Computers, Materials & Continua
DOI: 10.32604/cmc.2022.025604
Article

Tech Science Press

Cyber Security Analysis and Evaluation for Intrusion Detection Systems

Yoosef B. Abushark[1], Asif Irshad Khan[1,*], Fawaz Alsolami[1], Abdulmohsen Almalawi[1], Md Mottahir Alam[2], Alka Agrawal[3], Rajeev Kumar[4] and Raees Ahmad Khan[3]

[1]Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Department of Electrical and Computer Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[3]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, Uttar Pradesh, India
[4]Department of Computer Science and Engineering, Babu Banarasi Das University, Lucknow, 226028, India
*Corresponding Author: Asif Irshad Khan. Email: aikhan@kau.edu.sa
Received: 29 November 2021; Accepted: 11 January 2022

Abstract: Machine learning is a technique that is widely employed in both the academic and industrial sectors all over the world. Machine learning algorithms that are intuitive can analyse risks and respond swiftly to breaches and security issues. It is crucial in offering a proactive security system in the field of cybersecurity. In real time, cybersecurity protects information, information systems, and networks from intruders. In the recent decade, several assessments on security and privacy estimates have noted a rapid growth in both the incidence and quantity of cybersecurity breaches. At an increasing rate, intruders are breaching information security. Anomaly detection, software vulnerability diagnosis, phishing page identification, denial of service assaults, and malware identification are the foremost cyber-security concerns that require efficient clarifications. Practitioners have tried a variety of approaches to address the present cybersecurity obstacles and concerns. In a similar vein, the goal of this research is to assess the idealness of machine learning-based intrusion detection systems under fuzzy conditions using a Multi-Criteria Decision Making (MCDM)-based Analytical Hierarchy Process (AHP) and a Technique for Order of Preference by Similarity to Ideal-Solutions (TOPSIS). Fuzzy sets are ideal for dealing with decision-making scenarios in which experts are unsure of the best course of action. The projected work would support practitioners in identifying, prioritising, and selecting cybersecurity-related attributes for intrusion detection systems, allowing them to design more optimal and effective intrusion detection systems.

Keywords: Cybersecurity; machine learning; AHP-TOPSIS; fuzzy logic; intrusion detection systems

1 Introduction

The expansion of Information and Communications Technology (ICT) is one of the most evident trends in today's globe. During the previous few decades, the technological revolution has had a major impact on the world, changing people's thinking and behaviours. One of the most prominent and well-known technologies in this industry is machine learning. Machine learning was first established as a sub-domain of artificial intelligence by Arthur Samuel in 1959 [1,2]. Succeeding that, machine learning tactics became broadly employed in a variety of fields, and it is now recognised as one of the most important and rapidly evolving technologies, particularly for addressing issues such as future event prediction, disease diagnosis, market analysis, email filtering, intrusion detection, image and speech recognition, and so on [3]. Machine learning algorithms may learn from both structured and unstructured data, and they can assist in the automation of systems in a variety of scenarios. Machine learning allows algorithms to learn from earlier (historical) data. We all know that data is at the centre of the digital world. Scientists and researchers in this scenario use data mining and machine learning techniques to extract new and helpful insights from the data.

There are several interesting patterns in the existing data that can help us forecast future events, both normal and aberrant. The data is initially delivered as a dataset as input to the developed machine learning frameworks, which then train themselves accordingly. These machine learning-based frameworks learn from the data and enhance their performance as an outcome of machine learning algorithms. The suggested framework must be evaluated and verified with new yet relevant data after the training phase is completed in order to determine its efficiency and accuracy. It would thus be able to use learning behaviour to predict future occurrences and activities with minimal human participation and explicit programming [4]. The input data programme improves its performance measure with each accurate judgement. A computer programme is said to learn from experience with regard to some class of tasks T and a performance measure P if its performance at tasks in T, as measured by P, improves with experience [2]. The main focus is on these three things: a collection of tasks defined by T; performance estimation denoted by P; and E, which represents the program's source of experience.

In recent years, machine learning has acquired a lot of traction in the field of cyber security [5]. In general, supervised and unsupervised machine learning approaches are two popular types of machine learning that researchers utilise to design and build small intrusion detection systems [6]. Intrusion detection systems detect many sorts of intrusions and provide proactive security solutions. As the name implies, supervised machine learning-based intrusion detection systems operate in a supervised environment [7]. It employs labelled historical data to train and test the frameworks it develops. Frameworks are built using supervised machine learning algorithms that map given inputs to outputs based on prior information [8]. It infers an input object's output class based on information gleaned from tagged samples of training data. In most cases, the input object is a vector of characteristics from the most perfect class with which it shares common traits. Unsupervised machine learning is a contrastive study against supervised machine learning in which unsupervised machine learning algorithms are implemented to build intrusion detection systems. In supervised machine learning, frameworks are completely subjected to labelled data and the efficiency and accuracy of frameworks are directly proportional to the quality of data.

In contrast, unsupervised machine learning is a contrastive study against supervised machine learning, in which the efficiency and accuracy of frameworks are directly proportional to the quality of data. Frameworks are purely autonomous in their ability to compress internal representations of the given data based on their common traits [2], and the data is completely unlabeled in this context.

Unsupervised machine learning frameworks analyse data, and significant insights are discovered from this data, which is then employed to categorise future data. Deep insights into several real-life domains are provided by machine learning, and cybersecurity is one of them. Malware training data sets, spam identification data sets, intuition detention data sets, unified host and network datasets, malicious Uniform Resource Locators (URLs), and other cybersecurity datasets must be utilised to train machine learning-based frameworks, which will then be employed to detect future cyber security risks. Considering the idealness and prioritisation of the ideal features at the first stages of intrusion, however, detection system development has become a difficult and fascinating subject for cybersecurity specialists and researchers. Characteristic prioritisation and identification is a decision-making problem that necessitates the input of specialists and extensive investigation [8]. Furthermore, testing the proactive security preparation, efficacy, and accuracy of software security systems is a continual process that must be undertaken by specialists on a regular basis [9].

As an outcome, the goal of this study is to examine the impact of cyber security qualities on intrusion detection systems and to use MCDM tactics to assess the idealness of machine learning-based intrusion detection systems owned by Indian hospitals under fuzzy settings. The experts' opinions are employed to identify and choose the relevant characteristics for this estimation. In the context of machine learning-based intrusion detection systems, this idealness estimation will assist researchers and cybersecurity experts in identifying and prioritising the ideal cybersecurity qualities. Aside from that, the findings of the study will aid in the development of more reliable and optimal intrusion detection systems. Researchers have employed MCDM tactics in a number of studies for numerous project estimations and estimations. However, we were unable to locate any research that employed fuzzy-based MCDM tactics to analyse the idealness of intrusion detection systems. As an outcome, the purpose of this research is to develop a novel approach to evaluate machine learning-based intrusion detection systems under fuzzy conditions by employing AHP-TOPSIS approaches.

