Computers, Materials & Continua
DOI: 10.32604/cmc.2022.026554
Article

Tech Science Press

Selecting Best Software Vulnerability Scanner Using Intuitionistic Fuzzy Set TOPSIS

Navneet Bhatt[1], Jasmine Kaur[2], Adarsh Anand[2] and Omar H. Alhazmi[3,*]

[1]Anil Surendra Modi School of Commerce, Narsee Monjee Institute of Management Studies, Deemed to be University, Mumbai, 400056, India
[2]Department of Operational Research, Faculty of Mathematical Sciences, University of Delhi, Delhi, 110007, India
[3]Department of Computer Science, Taibah University, Medina, 30001, Saudi Arabia
*Corresponding Author: Omar H. Alhazmi. Email: ohhazmi@taibahu.edu.sa
Received: 30 December 2021; Accepted: 22 February 2022

Abstract: Software developers endeavor to build their products with the least number of bugs. Despite this, many vulnerabilities are detected in software that threatens its integrity. Various automated software i.e., vulnerability scanners, are available in the market which helps detect and manage vulnerabilities in a computer, application, or a network. Hence, the choice of an appropriate vulnerability scanner is crucial to ensure efficient vulnerability management. The current work serves a dual purpose, first, to identify the key factors which affect the vulnerability discovery process in a network. The second, is to rank the popular vulnerability scanners based on the identified attributes. This will aid the firm in determining the best scanner for them considering multiple aspects. The multi-criterion decision making based ranking approach has been discussed using the Intuitionistic Fuzzy set (IFS) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) to rank the various scanners. Using IFS TOPSIS, the opinion of a whole group could be simultaneously considered in the vulnerability scanner selection. In this study, five popular vulnerability scanners, namely, Nessus, Fsecure Radar, Greenbone, Qualys, and Nexpose have been considered. The inputs of industry specialists i.e., people who deal in software security and vulnerability management process have been taken for the ranking process. Using the proposed methodology, a hierarchical classification of the various vulnerability scanners could be achieved. The clear enumeration of the steps allows for easy adaptability of the model to varied situations. This study will help product developers become aware of the needs of the market and design better scanners. And from the user's point of view, it will help the system administrators in deciding which scanner to deploy depending on the company's needs and preferences. The current work is the first to use a Multi Criterion Group Decision Making technique in vulnerability scanner selection.

Keywords: Intuitionistic fuzzy set; group decision making; multi-criteria decision making (MCDM); ranking algorithm; software security; TOPSIS; vulnerability; vulnerability scanners

1 Introduction

Secure software is not an overnight creation. Like any other good quality product, it requires careful planning, scrutiny, wise decision-making, and efficient implementation throughout the life cycle. The adage 'Prevention is better than cure' holds in this context too and investing in each phase of the software development lifecycle (SDLC) to prevent the rise of security loopholes is much better than handling an issue when it arises. Any flaw which endangers the data, functionality and accessibility of software is considered a security threat. A security threat can be mitigated through efficient testing and an effective update and upgrade policy. Various types of testing such as vulnerability scanning, penetration testing, security scanning, risk assessment, security auditing, posture assessment, and ethical hacking are carried out to ensure software security. Tools like dynamic application security testing (DAST) and static application security testing (SAST) are commonly used for this purpose. According to The State of Application Security, 2020 report, software vulnerabilities and application weakness are the two major causes of an external attack on software [1].

