by incorporating point 10 and Equation (18) and is depicted in Table 5. By incorporating Equations (19) and (22), the normalized fuzzy decision-matrix cell values (performance-values) are multiplied by each attribute weight value, yielding a weighted fuzzy normalized decision-matrix, as shown in Table 6. The final findings are given in Table 7 under the column names dist+ and dist-, which were calculated by incorporating Equations (22) and (23) to determine positive and negative idealness of each option with regard to each characteristic. Then, by incorporating Equations (25) and (26), the relative closeness score for each choice was calculated as the CC-i satisfaction degree, and the results are given in Table 7.

**Table 4.** Subjective cognition results of evaluators in linguistic terms.

Attributes (SDA/Alternatives)	IDS-1	IDS-2	IDS-3	IDS-4	IDS-5	IDS-6	IDS-7	IDS-8	IDS-9	IDS-10
CSA1	3.25100,	3.15400,	2.82200,	1.55000,	1.46500,	2.54679,	2.91100,	1.45000,	1.18400,	2.09645,
	5.12100,	5.15400,	4.62400,	3.18000,	3.18500,	4.26458,	4.64100,	3.00000,	2.84200,	3.73200,
	7.14100,	6.91400,	6.64200,	5.18000,	5.18200,	6.22156,	6.00111,	4.91500,	4.84200,	5.74300,
	8.71200	7.74200	8.72200	6.72000	7.72400	8.64444	6.41500	5.43500	6.45400	6.45900
CSA2	4.21800,	2.45400,	2.91200,	1.45000,	1.18100,	2.15469,	3.18100,	1.45400,	0.82400,	3.01640,
	5.31700,	4.45400,	4.64200,	3.00000,	2.81200,	3.75467,	5.12800,	3.07200,	2.27400,	4.82300,
	6.31700,	6.45400,	6.00200,	4.91000,	4.82200,	5.73124,	7.10225,	4.91400,	4.27400,	6.82300,
	7.71200	7.44500	6.42500	5.45000	6.45200	6.45467	8.65200	5.62500	6.65400	7.65400
CSA3	4.21700,	2.84200,	3.18200,	1.45000,	0.82200,	3.31546,	2.45300,	0.94100,	2.45500,	3.91100,
	6.27100,	4.82400,	5.18200,	3.07000,	2.27300,	4.82167,	4.43500,	2.42500,	4.27500,	5.91300,
	8.14100,	5.84200,	7.10220,	4.91000,	4.27300,	6.83125,	6.45300,	4.45100,	6.27500,	7.82200,
	8.71200	6.45400	8.65100	5.65000	6.65300	7.69645	7.65300	5.65200	8.65500	8.65500
CSA4	3.25100,	3.14500,	2.82100,	1.55000,	1.43500,	2.91200,	1.45000,	1.18100,	2.15469,	3.18100,
	5.11200,	5.15400,	4.61400,	3.18000,	3.18300,	4.64200,	3.00000,	2.81200,	3.75467,	5.12800,
	7.14200,	6.94100,	6.64100,	5.18000,	5.18300,	6.00200,	4.91000,	4.82200,	5.73124,	7.10225,
	8.72200	7.72400	8.71200	6.72000	7.72300	6.42500	5.45000	6.45200	6.45467	8.65200
CSA5	4.22800,	2.44500,	2.91100,	1.45000,	1.18400,	3.18200,	1.45000,	0.82200,	3.31546,	2.45300,
	5.32700,	4.45400,	4.64100,	3.00000,	2.84200,	5.18200,	3.07000,	2.27300,	4.82167,	4.43500,
	6.37200,	6.45400,	6.00111,	4.91500,	4.84200,	7.10220,	4.91000,	4.27300,	6.83125,	6.45300,
	7.72200	7.45400	6.41500	5.43500	6.45400	8.65100	5.65000	6.65300	7.69645	7.65300
CSA6	4.27200,	2.82400,	3.18100,	1.45400,	0.82400,	3.01640,	3.18100,	1.45400,	0.82400,	3.01640,
	6.22700,	4.82300,	5.12800,	3.07200,	2.27400,	4.82300,	5.12800,	3.07200,	2.27400,	4.82300,
	8.14200,	5.82300,	7.10225,	4.91400,	4.27400,	6.82300,	7.10225,	4.91400,	4.27400,	6.82300,
	8.73200	6.45300	8.65200	5.62500	6.65400	7.65400	8.65200	5.62500	6.65400	7.65400
CSA7	5.36300,	3.7300,	2.45300,	0.94100,	2.45500,	3.91100,	2.45300,	0.94100,	2.45500,	3.91100,
	6.33600,	5.73300,	4.43500,	2.42500,	4.27500,	5.91300,	4.43500,	2.42500,	4.27500,	5.91300,
	7.12300,	7.55300,	6.45300,	4.45100,	6.27500,	7.82200,	6.45300,	4.45100,	6.27500,	7.82200,
	8.51300	8.65300	7.65300	5.65200	8.65500	8.65500	7.65300	5.65200	8.65500	8.65500
CSA8	4.64300,	3.03000,	2.18300,	2.82400,	1.91500,	2.55700,	2.85464,	1.91000,	1.45000,	1.18000,
	5.64300,	5.00300,	4.09300,	4.64400,	3.74300,	4.45500,	4.64540,	3.73000,	3.00000,	2.82000,
	7.55300,	7.14300,	6.14400,	6.64400,	5.73500,	6.45600,	6.64000,	5.73000,	4.91000,	4.82000,
	8.84300	7.51300	7.51300	8.51400	7.51200	8.51600	8.51000	7.51000	5.45000	6.45000