When it comes to handling hierarchical decision-making difficulties, AHP, an MCDM tactic, has a lot of promise. T L Saaty first offered the recommended approach in 1990 [9]. Since then, the approach has seen significant refinements. It provides a mechanism for computing the weight of criteria that is simple to use (characteristics). Rather than just assigning a value, they specialise in arriving at the optimum decision for their aim and understanding of the issue [10]. In addition, including fuzzy in this approach improves its efficiency and leads to more accurate outcomes [11]. When making a decision in AHP, experts frequently suffer hesitancy and are unable to agree on a single value because they desire to go beyond or below the values. These values, on the other hand, are inaccessible [12,13]. The fuzzy sets play a significant role in this scenario. Reluctant fuzzy sets are employed to reflect decision-makers' preferences. When establishing an element's membership in a fixed set is difficult, fuzzy logic can be employed to reduce uncertainty that may develop during the decision-making process. Conventional fuzzy logic [14] is insufficient to address such situations. The fuzzy collection has gotten a lot of attention from scholars both at home and abroad since its debut. Furthermore, the TOPSIS tactic is well-known for its capacity to generate the most alternative rankings imaginable [8]. As a consequence, combining fuzzy logic with the AHP-TOPSIS tactic increases the study's efficiency and qualifies it for evaluating the effectiveness of machine learning-based intrusion detection systems.

AHP-TOPSIS is capable of solving MCDM problems with imprecise and uncertain data [13,14]. AHP gives more accurate characteristic weights in fuzzy situations, outcomeing in more effective outcomes [15,16]. TOPSIS under fuzzy conditions [13] is a more well-known tactic for ranking choices in MCDM problem resolution. This study uses eight cybersecurity elements as criteria, with ten machine learning-based intrusion detection systems as alternatives. Expert opinions and well-known research studies are employed to identify and select the qualities. Our research team engaged

domain specialists in this case. Our team has also conducted a number of research studies utilising numerous MCDM tactics. The experts selected and determined the appropriate characteristic sets for the described problem that required being solved using MCDM tactics based on their knowledge and experience in this domain. After consulting with domain experts (characteristic set), we were able to reduce redundancy, inconsistency, and ambiguity from the data.

The study has also been broken down into the succeeding sections: The second section examines previous studies that are relevant. Section 3 describes the framework of cybersecurity characteristics related to machine learning-based intrusion detection systems; Section 4 elaborates on the tactic employed; Section 5 describes the mathematical calculations and outcomes; Section 6 incorporates the discussion; and Section 7 concludes the research.

2 Machine Learning in Cybersecurity

Machine learning, being a new technology, provides a lot of flexibility when it comes to extracting insights from enormous volumes of data. This, in turn, helps in analysing massive amounts of data and uncovering interesting patterns [17,18]. Machine learning provides huge benefits to current industries and commercial organisations by gaining insights from previous data. Furthermore, one of the intriguing features of machine learning approaches is that they provide proactive security measures in the realm of cybersecurity [19]. Intuition detection systems based on machine learning are an effective security strategy for tackling cybersecurity challenges, examining risks, and responding instinctively to intrusions and security incidents. Different machine learning tactics have been employed by cybersecurity experts and researchers to address numerous cybersecurity concerns [20,21]. Decision trees, support vector machines, nave Bayes classifier, artificial neural networks, k-means clustering, convolutional neural networks, k-nearest neighbour, recurrent neural networks, restricted Boltzmann machines, and fuzzy c-means clustering are the most commonly employed machine learning algorithms for designing and developing intrusion detection systems [22,23]. Researchers employ these algorithms to address cybersecurity challenges in a variety of working contexts. However, the goal of this study is to evaluate the idealness of these machine learning-based intrusion detection systems in terms of their stated cybersecurity qualities.

A case study was carried out on ten machine learning-based intrusion detection systems installed in hospitals in Uttar Pradesh, India. The identification and selection of characteristics for evaluating machine learning algorithms is a collaborative choice based on the authors' expert perspectives and experience. For this study, eight cybersecurity characteristics related to machine learning were investigated, along with ten potential options for assessing the idealness of intrusion detection systems. A−1, A−2, A-3, A-4, A-5, A-6, A-7, and A-8, are the 8 options (intrusion detection systems). The alternative selection procedure is the outcome of a group decision made by domain experts and owners of intrusion detection systems from several Indian hospitals for a comparative cyber-security estimation. The 10 selected intrusion detection systems have been installed in numerous hospitals for the detection of numerous cyber-security assaults. Different machine learning tactics were applied in these detection systems, ranging from basic to complicated levels of integration and hybridization. To detect different sorts of threats, each A employs multiple machine learning algorithms. Furthermore, each intrusion detection system has been assigned a value between 0 and 1 for each of the detected characteristics, as the study's authors employed fuzzy logic to make this determination. Furthermore, evaluators' subjective cognition outcomes in language words for each intrusion detection system are based on the scale and expert opinion stated in the tactic section. The process of estimation and quantitative outcomes for the 10 distinct intrusion detection systems have been reported in Section 5

of this study based on the identified characteristic set. The detected features and options are depicted in Fig. 1. In the diagram below, the subsection descriptions and relevance of the identified features are discussed.

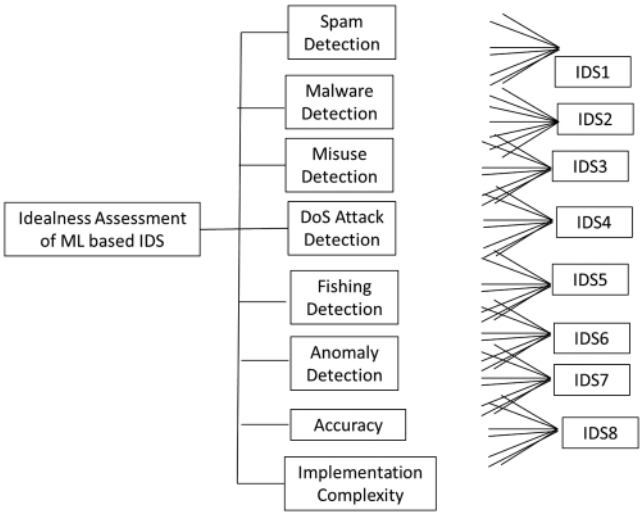

Figure 1: A characteristic tree that evaluates the idealness of machine learning-based intrusion detection systems

• Spam Detection: Spam detection is a key aspect of machine learning-based intrusion detection systems, which are employed to detect spam. Spam is a technical term for unsolicited mass mail that is largely connected to electronic messages. It is also known by other names, such as junk mail. Spammers employ several communications platforms to distribute unwanted and undesirable digital content [15]. It usually manifests itself in the form of unwelcome and needless emails sent via the internet. Spams are frequently employed for commercial objectives and are generally unappealing. Spam messages, on the other hand, can be disastrous for both the system and the user. Spammers' goal in this situation is to send malicious code, carry out phishing scams, and make money.

• Phishing Identification: Cyber intrusions are fairly common these days, and their prevalence has increased dramatically. Intruders utilise phishing as one of the most popular and fascinating social engineering attacks to steal personal data. Credit card numbers and login credentials are frequently included in the targeted data. Cyber fraudsters employ the notion of spoofing in phishing to impersonate a reputable and well-known source to the victim [14]. They mostly use it to impersonate reputable organisations' websites so that victims can readily trust and disclose their personal information. Phishing attacks are also employed to spread malware that steals system cookies and records keystrokes. As an outcome, detecting phishing assaults has become one of the key capabilities of machine learning-based intrusion detection systems.

• Malware Identification: Malware is a term employed to describe a collection of harmful software that includes viruses, spyware, keyloggers, and ransomware. Malware is a type of computer code created by cyber-criminals with the goal of causing significant damage to the victim's system or gaining unauthorised network access. In general, it is a coded file that is distributed by cyber-criminals over numerous communications tactics, such as e-mail, and needs the victim to run the virus. Intruders create several forms of malware programmes for numerous goals, and they are frequently employed to compromise the financial data of businesses and organisations [14]. Researchers have developed

machine learning tactics for both malware detection and classification into multiple classes or families. As an outcome, one of the important aspects of machine learning-based intrusion detection systems is the identification of malware.