A software vulnerability is a security threat that arises due to a bug, or a fault discovered in the operational phase of the software lifecycle. They are the potentially exploitable loopholes in the software caused due to insufficient testing, bad coding practices, compatibility issues arising due to new code addition in an upgrade, etc. A typical vulnerability undergoes the following lifecycle: it gets injected, detected, exposed, exploited, and patched. The types of vulnerabilities include Cross-Site Scripting, Buffer overflow, Path Traversal, SQL Injection, Command Injection, Open Redirect, etc. Common Vulnerability Scoring System (CVSS) is the most widely used system to assign a value to the severity of each vulnerability on a scale of 1 to 10 with 10 being the most severe. Common Vulnerability and Exposures (CVE), owned by Mitre organization also issues a unique CVE id to each known vulnerability using which the detailed information about its type, severity, impact, etc. can be obtained. The CVE database has known records of 151,798 vulnerabilities to date. According to National Vulnerability Database (NVD), 17220 vulnerabilities were reported in 2019 alone. Windows operating system and Chrome browser were deemed to be the most vulnerable in their respective category. This information about the vulnerabilities lies in the public domain and can be easily accessed by anyone. Hence, mitigating or eliminating vulnerabilities from the system is a time-sensitive issue. An efficient vulnerability management plan is required which handles the vulnerability before it is exploited. In April 2021, 530 million records of personal data from Facebook were released publically. The breach occurred back in August 2019 by exploiting a vulnerability. Even though the vulnerability was fixed by the company in the same month, the data breach had already occurred.

Vulnerability management involves identifying a vulnerability, classifying it and preventing its exploitation. A lot of effort and resources are put in to identify vulnerabilities. Many bounty hunting programs are financed by firms to detect vulnerabilities in their software. White hat hackers proactively work on detecting and ethically reporting them. Patching service is the most common approach to mitigate or remove the vulnerability from the system.

Vulnerability scanning is the first step in the process of vulnerability detection which are automated processes that detect vulnerabilities or weaknesses in a network, web application, system, and database. Each scanner has a database of the known vulnerabilities, and it compares the detected flaw with the database entries to determine the vulnerability type and then patch it. Various categories of vulnerability scanners are available like network-based scanners, database scanners, host-based scanners, application scanners and wireless scanners.

In the recent time, lot of firms are coming up with software which necessitates the use of vulnerability scanners to keep them safe. Choosing the right vulnerability scanner is a very difficult and important decision. Different surveys tend to focus on different parameters. Certain websites such as Gartner Peer Insights and g2.com provide a comparative performance evaluation of vulnerability scanners, usually based on popular opinions and peer reviews [2,3]. According to the Cybersecurity Insiders' 2018 Application Security Report, Tenable Inc.'s Nessus is the most adopted vulnerability scanner followed by Qualys and then Rapid 7. Tenable was a sponsor of this survey [4,5]. The top results of an internet search for vulnerability scanning software are the numerous lists by varied websites for the "top 10", "top 15", "best", "paid" and "free" vulnerability scanners. The definitions, the working, and the purpose of the vulnerability scanners come much later in the search results. This points to the high demand for such a ranking and also to the lack of a single comprehensive, industry-standard list. The proposed work aims to rectify it.

Decision making is a very complex process that requires taking care of multiple factors simultaneously. Manual evaluation or intuition-based decision making is not always reliable as some factor or the other tends to get overlooked. Making multiple decisions can also lead to decision fatigue which results in inadequate decisions. Hence, the need for a mathematical approach arises which is unbiased, thorough, and precise. Decision science is the subject that deals with such problems. It provides tools that make data-driven decisions. Multi-Criteria Decision Making (MCDM) is one of the popular decision-making approaches. It allows the decision maker to obtain an optimal solution considering multiple conflicting factors simultaneously. Analytical Hierarchy Process (AHP), Data Envelopment Analysis (DEA), ÉLimination et Choix Traduisant la REalité (ELECTRE), Vlsekriterijumska Optimizacija I Kompromisno Resenje (VIKOR), TOPSIS, Multi Attribute Utility Theory (MAUT), Fuzzy Set Theory, Goal Programming, Preference Ranking Organization Method for Enrichment Evaluation (PROMETHEE) are some of the commonly used MCDM techniques [6].