**Table 5.** The normalized fuzzy-decision matrix.

	IDS-1	IDS-2	IDS-3	IDS-4	IDS-5	IDS-6	IDS-7	IDS-8	IDS-9	IDS-10
CSA1	0.32450,	0.60040,	0.63690,	0.23210,	0.35250,	0.62555,	0.48350,	0.34620,	0.43370,	0.33540,
	0.46580,	0.81200,	0.81660,	0.38210,	0.55620,	0.87250,	0.61599,	0.55230,	0.63630,	0.52540,
	0.55250,	0.85800,	0.58960,	0.54280,	0.62970,	0.93560,	0.70350,	0.66240,	0.73360,	0.61580,
	0.63470	0.96090	0.96670	0.73262	0.84720	0.98590	0.83950	0.81270	0.85830	0.78050
CSA2	0.20040,	0.55440,	0.61160,	0.38020,	0.42210,	0.61520,	0.24520,	0.45220,	0.61310,	0.61250,
	0.32200,	0.84564,	0.77620,	0.57240,	0.65278,	0.85500,	0.39570,	0.66820,	0.77320,	0.85500,
	0.43700,	0.85467,	0.85660,	0.72220,	0.75720,	0.91570,	0.54750,	0.76210,	0.85360,	0.91570,
	0.54700	0.96497	0.94560	0.08220	0.91290	0.96580	0.74530	0.89800	0.94530	0.96850
CSA3	0.23010,	0.37320,	0.57460,	0.24920,	0.24220,	0.45520,	0.46510,	0.27250,	0.57430,	0.34620,
	0.35080,	0.56350,	0.72560,	0.41320,	0.39270,	0.66850,	0.65570,	0.45620,	0.72530,	0.55230,
	0.44070,	0.69330,	0.79260,	0.53220,	0.54270,	0.76150,	0.76550,	0.53320,	0.73920,	0.66240,
	0.57000	0.83350	0.89660	0.74210	0.74230	0.89580	0.90550	0.73230	0.89630	0.81270
CSA4	0.25074,	0.03730,	0.03968,	0.42230,	0.46310,	0.27550,	0.42210,	0.61520,	0.24520,	0.45220,
	0.38070,	0.10350,	0.10555,	0.62490,	0.65370,	0.45560,	0.65278,	0.85500,	0.39570,	0.66820,
	0.43700,	0.24320,	0.19250,	0.76240,	0.76350,	0.53350,	0.75720,	0.91570,	0.54750,	0.76210,
	0.54000	0.51030	0.38450	0.88200	0.90350	0.73530	0.91290	0.96580	0.74530	0.89800
CSA5	0.45090,	0.29430,	0.48350,	0.34620,	0.43370,	0.33540,	0.24220,	0.45520,	0.46510,	0.27250,
	0.61020,	0.43840,	0.61599,	0.55230,	0.63630,	0.52540,	0.39270,	0.66850,	0.65570,	0.45620,
	0.65030,	0.56330,	0.70350,	0.66240,	0.73360,	0.61580,	0.54270,	0.76150,	0.76550,	0.53320,
	0.68080	0.74203	0.83950	0.81270	0.85830	0.78050	0.74230	0.89580	0.90550	0.73230
CSA6	0.30750,	0.24390,	0.24520,	0.45220,	0.61310,	0.42230,	0.46310,	0.27550,	0.42210,	0.61520,
	0.44450,	0.41330,	0.39570,	0.66820,	0.77320,	0.62490,	0.65370,	0.45560,	0.65278,	0.85500,
	0.54457,	0.53320,	0.54750,	0.76210,	0.85360,	0.76240,	0.76350,	0.53350,	0.75720,	0.91570,
	0.64052	0.74310	0.74530	0.89800	0.94530	0.88200	0.90350	0.73530	0.91290	0.96580
CSA7	0.61020,	0.42330,	0.46510,	0.27250,	0.57430,	0.34620,	0.43370,	0.33540,	0.24220,	0.45520,
	0.80500,	0.64390,	0.65570,	0.45620,	0.72530,	0.55230,	0.63630,	0.52540,	0.39270,	0.66850,
	0.91070,	0.76340,	0.76550,	0.53320,	0.73920,	0.66240,	0.73360,	0.61580,	0.54270,	0.76150,
	0.96080	0.88044	0.90550	0.73230	0.89630	0.81270	0.85830	0.78050	0.74230	0.89580
CSA8	0.57400,	0.34560,	0.43570,	0.33240,	0.03980,	0.45220,	0.34650,	0.43750,	0.33540,	0.03580,
	0.72500,	0.55350,	0.63650,	0.52420,	0.10022,	0.66820,	0.55530,	0.63650,	0.52540,	0.10555,
	0.79200,	0.66450,	0.73650,	0.61820,	0.19220,	0.76210,	0.66450,	0.73560,	0.61850,	0.19520,
	0.89060	0.81570	0.85580	0.78200	0.38420	0.89800	0.81570	0.85580	0.78050	0.38450