• DoS Attacks Detection: Confidentiality, Integrity, And Availability (CIA) are the three essential components of security or cyber-security. The CIA triad is a set of three components that are deemed essential for any system or network's security. One of the most important aspects of all three is availability. Availability literally refers to the character that is to be employed or gained, but in the context of information security, it assures that authentic users have fast and reliable access to information and other resources [16]. Denial of Service (DoS) assaults are employed by cyber intruders to disrupt the system's operation and users' access to system resources. By flooding a server with traffic, DoS assaults are employed to make online system resources unavailable to its users. Teardrop attacks, flooding attacks, IP fragmentation attacks, protocol attacks, and application-based attacks are all examples of DoS attacks [14]. To detect DoS assaults, researchers employed a variety of machine learning tactics. As an outcome, detection of these attacks is a critical feature of machine learning-based intrusion detection frameworks.

• Misuse Detection: Misuse detection is a key feature of machine learning-based intrusion detection systems. Misuse detection ensures that cybersecurity attacks that are known to an intrusion detection system are identified [17]. The intrusion detection system is already aware of the nature of these attacks and has signatures for them in its database of support. These existing signatures are employed to analyse and detect new assaults. As an outcome, detection systems that only have this feature have a hard time detecting unexpected assaults whose signatures are not in the supporting database.

• Anomaly Detection: The detection or identification of zero-day attacks (unknown attacks) is a difficult problem, and one of the key characteristics addressed by machine learning-based tactics. The framework's supporting database does not record the behaviour of zero-day attack types. Based on its expertise and experience, an intelligent machine learning framework analyses numerous types of assaults and attempts to predict their class [17]. As an outcome, a machine learning-based intrusion detection system must be able to detect zero-day assaults. It is critical in ensuring that a machine learning-based intrusion detection framework is suitable for use in an installation scenario.

• Implementation Complexity: As the name implies, it enumerates all of the complexities that must be considered during a system's whole implementation process. It defines all of the complexity parameters that researchers, scientists, and other shareholders take into account when developing a machine learning-based intrusion detection system. It involves processing power, amount of training data, framework working complexity, algorithm implementation difficulty, overall framework cost, and other required resources, among other things. As an outcome, implementation complexity is an important characteristic to consider when evaluating a machine learning-based intrusion detection system, and it has been taken into account in our estimation.

• Accuracy: This is the metric for determining the degree of correctness and precision of any computation or process when compared to the appropriate standard. It is one of the most remarkable characteristics of machine learning algorithms. The accuracy of proposed machine learning-based frameworks in machine learning is determined by how successfully they generate the needed outputs [24]. Precision, sensitivity, specificity, area under the curve, and other metrics are employed to assess it. When compared to other frameworks or tactics, it describes how accurate a machine learning-based framework is.

In some way, all of the aforementioned qualities apply to machine learning-based intrusion detection systems. Furthermore, all of the observed features play a key influence in the overall idealness of machine learning-based intrusion detection systems due to their implicit requirements. The study's authors first defined a set of 20 traits that were important to the research. The domain experts' team was then contacted to complete the characteristic set. Experts undertook a group discussion about all of the discovered characteristics and eliminated any that were unnecessary or inconsistent. Individual expert arguments over characteristic selection were reduced, and after this expert group discussion, a set of eight cyber security characteristics were chosen. As an outcome, each of these characteristics was examined in this estimation.

3 Proposed Hybrid Tactic

From a cyber-security standpoint, the tactic for our proposed work lays out a sequential strategy for machine learning-based intrusion detection systems. Under hazy conditions, reluctant AHP and TOPSIS were employed to complete this task. This tactic assisted us in obtaining more precise outcomes. Fuzzy logic has gained a lot of momentum as an improved form of classical logic in sectors where the solution to a problem could be anything from absolutely true to completely false. It could be completely true, partially true, partially false, or completely false. It includes the ability to deal with unclear data [25–27]. The AHP is the best tactic for dealing with problems that have several hierarchical solutions. The problem is analysed in a hierarchical manner. AHP provides accurate estimations for both subjective and objective values of characteristics [28]. TOPSIS is a well-known alternative ranking algorithm in the MCDM problem field that looks at the best alternative in a given set of alternatives [29]. The weights of qualities are computed using AHP under fuzzy conditions, and the alternatives are then ranked using TOPSIS. Numerical equations are supplied in the next section to aid researchers in undertaking a numerical analysis of this work.

As an outcome, we believe that the fuzzy AHP-TOPSIS tactic is excellent for dealing with situations like this. Prior research has found the importance and utility of findings acquired from the fuzzy AHP tactic. Experts have also pointed out that this review tactic has a number of disadvantages and repercussions. The authors devised another effective equivalent approach, the fuzzy TOPSIS, to address these implications and obstacles, which complement the fuzzy AHP and its consequences.

In addition, the fuzzy AHP tactic was employed to generate a systematic tree-like framework of numerous selected parts as a strategy for analysing the characteristic's impact on healthcare web apps. These variables were then subjected to the numerical equations. As a second first step in the examination, the practitioners converted the original weights of the characteristics supplied by experts into the Triangular Fuzzy Set Number (TFN). Further, TFN values are routinely demonstrated and validated to be between 0 and 1 for each characteristic [30]. The succeeding headings are also discussed to provide a more descriptive knowledge of the tactics employed:

Stage1: Succeeding the successful building of a tree framework, the practitioners established a function called membership by using the succeeding Eqs. (1) and (2).

$$\mu_a(x) = \ a \to [0, 1] \tag{1}$$

$$\mu_a(x) = \{\frac{x}{mi - l} - \frac{l}{mi - l} x \in [l, mi] \frac{x}{mi - u} - \frac{u}{mi - u} x \in [mi, u] \tag{2}$$

The upper limit is represented by limit 1, the medium is represented by mi, and the lower limit is represented by ui.

Stage 2: The practitioners now construct TFN numbers for characteristics using the succeeding formulas as the next step in the examination.

It is necessary to comprehend the representation mechanism in order to estimate triangular numbers. Eqs. (3)–(6) now performs the original dialogue for TFN [9].

$$\Phi_{ij} = (l_{ij},\ mi_{ij},\ u_{ij}) \tag{3}$$

Where, $l_{ij} \le mi_{ij} \le u_{ij}$

$$l_{ij} = min(J_{ijd}) \tag{4}$$

$$mi_{ij} = (J_{ij1}, J_{ij2}, J_{ij3})^{\frac{1}{x}} \tag{5}$$

$$u_{ij} = max(J_{ijd}) \tag{6}$$

In the formulas above, J_{ijd} represents a group of experts designated by the letters I and j. Furthermore, in the formula employed by the inspectors to estimate the variance between two particular components, d indicates the geometric mean value. Eqs. (7)-(9) stated the formulas for operating the intended GM value once it was calculated.