The current work uses TOPSIS in combination with Intuitionistic Fuzzy Set to obtain a ranking for the vulnerability scanners. TOPSIS was proposed by Hwang and Yoon [7]. It determines a positive ideal solution and negative ideal solution and then using different distance measures, determines the optimal solution to be the one with the least distance from the positive ideal solution and farthest from the negative ideal solution. The intuitionistic fuzzy set is an extension of the set theory provided by Georg Cantor in the late 1700 s. Intuitionistic Fuzzy Set Theory was proposed by Krassimir Atanassov in 1983 [8]. According to the classical set theory, an element either belongs to a set or doesn't. But this theory was not able to cater to the uncertainty involved in many real-life situations. The Intuitionistic Fuzzy Set Theory allowed for a third component which deals with uncertainty. Hence, the set describes the membership function, a non-membership function, and a hesitation function. IFS TOPSIS uses intuitionistic fuzzy set in TOPSIS method to define a real-life situation.

A brief literature review has been provided in the following Section 2. Section 3 first discusses the methodology of IFS TOPSIS and is followed by a detailed description of the problem in the context of vulnerability scanners. Section 4 discusses a particular case for ranking a few vulnerability scanners. The results have been discussed in Section 5 while Section 6 concludes the work and is followed by a reference list.

2 Literature Review

Many vulnerability discovery models have been proposed by researchers which have contributed to vulnerability management literature. These models validated the vulnerability data based on their discovery timeline and then can be used to predict the future vulnerabilities to be discovered [9–18].

Some works have proposed vulnerability correction through patch management [19–23]. Researchers have also proposed vulnerability scoring and assessment techniques [24–27].

In contrast to the available mathematical models, software developers have worked on the development of various vulnerability scanning software that can ease the discovery process by just checking the source code or byte code in predeveloped software. Vulnerability Scanning Tools (VST) are automated tools that inspect various types of software vulnerabilities present in a web application and network. Fonseca et al. have compared the capability of various vulnerability scanners in detecting SQL injection and Cross-Site Scripting Vulnerabilities [28]. Bau et al. assessed the performance of various black box vulnerability scanners [29]. Holm et al. have evaluated the effectiveness of various vulnerability scanners [30]. Daud et al. have discussed a case study on the web application scanner tools used in their company [31]. Makino and Klyuev evaluated the performance of two vulnerability scanners, OWASP ZAP and Skipfish [32]. Alsaleh et al. performed a comparative analysis to assess open-source vulnerability scanners [33]. Esposito et al. proposed a tool JARVIS to enhance the performance of existing vulnerability scanners [34]. Rennhard et al. proposed a tool JARVIS to overcome the limitations of currently available vulnerability scanners [35]. As can be seen, the related research content in vulnerability domain contains very less or precisely no work pertaining to vulnerability scanner identification from multi criterion decision making point of view. The present work is an attempt in this very direction.

IFS TOPSIS has been used to propose a ranking technique for vulnerability scanners. TOPSIS is a popularly used MCDM technique with good applications in varied fields. Roszkowska has shown the application of TOPSIS on varied types of input data [36]. Zavadskas et al. have provided a very comprehensive literature review of the use and implementation of the TOPSIS method [37]. Avikal et al. used TOPSIS along with Fuzzy AHP to rank the power supply source for telecom towers [38]. IFS TOPSIS has been also used quite often as a ranking and selection technique. Boran et al. used it for supplier selection in the supply chain [39]. Boran et al. used it for the evaluation of renewable energy techniques [40]. Büyüközkan and Güleryüz used it for smartphone selection [41]. Sachdeva et al. used IFS TOPSIS for the selection of cloud solutions for big data projects [42]. Gupta et al. used it to determine the most important attribute of software quality throughout its lifecycle [43]. Different variants of Intuitionistic fuzzy set have also been used like Shen et al. proposed a different distance measure and also used it for credit risk assessment [44].

The above literature review highlights the gap in the current work done regarding vulnerability scanners. In this respect, an IFS TOPSIS based model has been proposed which will rank the various vulnerability scanners. For this, the methodology has been developed in the following section.