**Table 6.** The weighted normalized fuzzy-decision matrix.

	IDS-1	IDS-2	IDS-3	IDS-4	IDS-5	IDS-6	IDS-7	IDS-8	IDS-9	IDS-10
CSA1	0.00080,	0.11050,	0.14020,	0.05070,	0.05505,	0.04208,	0.05800,	0.02030,	0.00090,	0.08070,
	0.01020,	0.16070,	0.17900,	0.08500,	0.08070,	0.05900,	0.08050,	0.03700,	0.02300,	0.09040,
	0.01600,	0.18030,	0.19800,	0.10800,	0.10040,	0.06400,	0.09500,	0.04300,	0.04500,	0.09400,
	0.02100	0.19090	0.21090	0.13010	0.12200	0.06800	0.11800	0.05500	0.05900	0.10100
CSA2	0.00807,	0.07074,	0.13300,	0.03701,	0.03020,	0.03020,	0.14800,	0.03404,	0.04070,	0.04304,
	0.01035,	0.11800,	0.16800,	0.06106,	0.05300,	0.04070,	0.18091,	0.05700,	0.07040,	0.05010,
	0.01700,	0.14400,	0.18400,	0.07900,	0.07200,	0.05030,	0.20060,	0.08200,	0.09020,	0.06060,
	0.02100	0.17300	0.20080	0.11000	0.09800	0.06030	0.22040	0.11000	0.11020	0.06090
CSA3	0.01200,	0.12500,	0.14080,	0.03404,	0.04700,	0.04304,	0.14200,	0.05700,	0.05055,	0.04028,
	0.01800,	0.16090,	0.18091,	0.05700,	0.07400,	0.05100,	0.17090,	0.08500,	0.08070,	0.05900,
	0.02100,	0.18050,	0.20060,	0.08200,	0.09020,	0.06060,	0.19800,	0.10800,	0.10040,	0.06400,
	0.02040	0.20010	0.22040	0.11000	0.11020	0.06090	0.21090	0.13100	0.12020	0.06800
CSA4	0.00080,	0.11500,	0.14200,	0.05700,	0.05505,	0.04208,	0.13030,	0.03701,	0.03200,	0.03020,
	0.01200,	0.16070,	0.17090,	0.08500,	0.08700,	0.05900,	0.16080,	0.06106,	0.05300,	0.04700,
	0.01600,	0.18030,	0.19080,	0.10080,	0.10400,	0.06400,	0.18400,	0.07900,	0.07200,	0.05300,
	0.02010	0.19090	0.21900	0.13010	0.12020	0.06080	0.20080	0.11000	0.09800	0.06300

Table 6. Cont.