$$P + Q = (l_1 + l_2,\ mi_1 + mi_2,\ u_2 + u_2) \tag{7}$$

$$P \times Q = (l_1 \times l_2,\ mi_1 \times mi_2,\ u_1 \times u_2) \tag{8}$$

$$P^{-1} = \left(\frac{1}{u_1}, \frac{1}{mi_1}, \frac{1}{l_1}\right) \tag{9}$$

Stage3: For estimation, the succeeding Eq. (10) is employed:

$$\widetilde{A}^d = [\tilde{k}^d_{11}\tilde{k}^d_{12}\ldots.\tilde{k}^d_{1n}\tilde{k}^d_{21}\tilde{k}^d_{22}\ldots.\tilde{k}^d_{2n}\cdots\cdots\cdots\tilde{k}^d_{n1}\tilde{k}^d_{n2}\ldots\tilde{k}^d_{nn}] \tag{10}$$

where $\widetilde{k}^k_{ij}$ represents the opinions of experts. When there are numerous experts, the practitioners use the succeeding Eq. (11) to represent their opinions for estimation.

$$\tilde{k}_{ij} = \sum_{d=1}^{d} \tilde{k}^d_{ij} \tag{11}$$

Stage 4: It's also time to create a choice-based matrix using the succeeding Eq. (12).

$$\tilde{A} = \widetilde{k_{11}}\ldots\widetilde{k_{1n}}\cdots\ddots\cdots\widetilde{k_{n1}}\cdots\tilde{k}_{nn} \tag{12}$$

Stage 5: In a tree-based framework, Eq. (13) is employed to calculate GM, and Eq. (14) provides an estimation step for specific weights.

$$\tilde{p}_i = \left(\prod_{j=1}^{n} \tilde{k}_{ij}\right)^{\frac{1}{n}},\ i = 1, 2, 3\ldots\ldots.n \tag{13}$$

$$\tilde{w}_i = \tilde{p}_i \otimes (\tilde{p}_1 \oplus \tilde{p}_2 \oplus \tilde{p}_3\ldots. \oplus \tilde{p}_n)^{-1} \tag{14}$$

Stage 6: The practitioners now use Eqs. (15) and (16) to normalise the numbers after determining the particular weights for each characteristic.

$$M_i = \frac{\tilde{w}_1 \oplus \tilde{w}_2 \ldots\ldots \oplus \tilde{w}_n}{n} \tag{15}$$

$$Nr_i = \frac{M_i}{M_1 \oplus M_2 \oplus \ldots\ldots \oplus M_n} \tag{16}$$

Stage 7: The succeeding Eq. (17) is employed to calculate the best characteristic and ranking list of selected qualities.

$$BNPwD1 = \frac{[(uw1 - lw1) + (miw1 - lw1)]}{3} + lw1 \tag{17}$$

The estimations that were carried out using the fuzzy AHP tactic are now finished. After defining the ranking list and the weights of the criteria, the practitioners utilise a fuzzy TOPSIS MCDM tactic to test the evaluated outcomes. TOPSIS is a tactic for creating a numeric testing plot that resembles real-life testing [31]. The TOPSIS tactic is a powerful tool for assessing the efficiency and quality of fuzzy AHP outputs. The approach executes the estimation stages using some applications related to the field of hierarchy, and then employs them as an alternative in the estimation procedure. The headings below provide a concise overview of the tactic:

Stage 1: The practitioners assign weights for specific characteristics to the specific options chosen by the writers as the first step in the estimation process.

Stage 2: Apply Eq. (18) to create a matrix.

$$\tilde{K} = \begin{matrix} \\ A_1 \\ \ldots \\ A_m \end{matrix} \begin{matrix} \begin{matrix} C_1 & \ldots\ldots C_n \end{matrix} \\ \begin{bmatrix} \tilde{x}_{11} & \cdots \tilde{x}_{1n} \\ \ldots & \ddots \ldots \\ \tilde{x}_{m1} & \cdots \tilde{x}_{mn} \end{bmatrix} \end{matrix} \tag{18}$$

Stage3: Furthermore, after constructing a systematic matrix using Eq. (18), practitioners must normalise the values identified in the preceding phase, as shown in Eqs. (19) and (20).

$$\tilde{P} = [\tilde{p}_{ij}]_{m \times n} \tag{19}$$

$$\tilde{p}_{ij} = \left(\frac{l_{ij}}{u_j^+}, \frac{mi_{ij}}{u_j^+}, \frac{u_{ij}}{u_j^+} \right), \; u_j^+ = max\{u_{ij}, \; i = 1, 2, 3..n\} \tag{20}$$

The value of j is taken to be between 1 and 0. Furthermore, before the TFN values conversation, the normalisation tactic is widely employed. Stage 4: The practitioners obtains a numerical matrix for alternative estimation by applying Eq. (21).

$$\tilde{Q} = [\tilde{q}_{ij}]_{m \times n} i = 1, 2, ..m; \; j = 1, 2, 3 \ldots n \tag{21}$$

where, $\tilde{q}_{ij} = \tilde{p}_{ij} \otimes \tilde{w}_{ij}$

It's worth noting that during the estimation, normalised values are frequently shown to represent TFN values between 0 and 1.

Stage 5: To numerically quantify the +ve and –ve ideal solution value by applying Eqs. (22)–(25).

$$A^{+} = (\tilde{q}^{*}_{1,\ldots\ldots}\tilde{q}^{*}_{j,\ldots\ldots}\tilde{q}^{*}_{n,}) \tag{22}$$

$$A^{-} = (\tilde{q}^{*}_{1,\ldots\ldots}\tilde{q}^{*}_{j,\ldots\ldots}\tilde{q}^{*}_{n,}) \tag{23}$$

Here, $\tilde{q}^{*}_{1} = (1,1,1) \otimes \tilde{w}_{ij} = (Lw_j, Mw_j, Hw_j)$; $and\, \tilde{q}^{-}_{ij} = (0,0,0), \quad j = 1,2,3\ldots n$

$$\tilde{d}^{+}_{i} = \sum_{j=1}^{n} d(\tilde{q}_{ij}, \tilde{q}^{*}_{ij}), \quad i = 1,2,..m;\ j = 1,2,3\ldots n \tag{24}$$

$$\tilde{d}^{-}_{i} = \sum_{j=1}^{n} d(\tilde{q}_{ij}, \tilde{q}^{*}_{ij}), \quad i = 1,2,..m;\ j = 1,2,3\ldots n \tag{25}$$

Stage 6: The practitioners use Eq. (26) to calculate the optimal gap degree of alternative values in this final step of the estimation. For ideal alternative testing, the calculation of coefficient gap degree must be reviewed [32,33].

$$C\tilde{C}_{i} = \frac{\tilde{k}^{-}_{i}}{\tilde{k}^{+}_{i} + \tilde{k}^{-}_{i}} = 1 - \frac{\tilde{k}^{+}_{i}}{\tilde{k}^{+}_{i} + k^{-}_{i}}\ ,\ i = 1,2,\ldots.,m \tag{26}$$

where $\frac{\tilde{k}^{-}_{i}}{\tilde{k}^{+}_{i} + \tilde{k}^{-}_{i}}$ represents the degree of satisfaction with an alternative and displays the degree of a gap.

Using the above-mentioned systematic step-by-step tactic, this project will undertake a case study on machine learning-based intrusion detection systems for the idealness estimation from a cybersecurity aspect. The numerical computations for this examination are detailed in the next section of this article.