3 Building Block of the Model

3.1 Intuitionistic Fuzzy Set

The intuitionistic fuzzy set M on a set Y is defined as follows:

$$M = \{\langle y, \mu_M(y), v_M(y)\rangle \,|y \in Y\} \tag{1}$$

where] $\mu_M(y) : Y \to [0,1]$ denotes the membership function and $v_M(y) : Y \to [0,1]$ denotes the non-membership function given that:

$$0 \le \mu_M(y) + v_M(y) \le 1 \quad \forall y \in Y \tag{2}$$

The uncertainty or hesitation or non-determinacy of an element $y \in Y$ is given by

$$\pi_M(y) = 1 - \mu_M(y) - v_M(y) \tag{3}$$

$$\text{Also, } 0 \leq \pi_M(y) \leq 1 \quad \forall y \in Y \tag{4}$$

The function $\pi_M(y)$ caters to the uncertainty regarding the membership of y where a smaller value of the function gives us more certainty about y and vice versa. In our problem of determining the best vulnerability scanner, the uncertainty function deals with the uncertainty or incomplete information regarding the responses of the decision makers about the various scanners.

3.2 Intuitionistic Fuzzy Set TOPSIS

The IFS TOPSIS combines the principles of Intuitionistic Fuzzy Set and TOPSIS to create a selection and ranking approach. The methodology of IFS TOPSIS has been provided by Boran et al. [39]. The general steps followed have been enumerated in the following Tab. 1.

Table 1: Methodology of IFS TOPSIS

Steps	Step detail
I	Determine the weights for each decision maker
II	Create the aggregated intuitionistic fuzzy decision matrix
III	Determine the weights of each criterion
IV	Create the aggregated weighted intuitionistic fuzzy decision matrix
V	Determine the distances from the intuitionistic fuzzy positive and negative ideal solution
VI	Calculate the separation measures
VII	Determine the relative proximity coefficient to the intuitionistic ideal solution
VIII	Rank the alternatives

In the current framework, the above-stated methodology has been used to obtain a hierarchical list of the different vulnerability scanners available in the market. It can be obtained as follows:

For the current study, let $E = \{E_1, E_2, \ldots, E_m\}$ denote the set of m alternatives i.e., the vulnerability scanners available to the decision makers. According to a list by OWASP, there are more than 60 vulnerability scanners currently available in the market [45]. There are different alternatives available for different platforms, some are commercial while others have a free license. The list has also been segregated on the availability of a free version or not.

Many factors affect the choice of a particular product. For vulnerability scanners, its performance i.e., issue tracking ability, detection rate, type of testing, network scanning ability, ease of use, false positives, price, etc. are crucial factors [3]. In this work, the following seven criteria associated with a good vulnerability scanner have been determined after exhaustive literature review and discussion with security specialists.

Let $Y = \{Y_1, Y_2, \ldots, Y_n\}$ denote the criteria that are used to determine the best vulnerability scanner.

1. *Static application security testing:* The SAST is a testing process that looks at the application from the inside out. It performs an examination of source code, byte code, or application binaries for any sign of vulnerabilities. A scanner that performs efficient SAST testing is considered to be more efficient.
2. *Dynamic application security testing:* The DAST looks at the application from the outside in, by examining it in its running state and trying to manipulate it to discover security vulnerabilities.
3. *Network and Endpoint Security:* It refers to the technologies that are used to keep the network and the devices that connect to the network in secure working order.
4. *Vulnerability Repository/Coverage:* A vulnerability repository represents different types of vulnerabilities a scanning tool may discover.
5. *Ease of Use:* The extent to which software can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.
6. *Detection rate:* It represents how many vulnerabilities did the vulnerability scanners detect in a given time period.
7. *Technological coverage:* It represents multi-language support provided to access the security of applications based on various platforms.

The steps of the algorithm have been discussed below in detail:

Step I. Determine the weights for each decision maker

In each firm, there is a team for software security administration. All decisions regarding the choices of security software like antivirus, vulnerability scanners, firewall, anti-spyware, SaaS security, payment gateway software, etc. are made by the security administrators. Hence, the choice of the vulnerability scanners is made by this team, and they are the decision makers in the current study. Not all members in the team hold equal importance and the value of their opinion may vary due to their knowledge, experience, position, etc. The IFS TOPSIS can cater to this, and weightage is assigned to the opinion of each decision maker in the group. The rating for each decision maker is taken on a linguistic scale and converted into an intuitionistic fuzzy number as shown in Tab. 2.