	IDS-1	IDS-2	IDS-3	IDS-4	IDS-5	IDS-6	IDS-7	IDS-8	IDS-9	IDS-10
CSA5	0.00807, 0.01305, 0.01070, 0.02100	0.07704, 0.11800, 0.14400, 0.17300	0.13300, 0.16800, 0.18400, 0.20080	0.03701, 0.06016, 0.07090, 0.11000	0.03200, 0.05300, 0.07020, 0.09800	0.03200, 0.04700, 0.05300, 0.06300	0.00090, 0.02030, 0.04050, 0.05090	0.06300, 0.09709, 0.11400, 0.13100	0.06010, 0.08700, 0.10100, 0.12000	0.01900, 0.03025, 0.03800, 0.05100
CSA6	0.01000, 0.01500, 0.01011, 0.02000	0.00800, 0.02204, 0.05002, 0.10000	0.00900, 0.02300, 0.04500, 0.05090	0.06300, 0.09709, 0.11400, 0.13100	0.06010, 0.08070, 0.10010, 0.12000	0.01900, 0.03205, 0.03800, 0.05010	0.11200, 0.14040, 0.16030, 0.19050	0.05160, 0.08200, 0.09900, 0.12200	0.05800, 0.08050, 0.09500, 0.11080	0.02300, 0.03700, 0.04300, 0.05500
CSA7	0.01073, 0.02033, 0.02500, 0.02700	0.06101, 0.10100, 0.11070, 0.15400	0.11020, 0.14040, 0.16030, 0.19050	0.05016, 0.08020, 0.09900, 0.12200	0.05080, 0.08050, 0.09050, 0.11800	0.02300, 0.03700, 0.04300, 0.05500	0.14200, 0.17090, 0.19080, 0.21090	0.05700, 0.08500, 0.10800, 0.13100	0.05505, 0.08070, 0.10400, 0.12200	0.04208, 0.05900, 0.06400, 0.06800
CSA8	0.08504, 0.09030, 0.09300, 0.09086	0.03701, 0.06016, 0.07090, 0.11000	0.03200, 0.05030, 0.07200, 0.09080	0.03020, 0.04700, 0.05030, 0.06030	0.14020, 0.17090, 0.19080, 0.21900	0.03200, 0.04700, 0.05300, 0.06300	0.13300, 0.16800, 0.18400, 0.20080	0.03701, 0.06106, 0.07900, 0.11000	0.03200, 0.05300, 0.07200, 0.09800	0.03200, 0.04700, 0.05300, 0.06300

Table 7. Closeness coefficients to aspired level among different alternatives.

Alternatives	Dist+	Dist−	Gaps Degree of CC <sup>+i</sup>	Satisfaction Degree of CC <sup>−i</sup>	Alternative Ranks
IDS-1	0.338458	0.589857	0.655256	0.358566	9
IDS-2	0.035659	0.047455	0.640454	0.355475	10
IDS-3	0.035659	0.043458	0.535425	0.464597	7
IDS-4	0.039457	0.046855	0.535635	0.465465	6
IDS-5	0.035459	0.042857	0.583459	0.484545	5
IDS-6	0.045566	0.025855	0.366855	0.635660	1
IDS-7	0.035485	0.035555	0.469457	0.525646	4
IDS-8	0.044455	0.026460	0.394564	0.615453	2
IDS-9	0.035549	0.026457	0.483546	0.575626	3
IDS-10	0.298855	0.445685	0.586599	0.455696	8

The final analysis of the numerical results depicts that, on the basis of the performance scores, the competitive alternative rankings (10 ML-based intrusion detection systems) is generated as: IDS-6, IDS-8, IDS-9, IDS-7, IDS-5, IDS-4, IDS-3, IDS-10, IDS-1, and IDS-2 in an idealness assessment concerning ML-based cybersecurity. On the basis of chosen criteria, the idealness evaluation performed on 10 different ML-based intrusion detection systems revealed that IDS-6 is more ideal and effective in addressing serious cybersecurity concerns and difficulties. Furthermore, using a TOPSIS approach under HF conditions, the identified attributes for the idealness assessment of ML-based intrusion detection systems have been prioritized in the following order: accuracy, anomaly detection, misuse detection, DoS attack detection, malware detection, implementation complexity, spam detection, and phishing detection with the global normalized weights 0.273937, 0.222015, 0.127306, 0.122505, 0.10973, 0.053217, 0.052354, and 0.038937, respectively.