4 Numerical Analysis

Because quantitative estimation of a qualitative characteristic is a challenging procedure, evaluating the quality characteristics of any software-based system, including cybersecurity, is a difficult process [8]. The numerical analysis presented in this paper will provide a quantitative estimation of machine learning-based intrusion detection systems. As an outcome, this article conducts a case study on 8 distinct machine learning-based intrusion detection systems in order to evaluate their optimum cybersecurity qualities. For this project, 8 different intrusion detection systems were chosen as possibilities. The tactic we adopted for our study requires the identification of alternatives and the ranking of those options. Furthermore, these 8 different intrusion detection systems were chosen as options for their comparative cyber-security estimation based on the collaborative choice of domain experts and intrusion detection system owners. To make this activity more corroborative and efficient, AHP-TOPSIS was employed under fuzzy conditions. This experiment looked at eight characteristics, including spam detection, phishing detection, malware detection, DoS attack detection, abuse detection, anomaly detection, implementation difficulty, and accuracy, to establish the idealness estimation of a machine learning-based intrusion detection system. In the succeeding research, the identified features were designated as F1, F2, F3, F4, F5, F6, F7, and F8. Idealness estimation of machine learning-based intrusion detection systems has been performed using AHP-TOPSIS under the succeeding conditions, as given in Eqs. (1)–(26) in Section 4 of this paper:

Initially, the language concepts were translated into numeric values and later into fuzzy logic based crisp numeric values by considering Eqs. (1)–(9). The outcomes of the numerical calculations

were then employed to generate a pair-wise comparison matrix, as shown in Tab. 1. The procedure encountered the implementation of fuzzy wrappers by approaching Eq. (1); approaching Eqs. (2) and (5); estimation of trapezoidal numbers C = (l, m, n, o); and approaching Eqs. (6) and (7), and considering, which represents a number between (0–1), the 1st and 2nd weight types have been discovered. Finally, the experts calculated the pair-wise comparison matrix using Eqs. (8) and (9). We haven't included the intermediate processes because they aren't really important.

Table 1: Trapezoidal fuzzy pair-wise comparison matrix at level 1

	F1	F2	F3	F4	F5	F6	F7	F8
F1	1.00000, 1.00000, 1.00000	0.23254, 0.28547, 0.36569	0.30758, 0.44456, 0.80587	0.49857, 0.64635, 1.00256	0.27212, 0.31425, 0.52253	1.00568, 1.57582, 1.93564	0.49758, 0.64745, 1.00746	0.27745, 0.35457, 0.52463
F2	-	1.00000, 1.00000, 1.00000	0.66474, 1.17452, 1.69474	0.66547, 1.17457, 1.69563	1.15542, 1.44154, 1.70236	0.22453, 0.24759, 0.42635	1.00475, 1.32475, 1.55556	1.15458, 1.44745, 1.70745
F3	-	-	1.00000, 1.00000, 1.00000	1.19745, 1.58475, 2.15653	0.49457, 0.64745, 1.00457	0.27532, 0.37895, 0.52856	0.37540, 0.44745, 0.88589	0.49758, 0.68544, 1.07780
F4	-	-	-	1.00000, 1.00000, 1.00000	1.00747, 1.32456, 1.55444	1.15596, 1.44414, 1.70444	0.66485, 1.17774, 1.69465	0.66566, 1.14587, 1.67899
F5	-	-	-	-	1.00000, 1.00000, 1.00000	0.49474, 0.64454, 1.00114	1.00263, 1.32214, 1.55345	1.11235, 1.42564, 1.74570
F6	-	-	-	-	-	1.00000, 1.00000, 1.00000	0.27748, 0.35563, 0.52474	0.47459, 0.64745, 1.07450
F7	-	-	-	-	-	-	1.00000, 1.00000, 1.00000	1.17455, 1.44574, 1.77780
F8	-	-	-	-	-	-	-	1.00000, 1.00000, 1.00000

The defuzzified values and normalised weights of the level 1 characteristic were computed using Eqs. (10)–(16), and the outcomes are displayed in Tab. 2. In order to calculate Tab. 2, the succeeding intermediate steps were employed: For the defuzzification procedure, Eq. (10) was employed to turn the pair-wise comparison matrixes into united defuzzified values. Then, to ensure matrix consistency, Eqs. (11) and (12) were employed to calculate the consistency index and consistency ratio (CR), and we found that CR = 0.03485540 for this study, which equals 0.1, indicating that our evaluated matrix is consistent. After that, numerical calculations were performed to determine the geometric mean for row values and the most relevant qualities, using Eqs. (13) and (14) as a guide. Then, using Eqs. (15) and (16), the defuzzified data was analysed and converted to normalised weights.

Table 2: Weights after defuzzification

	F1	F2	F3	F4	F5	F6	F7	F8	Defuzzified weights
F1	1.00000	0.24587	0.98547	0.38547	0.64857	0.36522	0.92545	0.18547	0.059362
F2	4.06719	1.00000	0.18574	0.17584	0.17458	0.18596	0.19658	0.38898	0.049009
F3	1.01474	5.38387	1.00000	1.74578	1.04554	0.72565	0.13652	0.92565	0.105436
F4	2.59424	5.68699	0.57281	1.00000	0.93365	0.12565	0.32563	0.75874	0.092310
F5	1.54185	5.72803	0.95644	1.07107	1.00000	0.95857	0.74587	1.77458	0.133181
F6	2.73808	5.3775	1.37807	7.95862	1.04322	1.00000	1.02545	1.22541	0.205979
F7	1.08056	5.08699	7.32493	3.07097	1.34072	0.97518	1.00000	0.48574	0.204074
F8	5.39171	2.57083	1.08032	1.31797	0.56351	0.81605	2.05871	1.00000	0.150648
					C.R. = 0.01254024				

Succeeding that, this section of the paper gives a realistic estimation of the evaluated outcomes of extremely sensitive machine learning-based intrusion detection systems employed in Indian hospitals. The global ranking of competing alternatives was constructed using TOPSIS under fuzzy logic conditions after the defuzzified and normalised weights of characteristics were obtained using an AHP tactic under fuzzy logic conditions. The summarised outcomes displayed in Tab. 3 were computed by combining the standard scale specified in the Tactic sub-section at step 10 and Eqs. (1) and (17) from the technological data of 8 machine learning-based intrusion detection systems. The AHP-derived characteristic weights are fed into the TOPSIS tactic under fuzzy logic conditions to get the ranking order for the alternatives. Tab. 4 shows the normalised fuzzy decision-matrix for 8 qualities and 8 competitive options, which was calculated using certain intermediary operations and combining step 10 and Eq. (18). Using Eqs. (19)–(22), the normalised fuzzy decision-matrix cell values (performance-values) are multiplied by each characteristic weight value, yielding a weighted fuzzy normalised decision-matrix, as shown in Tab. 5. The final outcomes are listed in Tab. 6 under the column headings dist+ and dist-, which were calculated using Eqs. (22) and (23) to determine the positive and negative idealness of each alternative for each characteristic. The CC-i satisfaction degree was then calculated as the relative closeness score for each choice using Eqs. (25) and (26), and the outcomes are shown in Tab. 6 and Fig. 2.