Table 2: Linguistic terms and their corresponding Intuitionistic fuzzy number for decision maker [39]

Linguistic terms	Intuitionistic fuzzy number
Very important	[0.9, 0.1]
Important	[0.75, 0.2]
Medium	[0.5, 0.45]
Unimportant	[0.35, 0.6]
Very unimportant	[0.1, 0.9]

Let L denote the number of decision makers, then $DM_k = [\mu_k, v_k, \pi_k]$ denotes the intuitionistic fuzzy number for k^{th} decision maker and the corresponding weight can be obtained as:

$$\lambda_k = \left(\frac{\mu_k + \pi_k \left(\frac{\mu_k}{\mu_k + v_k} \right)}{\sum_1^L \left(\mu_k + \pi_k \left(\frac{\mu_k}{\mu_k + v_k} \right) \right)} \right) \text{ and } \sum\nolimits_1^L \lambda_k = 1,\ \lambda_k \in [0, 1] \tag{5}$$

Step II. Create the aggregated intuitionistic fuzzy decision matrix

The linguistic input of the decision makers regarding the various alternatives can be converted into Intuitionistic fuzzy number using Tab. 3. Let $T^k = \left(t_{ij}^k\right)_{m\times n}$ be an intuitionistic fuzzy decision matrix for the k[th] decision maker created on the basis of the inputs given by a decision maker regarding the m alternatives on the n criteria.

Table 3: Linguistic terms and the corresponding intuitionistic fuzzy number to rank the alternatives and create the decision matrix [39]

Linguistic terms	Intuitionistic fuzzy number
Extremely high (EH)	**[1.00, 0.00]**
Very very high (VVH)	**[0.90, 0.10]**
Very high (VH)	**[0.80, 0.10]**
High (H)	**[0.70, 0.20]**
Medium high (MH)	**[0.60, 0.30]**
Medium (M)	**[0.50, 0.40]**
Medium low (ML)	**[0.40, 0.50]**
Low (L)	**[0.25, 0.60]**
Very low (VL)	**[0.10, 0.75]**
Very very low (VVL)	**[0.10, 0.90]**

Let $\lambda = \{\lambda_1, \lambda_2, \ldots, \lambda_L\}$ denote the weights associated with each decision maker. The opinions of all the decision makers needs to be aggregated to obtain a group opinion. Hence, IFWA by Xu [46] has been deployed. Then, $T = \left(t_{ij}\right)_{m\times n}$ such that:

$$t_{ij} = IFWA_{\lambda}\left(t_{ij}^{\ 1}, t_{ij}^{\ 2}, \ldots, t_{ij}^{\ L}\right) \tag{6}$$

$$= \lambda_1 t_{ij}^{\ 1} \oplus \lambda_2 t_{ij}^{\ 2} \oplus \ldots \oplus \lambda_L t_{ij}^{\ L} \tag{7}$$

$$= \left[1 - \prod_{1}^{L}\left(1-\mu_{ij}^k\right)^{\lambda_k}, \prod_{1}^{L}\left(v_{ij}^k\right)^{\lambda_k}, \prod_{1}^{L}\left(1-\mu_{ij}^k\right)^{\lambda_k} - \prod_{1}^{L}\left(v_{ij}^k\right)^{\lambda_k}\right] \tag{8}$$

where $t_{ij} = \left(\mu_{E_i}\left(y_j\right), v_{E_i}\left(y_j\right), \pi_{Ei}\left(y_j\right)\right) \quad (i = 1, 2, \ldots, m); (j = 1, 2, \ldots, n)$.