In addition to this, the applicability of our proposed work is not null. We have considered 10 real-time intrusion detection systems from different hospitals of India as alternatives. As, revealed from existing relevant research works, the alternative selection for assessment is an integral part of our proposed methodology [8–17]. The alternative selection is a result of collective decision of domain experts and owners of intrusion detection systems for this case study. Further, the above examined quantitative results reveal that the IDS-6 have acquired a maximum number of the attributes among the



identified attribute set for this work. Due to its hybrid characteristic, it integrates different machine learning algorithms for the detection of different kinds of cyber-security attacks that are the concern of our study. In the same way, the other intrusion detection systems, namely IDS-8, IDS-9, IDS-7, etc., gain less performance score in descending order with respect to the identified attributes and the domain of their detection of identified cyber-security attacks.

## 6. Discussion

Cybersecurity ensures real-time protection of information, information systems, and networks from intruders. There has been an immense increase in cybersecurity breaches over the last decade, and instances of data theft continue to rise by the day. To address these cybersecurity issues, organizations have spent huge amounts and various efforts to overcome these intrusions are already underway. Different approaches and techniques have been practiced by experts and researchers to provide reliable and robust security mechanisms. One of the most prominent among them is machine learning, which plays a vital role in the cybersecurity domain [24]. ML has a proactive character that can address cybersecurity issues effectively and examine the threats and respond to intrusions and security incidents swiftly in an instinctive way [24]. Thus, this makes the ML techniques more suitable for detecting and classifying various kinds of cyber-attacks. More specifically, supervised and unsupervised machine learning techniques possess a great ability to address different cybersecurity issues [23]. In this row, cybersecurity experts and researchers have proposed and designed various intrusion detection systems to detect different kinds of cybersecurity attacks [6]. As stated, the main objective of this work was to make an idealness assessment of intrusion detection systems through integrated hesitant fuzzy based AHP-TOPSIS approaches. Experts' views and current relevant research findings were used to identify and choose the attributes that were included in this evaluation. AHP under HF conditions results reveal that the accuracy attribute has gained the top priority, followed by anomaly detection, misuse detection, DoS attack detection, malware detection, implementation complexity, spam detection, and phishing detection. TOPSIS under HF conditions depicts that IDS-6 has gained the highest ranking, while the IDS-2 gains the least ranking with a performance score of 0.355475 computed with respect to ML concerned cybersecurity attributes. The findings demonstrate that IDS-6 is more ideal and trustworthy cybersecurity than the security offered by the other nine alternatives. This research will aid in the development of safe and reliable intrusion detection systems, as well as ML-based cybersecurity attribute analyses.

According to the study's findings, intrusion detection system IDS-6 best meets the ML-based cyber security attributes that were used to evaluate the idealness of intrusion detection systems from a ML-based cybersecurity perspective. With a performance score of 0.635660, it was determined to be the best in terms of delivering an ideal and trustworthy ML-based cybersecurity mechanism against potential threats. The main observations and results of the study are concluded in the following points.

- In this research experiment, the ML-based cybersecurity attributes are prioritized in this sequential order: accuracy, anomaly detection, misuse detection, DoS attack detection, malware detection, implementation complexity, spam detection, and phishing detection, having the global normalized weights 0.273937, 0.222015, 0.127306, 0.122505, 0.10973, 0.053217, 0.052354, and 0.038937, respectively.
- After IDS-6, the following competing alternatives are ranked in order based on their produced performance scores: IDS-8, IDS-9, IDS-7, IDS-5, IDS-4, IDS-3, IDS-10, IDS-1, and IDS-2 in terms of identified weighted ML-based cybersecurity attributes.
- ML-based cybersecurity provided by intrusion detection systems is a challenging issue, and in this league, our study offers accurate recommendations for developing ideal and effective machine learning-based intrusion detection systems.
- This study was performed specifically for the intrusion detection systems deployed in healthcare environments. However, it may be used as a guideline for building any sort

of ideal and effective intrusion detection systems, because the assessment attributes are identified on the basis of generalization.