Table 3: Subjective cognition outcomes

Characteristics (SDA)/ alternatives	A-1	A-2	A-3	A-4	A-5	A-6	A-7	A-8
F1	1.1800, 3.0000, 5.0000	1.6400, 3.3600, 5.3600	0.3600, 1.7300, 3.7300	6.2700, 8.2700, 9.4500	1.1800, 3.0000, 5.0000	1.6400, 3.3600, 5.3600	0.3600, 1.7300, 3.7300	6.2700, 8.2700, 9.4500
F2	0.7300, 2.4500, 4.4500	0.8200, 2.4500, 4.4500	1.1800, 3.0000, 5.0000	4.1800, 6.0900, 7.6400	0.7300, 2.4500, 4.4500	0.8200, 2.4500, 4.4500	1.1800, 3.0000, 5.0000	4.1800, 6.0900, 7.6400

(Continued)

Table 3: Continued

Characteristics (SDA)/ alternatives	A-1	A-2	A-3	A-4	A-5	A-6	A-7	A-8
F3	0.8200, 2.4500, 4.4500	1.0000, 2.6400, 4.6400	0.7300, 2.4500, 4.4500	5.0000, 7.0000, 8.4500	1.0000, 2.6400, 4.6400	0.7300, 2.4500, 4.4500	5.0000, 7.0000, 8.4500	2.8200, 4.8200, 6.7300
F4	1.0000, 2.6400, 4.6400	0.7300, 2.4500, 4.4500	5.0000, 7.0000, 8.4500	2.8200, 4.8200, 6.7300	0.7300, 2.2700, 4.2700	0.6400, 2.2700, 4.2700	5.3600, 7.3600, 8.7300	1.1800, 3.0000, 5.0000
F5	0.7300, 2.2700, 4.2700	0.6400, 2.2700, 4.2700	5.3600, 7.3600, 8.7300	1.1800, 3.0000, 5.0000	1.6400, 3.3600, 5.3600	0.3600, 1.7300, 3.7300	6.2700, 8.2700, 9.4500	4.0900, 6.0900, 7.7300
F6	1.6400, 3.3600, 5.3600	1.1800, 3.0000, 5.0000	1.6400, 3.3600, 5.3600	0.3600, 1.7300, 3.7300	1.1800, 3.0000, 5.0000	1.6400, 3.3600, 5.3600	0.3600, 1.7300, 3.7300	6.2700, 8.2700, 9.4500
F7	0.8200, 2.4500, 4.4500	0.7300, 2.4500, 4.4500	0.8200, 2.4500, 4.4500	1.1800, 3.0000, 5.0000	0.7300, 2.4500, 4.4500	0.8200, 2.4500, 4.4500	1.1800, 3.0000, 5.0000	4.1800, 6.0900, 7.6400
F8	1.0000, 2.6400, 4.6400	0.8200, 2.4500, 4.4500	1.0000, 2.6400, 4.6400	0.7300, 2.4500, 4.4500	0.8200, 2.4500, 4.4500	1.0000, 2.6400, 4.6400	0.7300, 2.4500, 4.4500	5.0000, 7.0000, 8.4500

Table 4: The normalized fuzzy-decision matrix

	A-1	A-2	A-3	A-4	A-5	A-6	A-7	A-8
F1	0.4200, 0.6900, 0.9900	0.3800, 0.6600, 0.9600	0.2000, 0.5000, 0.8000	0.5500, 0.7600, 0.9300	0.2000, 0.4700, 0.7700	0.4600, 0.6800, 0.8700	0.1800, 0.4500, 0.7400	0.2000, 0.5000, 0.8000
F2	0.2000, 0.4700, 0.7700	0.2000, 0.5000, 0.8000	0.2000, 0.5000, 0.8000	0.4700, 0.6800, 0.8800	0.2000, 0.5000, 0.8000	0.5500, 0.7600, 0.9300	0.2000, 0.4700, 0.7700	0.1200, 0.3900, 0.6900
F3	0.4700, 0.6800, 0.8800	0.2000, 0.5000, 0.8000	0.5500, 0.7600, 0.9300	0.2000, 0.4700, 0.7700	0.1200, 0.3900, 0.6900	0.4700, 0.6800, 0.8800	0.2000, 0.4700, 0.7700	0.5400, 0.7500, 0.9300
F4	0.2000, 0.4700, 0.7700	0.2000, 0.5000, 0.8000	0.4700, 0.6800, 0.8800	0.2000, 0.4700, 0.7700	0.5400, 0.7500, 0.9300	0.2000, 0.4700, 0.7700	0.1600, 0.4200, 0.7200	0.3000, 0.5700, 0.8300
F5	0.2000, 0.5000, 0.8000	0.5500, 0.7600, 0.9300	0.4700, 0.6800, 0.8800	0.2000, 0.5000, 0.8000	0.5500, 0.7600, 0.9300	0.2000, 0.4700, 0.7700	0.1200, 0.3900, 0.6900	0.1800, 0.4500, 0.7400

(Continued)

Table 4: Continued

	A-1	A-2	A-3	A-4	A-5	A-6	A-7	A-8
F6	0.5200, 0.7400, 0.9200	0.2000, 0.4700, 0.7700	0.2000, 0.4700, 0.7700	0.2000, 0.5000, 0.8000	0.4700, 0.6800, 0.8800	0.2000, 0.4700, 0.7700	0.5400, 0.7500, 0.9300	0.2000, 0.4700, 0.7700
F7	0.6000, 0.8100, 1.0000	0.4700, 0.6800, 0.8800	0.2000, 0.5000, 0.8000	0.5500, 0.7600, 0.9300	0.2000, 0.4700, 0.7700	0.1200, 0.3900, 0.6900	0.3000, 0.5700, 0.8300	0.2000, 0.4700, 0.7700
F8	0.4600, 0.6800, 0.8800	0.2000, 0.4700, 0.7700	0.2000, 0.5000, 0.8000	0.4700, 0.6800, 0.8800	0.2000, 0.4700, 0.7700	0.5400, 0.7500, 0.9300	0.2000, 0.5000, 0.8000	0.5500, 0.7600, 0.9300

Table 5: The weighted normalized fuzzy-decision matrix

	A-1	A-2	A-3	A-4	A-5	A-6	A-7	A-8
F1	0.0020, 0.0070, 0.0270	0.0020, 0.0070, 0.0250	0.0020, 0.0060, 0.0200	0.0010, 0.0050, 0.0190	0.0020, 0.0100, 0.0370	0.0020, 0.0090, 0.0380	0.0020, 0.0100, 0.0390	0.0020, 0.0090, 0.0380
F2	0.0020, 0.0100, 0.0370	0.0020, 0.0090, 0.0380	0.0000, 0.0020, 0.0090	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0190	0.0010, 0.0050, 0.0180	0.0010, 0.0040, 0.0170	0.0010, 0.0050, 0.0180
F3	0.0010, 0.0050, 0.0190	0.0010, 0.0050, 0.0180	0.0020, 0.0100, 0.0390	0.0020, 0.0090, 0.0380	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0190	0.0020, 0.0100, 0.0370	0.0020, 0.0090, 0.0380
F4	0.0020, 0.0060, 0.0200	0.0010, 0.0050, 0.0190	0.0010, 0.0050, 0.0180	0.0020, 0.0100, 0.0390	0.0020, 0.0070, 0.0250	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0190	0.0010, 0.0050, 0.0180
F5	0.0010, 0.0050, 0.0190	0.0020, 0.0100, 0.0370	0.0020, 0.0090, 0.0380	0.0010, 0.0040, 0.0170	0.0020, 0.0090, 0.0380	0.0020, 0.0090, 0.0380	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090
F6	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0190	0.0010, 0.0050, 0.0180	0.0020, 0.0100, 0.0390	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0190	0.0020, 0.0100, 0.0370	0.0020, 0.0090, 0.0380
F7	0.0020, 0.0090, 0.0380	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090	0.0000, 0.0040, 0.0170	0.0010, 0.0050, 0.0190	0.0010, 0.0050, 0.0180	0.0010, 0.0050, 0.0190	0.0010, 0.0050, 0.0180
F8	0.0020, 0.0100, 0.0390	0.0020, 0.0070, 0.0250	0.0020, 0.0060, 0.0200	0.0000, 0.0020, 0.0090	0.0010, 0.0050, 0.0180	0.0020, 0.0090, 0.0380	0.0010, 0.0050, 0.0180	0.0000, 0.0020, 0.0090