Hence, the aggregated decision matrix containing the weighted opinions of all the decision makers is:

$$T = \begin{bmatrix} t_{11} & t_{12} & t_{13} & \ldots & t_{1m} \\ t_{21} & t_{22} & t_{23} & \ldots & t_{2m} \\ . & . & . & \ldots & . \\ . & . & . & \ldots & . \\ . & . & . & \ldots & . \\ t_{n1} & t_{n2} & t_{n3} & \ldots & t_{nm} \end{bmatrix} \tag{9}$$

Step III. Determine the weights of each criterion

As is the case with decision makers, all the criteria under consideration may not bear the same level of importance. Let W represent the importance level which is obtained by aggregating the weights assigned by each decision maker. Let $w_j^k = \left[\mu_j^k, v_j^k, \pi_j^k\right]$ be the intuitionistic fuzzy number pertaining

to criteria j assigned by decision maker k. Then, using the IFWA operator, the criteria weight can be obtained as:

$$w_j = IFWA_\lambda\left(w_j^1, w_j^2, \ldots, w_j^L\right) \tag{10}$$

$$= \lambda_1 w_j^1 \oplus \lambda_2 w_j^2 \oplus \ldots \oplus \lambda_L w_j^L \tag{11}$$

$$= \left[1 - \prod_1^L \left(1-\mu_j^k\right)^{\lambda_k}, \prod_1^L \left(v_j^k\right)^{\lambda_k}, \prod_1^L \left(1-\mu_j^k\right)^{\lambda_k} - \prod_1^L \left(v_j^k\right)^{\lambda_k}\right] \tag{12}$$

Hence, the matrix is

$$W = \left[w_1, w_2, \ldots, w_j\right] \tag{13}$$

where $w_j = \left(\mu_j, v_j, \pi_j\right) \quad (j = 1, 2, \ldots, n)$

Step IV. Create the aggregated weighted intuitionistic fuzzy decision matrix

Using the aggregated decision matrix obtained in Step II and weights matrix obtained in Step III, the aggregated weighted intuitionistic fuzzy decision matrix is determined as given by [8] as:

$$T \otimes W = \left\{\left\langle y.\mu_{E_i}(y).\mu_W(y), v_{E_i}(y) + v_W(y) - v_{E_i}(y).v_W(y)\right\rangle | y \in Y\right\} \tag{14}$$

$$\text{And } \pi_{E_i.W}(y) = \left\{1 - v_{E_i}(y) - v_W(y) - \mu_{E_i}(y).\mu_W(y) + v_{E_i}(y).v_W(y)\right\} \tag{15}$$

Thus, the aggregated weighted intuitionistic fuzzy decision matrix is:

$$T' = \begin{bmatrix} t_{11}' & t_{12}' & t_{13}' & \ldots & t_{1m}' \\ t_{21}' & t_{22}' & t_{23}' & \ldots & t_{2m}' \\ . & . & . & \ldots & . \\ . & . & . & \ldots & . \\ . & . & . & \ldots & . \\ t_{n1}' & t_{n2}' & t_{n3}' & \ldots & t_{nm}' \end{bmatrix} \tag{16}$$

where $t_{ij}' = \left(\mu_{ij}', v_{ij}', \pi_{ij}'\right) = \left(\mu_{E_iW}\left(y_j\right), v_{E_iW}\left(y_j\right), \pi_{E_iW}\left(y_j\right)\right)$

Step V. Determine the distances from the intuitionistic fuzzy positive and negative ideal solution

Let J_1 and J_2 be the benefit and cost criteria respectively i.e., a higher value of attributes J_1 is desirable while a lower value of attributes J_2 is appreciated. Let E^+ be the intuitionistic fuzzy positive ideal solution i.e., $E^+ = \left(\mu_{E^+W}\left(y_j\right), v_{E^+W}\left(y_j\right)\right)$ and E^- be the intuitionistic fuzzy negative ideal solution i.e., $E^- = \left(\mu_{E^-W}\left(y_j\right), v_{E^-W}\left(y_j\right)\right)$ where