## 7. Conclusions

The findings of this research reveal that cyber security issues and breaches have been a tough challenge to researchers and security experts for the last few years. The experts and the researchers have used a variety of methodologies and strategies to develop trustworthy and effective security systems. Machine learning is one of the most famous ones, and it plays a crucial role in the cybersecurity sphere. In this league, we analyzed the impact of cyber security related attributes for intrusion detection systems through hesitant fuzzy-based AHP-TOPSIS. This methodology will help the researchers and the developers to prioritize the cyber security attributes accordingly and develop more secure and reliable intrusion detection systems. However, research is both a dynamic and continuous activity. As a result, while our ML-based cybersecurity evaluation is accurate, it cannot contend for the optimality of outcomes. There are additional MCDM approaches that may be utilized to provide more efficient outcomes. Nonetheless, our empirical findings show that we have selected a reliable method for this evaluation.

**Author Contributions:** All authors have contributed equally to the manuscript. All authors have read and agreed to the published version of the manuscript.

**Funding:** The project has been funded by Taif University, Kingdom of Saudi Arabia.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** The data presented in this study are available on request from the corresponding author. The data are not publicly available due to security and privacy issues.

**Acknowledgments:** This research was supported by Taif University Researchers Supporting Project number (TURSP-2020/231), Taif University, Taif, Saudi Arabia.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

- Samuel, A.L. Some Studies in Machine Learning Using the Game of Checkers. *IBM J. Res. Dev.* **1959**, *3*, 210–229. [\[CrossRef\]](#)
- Mitchell, T.M. *Machine Learning*; McGraw-Hill: New York, NY, USA, 1997; pp. 386–387.
- Jordan, M.I.; Mitchell, T.M. Machine learning: Trends, perspectives, and prospects. *Science* **2015**, *349*, 255–260. [\[CrossRef\]](#) [\[PubMed\]](#)
- Harrington, P. *Machine Learning in Action*; Simon and Schuster: New York, NY, USA, 2012.
- Dua, S.; Du, X. *Data Mining and Machine Learning in Cybersecurity*; CRC Press: New York, NY, USA, 2016.
- Tsai, C.-F.; Hsu, Y.-F.; Lin, C.-Y.; Lin, W.-Y. Intrusion detection by machine learning: A review. *Expert Syst. Appl.* **2009**, *36*, 11994–12000. [\[CrossRef\]](#)
- Belavagi, M.C.; Muniyal, B. Performance Evaluation of Supervised Machine Learning Algorithms for Intrusion Detection. *Procedia Comput. Sci.* **2016**, *89*, 117–123. [\[CrossRef\]](#)
- Agrawal, A.; Seh, A.H.; Baz, A.; AlHakami, H.; AlHakami, W.; Baz, M.; Kumar, R.; Khan, R.A. Software Security Estimation Using the Hybrid Fuzzy ANP-TOPSIS Approach: Design Tactics Perspective. *Symmetry* **2020**, *12*, 598. [\[CrossRef\]](#)
- Kumar, R.; Khan, A.I.; Abushark, Y.B.; ALAM, M.; Agrawal, A.; Khan, R.A. An Integrated Approach of Fuzzy Logic, AHP and TOPSIS for Estimating Usable-Security of Web Applications. *IEEE Access* **2020**, *8*, 50944–50957. [\[CrossRef\]](#)
- Solangi, Y.A.; Tan, Q.; Mirjat, N.H.; Das Valasai, G.; Khan, M.W.A.; Ikram, M. An integrated Delphi-AHP and fuzzy TOPSIS approach toward ranking and selection of renewable energy resources in Pakistan. *Processes* **2019**, *7*, 118. [\[CrossRef\]](#)
- Kumar, R.; Baz, A.; Alhakami, H.; Alhakami, W.; Baz, M.; Agrawal, A.; Khan, R.A. A Hybrid Model of Hesitant Fuzzy Decision-Making Analysis for Estimating Usable-Security of Software. *IEEE Access* **2020**, *8*, 72694–72712. [\[CrossRef\]](#)
- Alharbe, N. A fuzzy-Delphi based decision-making process for measuring usable-security of Web based smart hospital management system. *ICIC Express Lett.* **2020**, *14*, 15–21.
- Şengül, U.; Eren, M.; Shiraz, S.E.; Gezder, V.; Şengül, A.B. Fuzzy TOPSIS method for ranking renewable energy supply systems in Turkey. *Renew. Energy* **2015**, *75*, 617–625. [\[CrossRef\]](#)
- Qian, G.; Wang, H.; Feng, X. Generalized hesitant fuzzy sets and their application in decision support system. *Knowl. Based Syst.* **2013**, *37*, 357–365. [\[CrossRef\]](#)