Table 6: Closeness coefficients of selected alternatives

Alternatives	Dist+	Dist−	Gaps degree of CC+ i	Satisfaction degree of CC −i	Alternative Ranks
A-1	0.345254	0.596587	0.595652	0.3652587	7
A-2	0.036525	0.056524	0.652587	0.3475859	8
A-3	0.034742	0.052566	0.502547	0.4889876	5
A-4	0.040221	0.054745	0.523695	0.4856 + 97	6
A-5	0.036874	0.063526	0.555645	0.4933021	4
A-6	0.063587	0.026789	0.385989	0.6232547	2
A-7	0.036524	0.036252	0.456362	0.5321255	3
A-8	0.042415	0.024525	0.402560	0.6554744	1

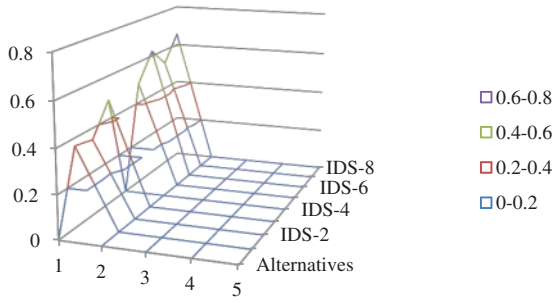

Figure 2: Graphical representation of satisfaction degree

In an idealness estimation of machine learning-based cybersecurity, the numerical findings demonstrate that, based on the performance scores, the competitive alternative rankings (8 machine learning-based intrusion detection systems) are generated as: A-6, A-8, A-7, A-5, A-4, A-3, A-1, and A-2. The idealness estimation of 8 alternative machine learning-based intrusion detection systems based on defined criteria found that A-6 is more ideal and effective in addressing important cybersecurity problems and difficulties. Furthermore, the identified characteristics for the idealness estimation of machine learning-based intrusion detection systems have been prioritised in the succeeding order, using a TOPSIS approach under fuzzy logic conditions: accuracy, anomaly detection, misuse detection, DoS attack detection, malware detection, implementation complexity, spam detection, and phishing detection, with global normalised weights of 0.273937, 0.222015, 0.127306, 0.122505, 0.10973, 0.053217, 0.052354, and 0.

Furthermore, the applicability of our suggested research is not nil. As an alternative, we looked at 8 real-time intrusion detection systems from numerous Indian hospitals. According to current relevant research works [8–17], alternative estimation selection is an inherent aspect of our proposed tactic. For this case study, the alternative selection is the outcome of a group decision made by domain experts and owners of intrusion detection systems. Furthermore, the quantitative outcomes show that the A-6 has acquired the greatest number of qualities from the defined characteristic set for this research. Due to its hybrid properties, it integrates several machine learning tactics for the detection of different types of cyber-security assaults, which is the subject of our investigation. Similarly, other intrusion detection

systems, receive a lower performance score in descending order for the identified qualities and domain of their detection of known cyber-security assaults.

5 Discussion

Cybersecurity protects information, information systems, and networks against intruders in real time. Over the last decade, there has been a massive surge in cybersecurity breaches, and cases of data theft are increasing by the day. Organizations have spent a significant amount of money to solve these cybersecurity vulnerabilities, and attempts to combat these incursions have already begun. Experts and researchers have employed a variety of tactics and strategies to develop trustworthy and effective security systems. Machine learning is one of the most well-known of them, and it plays an important role in cybersecurity [4]. Machine learning has a proactive personality that can successfully manage cybersecurity challenges, assess risks, and respond to breaches and security incidents in a timely and instinctive manner [6–8]. As an outcome, machine-learning approaches are better suited to identifying and classifying diverse types of cyber-attacks. In particular, supervised and unsupervised machine learning approaches are capable of addressing a wide range of cybersecurity concerns [9]. Numerous intrusion detection systems have been developed and designed by cybersecurity experts and academics in the past few years to identify numerous types of cybersecurity threats [6].

The major goal of this research was to examine the idealness of intrusion detection systems using integrated fuzzy-based AHP-TOPSIS tactics, as indicated. The features that were included in this estimation were identified and chosen using expert opinions and current relevant research findings. The accuracy characteristic has obtained the highest importance in AHP under fuzzy logic conditions, followed by anomaly detection, misuse detection, DoS attack detection, malware detection, implementation complexity, spam detection, and phishing detection. With a performance score of 0.355475 computed with respect to machine learning relevant cybersecurity characteristics, TOPSIS under fuzzy logic conditions shows that A-6 has earned the highest ranking, while A-2 has gained the lowest ranking. The findings show that A-6 provides better and more reliable cybersecurity than the other nine options. This study will contribute to the development of secure and dependable intrusion detection systems as well as machine learning-based cybersecurity characteristic estimations.

According to the study's findings, the intrusion detection system A-6 best matches the machine learning-based cyber security characteristics that were employed to evaluate the idealness of intrusion detection systems from a machine learning-based cybersecurity perspective. It was decided to be the best in terms of supplying an optimal and trustworthy machine learning-based cybersecurity mechanism against probable threats, with a performance score of 0.635660. The succeeding points summarise the study's main findings and conclusions.

The succeeding machine learning-based cybersecurity characteristics are prioritised in this research experiment: accuracy, anomaly detection, misuse detection, DoS attack detection, malware detection, implementation complexity, spam detection, and phishing detection, with global normalised weights of 0.273937, 0.222015, 0.127306, 0.122505, 0.10973, 0.053217, 0.052354, and 0.038937, respectively.

In terms of recognised weighted machine learning-based cybersecurity qualities, after A-6, the succeeding competing alternatives are rated in order based on their produced performance scores: A-8, A-7, A-5, A-4, A-3, A-1, and A-2.

Intrusion detection systems that use machine learning to provide cybersecurity are a difficult problem to solve, and our study provides correct recommendations for constructing optimal and effective machine learning-based intrusion detection systems.

This research was carried out primarily for intrusion detection systems employed in healthcare settings. Because the estimation characteristics are determined on the basis of generalisation, they may be employed as a guideline for developing any type of ideal and successful intrusion detection system.

6 Conclusions

According to the conclusions of this study, cyber security issues and breaches have been a difficult challenge for researchers and security specialists in recent years. To construct trustworthy and effective security systems, experts and researchers have employed a number of approaches and strategies. One of the most well-known is machine learning, which plays an important role in cybersecurity. We employed fuzzy-based AHP-TOPSIS to investigate the impact of cyber security-related characteristics on intrusion detection systems in this league. Researchers and developers will be able to use this tactic to prioritise cyber security characteristics and design safer and more reliable intrusion detection systems using this tactic. Research, on the other hand, is a dynamic and ongoing endeavour. As an outcome, while our machine learning-based cybersecurity estimation is accurate, it falls short of achieving optimal outcomes. There are other MCDM tactics that can be employed to achieve more efficient outcomes. Nonetheless, our empirical data suggests that we employed a trustworthy strategy for this estimation.

Acknowledgement: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number "IFPHI: 268-611-2020" and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Funding Statement: Funding for this study was received from the Ministry of Education and Deanship of Scientific Research at King Abdulaziz University, Kingdom of Saudi Arabia under the Grant No. IFPHI-268-611-2020.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] D. Koo, Y. Shin, J. Yun and J. Hur, "A hybrid reduplication for secure and efficient data outsourcing in fog computing," in *Proc. of the 2016 IEEE 8th Int. Conf. on Cloud Computing Technology and Science*, Luxembourg City, Luxembourg, pp. 285–293, 2016.

[2] M. T. J. Ansari, A. Baz, H. Alhakami, W. Alhakami, R. Kumar *et al.,* "P-STORE: Extension of store tactic to elicit privacy requirements," *Arabian Journal for Science and Engineering*, Article, in press, vol. 36, pp. 1–24, 2021.

[3] J. Zadeh and D. Devolder, "Software development and related security issues," in *Proc. of the 2007 IEEE Southeast Conf.*, Beijing, China, Richmond, VA, USA, pp. 746–748, 2007.

[4] F. A. Alzahrani, M. Ahmad, M. Nadeem, R. Kumar and R. A. Khan, "Integrity estimation of medical devices for improving hospital services," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3619–3633, 2021.

[5] T. L. Satty, "The analytic hierarchy process," *Analytic Hierarchy Process Journal*, vol. 5, no. 6, pp. 187–194, 1980.

[6] L. A. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338–353, 1965.
[7] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Evaluating the impact of prediction techniques: Software reliability perspective," *Computers, Materials & Continua*, vol. 67, no. 2, pp. 1471–1488, 2021.
[8] S. F. Gürses and T. Santen, "Contextualizing security goals: A method for multilateral security requirements elicitation," *Sicherheit–Schutz und Zuverlässigkeit*, vol. 5, no. 8, pp. 1–44, 2006.
[9] T. L. Saaty, "How to make a decision: The analytic hierarchy process," *European Journal of Operational Research*, vol. 48, no. 1, pp. 9–26, 1990.
[10] K. Sahu and R. K. Srivastava, ""'Predicting software bugs of newly and large datasets through a unified neuro-fuzzy approach: Reliability perspective," *Advances in Mathematics: Scientific Journal*, vol. 10, no. 1, pp. 543–555, 2021.
[11] M. Zarour, M. T. J. Ansari, M. Alenezi, A. K. Sarkar, M. Faizan *et al.,* "Evaluating the impact of blockchain frameworks for secure and trustworthy electronic healthcare records," *IEEE Access*, vol. 8, no. 8, pp. 157959–157973, 2020.
[12] C. L. Hwang and K. Yoon, "Methods for multiple attribute decision making," in *Lecture Notes in Economics and Mathematical Systems*, LA, USA, Berlin, Heidelberg, vol. 186, pp. 58–191, 1981.
[13] R. M. Rodriguez, L. Martinez and F. Herrera, "Hesitant fuzzy linguistic term sets for decision making," *IEEE Transaction Fuzzy System*, vol. 20, no. 7, pp. 109–119, 2011.
[14] V. Torra and Y. Narukawa, "On hesitant fuzzy sets and decision," in *Proc. of the 2009 IEEE Int. Conf. on Fuzzy Systems*, Jeju Island, South Korea, pp. 1378–1382, 2009.
[15] İ Ertuğrul and N. Karakaşoğlu, "Comparison of fuzzy AHP and fuzzy TOPSIS methods for facility location selection," *the International Journal of Advanced Manufacturing Technology*, vol. 39, no. 8, pp. 783–795, 2008.
[16] F. A. Nouri, S. K. Esbouei and J. Antucheviciene, "A hybrid MCDM approach based on fuzzy AHP and fuzzy TOPSIS for technology selection," *Informatica*, vol. 26, no. 3, pp. 369–388, 2015.
[17] R. J. Kuo, C. W. Hsu and Y. L. Chen, "Integration of fuzzy AHP and fuzzy TOPSIS for evaluating carbon performance of suppliers," *International Journal of Environmental Science and Technology*, vol. 12, no. 12, pp. 3863–3876, 2015.
[18] B. C. Ervural, S. Zaim, O. F. Demirel, Z. Aydin and D. Delen, "An AHP and fuzzy TOPSIS-based SWOT analysis for Turkey's energy planning," *Renewable and Sustainable Energy Reviews*, vol. 82, no. 5, pp. 1538–1550, 2018.
[19] A. Abbaspour, M. Saremi, A. Alibabaei and P. S. Moghanlu, "Determining the optimal human reliability analysis (HRA) method in healthcare systems using fuzzy AHP and fuzzy TOPSIS," *Journal of Patient Safety and Risk Management*, vol. 8, no. 6, pp. 1–20, 2020.
[20] N. R. Alharbe, "A Fuzzy-delphi based decision-making process for measuring usable-security of web based smart hospital management system," *ICIC Express Letters*, vol. 14, no. 1, pp. 15–21, 2020.
[21] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* "An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications," *IEEE Access*, vol. 8, no. 8, pp. 50944–50957, 2020.
[22] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* "A Knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications," *IEEE Access*, vol. 8, no. 8, pp. 48870–48885, 2020.
[23] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal and R. A. Khan, "Measuring security durability of software through fuzzy-based decision-making process," *International Journal of Computational Intelligence Systems*, vol. 12, no. 2, pp. 627–642, 2019.
[24] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Hesitant fuzzy sets based symmetrical framework of decision-making for estimating the durability of web application," *Symmetry*, vol. 12, no. 6, pp. 1770–1792, 2020.
[25] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *ICIC Express Letters*, vol. 12, no. 12, pp. 1213–1222, 2018.

[26] K. Sahu and R. K. Srivastava, "Needs and importance of reliability prediction: An industrial perspective," *Information Sciences Letters*, vol. 9, no. 1, pp. 33–37, 2020.
[27] K. Sahu and R. K. Srivastava, "Revisiting software reliability," *Advances in Intelligent Systems and Computing*, vol. 802, pp. 221–235, 2019.
[28] A. I. Khan, A. Saad, F. J. Alsolami, Y. B. Abushark, A. Almalawi *et al.,* "Integrating blockchain technology into healthcare through an intelligent computing technique," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2835–2860, 2022.
[29] A. S. Alfakeeh, A. Almalawi, F. J. Alsolami, Y. B. Abushark, A. I. Khan *et al.,* "Hesitant fuzzy-sets based decision-making framework for security risk assessment," *Computers, Materials & Continua*, vol. 70, no. 2, pp. 2297–2317, 2022.
[30] F. J. Alsolami, A. S. A. Alghamdi, A. I. Khan, Y. B. Abushark, A. Almalawi *et al.,* "Impact assessment of covid-19 pandemic through machine learning frameworks," *Computers, Materials & Continua*, vol. 68, no. 3, pp. 2895–2912, 2021.
[31] Y. B. Abushark, A. I. Khan, F. J. Alsolami, A. Almalawi, M. M. Alam *et al.,* "Usability evaluation through fuzzy AHP-TOPSIS approach: Security requirement perspective," *Computers, Materials & Continua*, vol. 68, no. 1, pp. 1203–1218, 2021.
[32] J. Kaur, A. I. Khan, Y. B. Abushark, M. Alam, S. A. Khan *et al.,* "Security risk assessment of healthcare web application through adaptive neuro-fuzzy inference system: A design perspective," *Risk Management and Healthcare Policy*, vol. 13, no. 5, pp. 355–371, 2020.
[33] A. Alharbi, A. H. Seh, W. Alosaimi, H. Alyami, A. Agrawal *et al.,* "Analyzing the Impact of Cyber Security Related Attributes for Intrusion Detection Systems," *Sustainability*, vol. 13, no. 22, pp. 1–18, 2021.