15. Sahu, K.; Alzahrani, F.A.; Srivastava, R.K.; Kumar, R. Hesitant Fuzzy Sets Based Symmetrical Model of Decision-Making for Estimating the Durability of Web Application. *Symmetry* **2020**, *12*, 1770. [[CrossRef](#)]
16. Torra, V.; Narukawa, Y. On hesitant fuzzy sets and decision. In Proceedings of the 2009 IEEE International Conference on Fuzzy Systems, Jeju, Korea, 20–24 August 2009; pp. 1378–1382.
17. AlMotiri, S.H. Integrated Fuzzy Based Computational Mechanism for the Selection of Effective Malicious Traffic Detection Approach. *IEEE Access* **2021**, *9*, 10751–10764. [[CrossRef](#)]
18. Bekesiene, S.; Vasiliauskas, A.V.; Hošková-Mayerová, Š.; Vasilienė-Vasiliauskienė, V. Comprehensive Assessment of Distance Learning Modules by Fuzzy AHP-TOPSIS Method. *Mathematics* **2021**, *9*, 409. [[CrossRef](#)]
19. Kaur, J.; Khan, A.I.; Abushark, Y.B.; Alam, M.; Khan, S.A.; Agrawal, A.; Kumar, R.; Khan, R.A. Security risk assessment of healthcare Web application through adaptive neuro-fuzzy inference system: A design perspective. *Risk Manag. Healthc. Policy* **2020**, *13*, 355–371. [[CrossRef](#)]
20. Goutam, A.; Tiwari, V. Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application. In Proceedings of the 2019 4th International Conference on Information Systems and Computer Networks (ISCON), Mathura, India, 21–22 November 2019; pp. 601–605.
21. Büyükköçkan, G.; Çifçi, G. A combined fuzzy AHP and fuzzy TOPSIS based strategic analysis of electronic service quality in healthcare industry. *Expert Syst. Appl.* **2012**, *39*, 2341–2354. [[CrossRef](#)]
22. Handa, A.; Sharma, A.; Shukla, S.K. Machine learning in cybersecurity: A review. *Wiley Interdiscip. Rev. Data Min. Knowl. Discov.* **2019**, *9*, 1306. [[CrossRef](#)]
23. Dasgupta, D.; Akhtar, Z.; Sen, S. Machine learning in cybersecurity: A comprehensive survey. *J. Def. Model. Simul. Appl. Methodol. Technol.* **2020**, *154*, 8. [[CrossRef](#)]
24. Thomas, T.; Vijayaraghavan, A.P.; Emmanuel, S. *Machine Learning Approaches in Cyber Security Analytics*; Springer: New York, NY, USA, 2020; pp. 37–200.
25. Crawford, M.; Khoshgoftaar, T.M.; Prusa, J.D.; Richter, A.N.; Al Najada, H. Survey of review spam detection using machine learning techniques. *J. Big Data* **2015**, *2*, 23. [[CrossRef](#)]
26. Forouzan, A.B. *Data Communications Networking*, 3rd ed.; Tata McGraw-Hill Education: New York, NY, USA, 2007.
27. Seh, A.H.; Al-Amri, J.F.; Subahi, A.F.; Agrawal, A.; Kumar, R.; Khan, R.A. Machine Learning Based Framework for Maintaining Privacy of Healthcare Data. *Intell. Autom. Soft Comput.* **2021**, *29*, 697–712. [[CrossRef](#)]
28. Sahu, K.; Alzahrani, F.A.; Srivastava, R.K.; Kumar, R. Evaluating the Impact of Prediction Techniques: Software Reliability Perspective. *Comput. Mater. Contin.* **2021**, *67*, 1471–1488. [[CrossRef](#)]
29. Agrawal, A.; Alenezi, M.; Khan, S.A.; Kumar, R.; Khan, R.A. Multi-Level Fuzzy system for usable-Security assessment. *J. King Saud Univ. Comput. Inf. Sci.* **2019**, 1–21. [[CrossRef](#)]