$$\mu_{E^+W}\left(y_j\right) = \left(\left(\max_i \mu_{E_iW}\left(y_j\right) | j \in J_1\right), \left(\min_i \mu_{E_iW}\left(y_j\right) | j \in J_2\right)\right) \tag{17}$$

$$v_{E^+W}\left(y_j\right) = \left(\left(\min_i v_{E_iW}\left(y_j\right) | j \in J_1\right), \left(\max_i v_{E_iW}\left(y_j\right) | j \in J_2\right)\right) \tag{18}$$

$$\mu_{E^-W}\left(y_j\right) = \left(\left(\min_i \mu_{E_iW}\left(y_j\right) | j \in J_1\right), \left(\max_i \mu_{E_iW}\left(y_j\right) | j \in J_2\right)\right) \tag{19}$$

$$v_{E^-W}\left(y_j\right) = \left(\left(\max_i v_{E_iW}\left(y_j\right) | j \in J_1\right), \left(\min_i v_{E_iW}\left(y_j\right) | j \in J_2\right)\right) \tag{20}$$

Step VI. Calculate the separation measures

The separation measures are obtained using the normalized Euclidean distance as described by [39] as:

$$D^{+} = \sqrt{\frac{1}{2n}\sum_{1}^{n}\left[\left(\mu_{E_iW}\left(y_j\right) - \mu_{E^{+}W}\left(y_j\right)\right)^2 + \left(v_{E_iW}\left(y_j\right) - \mu_{E^{+}W}\left(y_j\right)\right)^2 + \left(\pi_{E_iW}\left(y_j\right) - \pi_{E^{+}W}\left(y_j\right)\right)^2\right]} \tag{21}$$

and

$$D^{-} = \sqrt{\frac{1}{2n}\sum_{1}^{n}\left[\left(\mu_{E_iW}\left(y_j\right) - \mu_{E^{-}W}\left(y_j\right)\right)^2 + \left(v_{E_iW}\left(y_j\right) - \mu_{E^{-}W}\left(y_j\right)\right)^2 + \left(\pi_{E_iW}\left(y_j\right) - \pi_{E^{-}W}\left(y_j\right)\right)^2\right]} \tag{22}$$

where D^{+} denotes the distance from the intuitionistic fuzzy positive ideal solution and D^{-} denotes the distance from the intuitionistic fuzzy negative ideal solution.

Step VII. Determine the relative proximity coefficient to the intuitionistic ideal solution

The relative proximity coefficient of an alternative E_i to the intuitionistic fuzzy positive ideal solution E^{+} is obtained as:

$$P_{i^{+}} = \frac{D_{i^{-}}}{D_{i^{+}} + D_{i^{-}}} \quad where \quad 0 \le P_{i^{+}} \le 1 \tag{23}$$

Step VIII. Rank the alternatives

Using the proximity values obtained in step VII, the alternative with the highest value of $P_{i^{+}}$is given the highest rank, and so on. Thus, the ranking for the various vulnerability scanners is attained.

4 Model Illustration

To demonstrate the working of the above-discussed algorithm, five vulnerability scanners have been considered in the study, namely Nessus, Fsecure Radar, Greenbone, Qualys, and Nexpose. A brief description about them is given below:

Nessus: Nessus is a proprietary vulnerability scanner by Tenable, Inc. and is one of the most popularly used scanners. It has a web interface and a server component that performs the scanning. Firstly, port scanning takes place which detects which hosts are alive and further which ports are open on those hosts. This is followed by service detection which detects which application is running on that port, its name and version number. Then the discovered information is compared with the known vulnerabilities to determine the vulnerability present in the network. Then further probing takes place to identify whether it is a false positive or the vulnerability exists. Nessus is a remote scanning tool and runs numerous checks to detect malicious activity over the network. It covers a wide range of technologies including operating systems, network devices, hypervisors, databases, web servers, and critical infrastructure [4].

Fsecure Radar: Fsecure Radar uses cloud-based management which provides high level automation. It scans the deep web along with the network and its assets. It has built-in features like a security center dashboard, internet asset discovery, discovery scans, vulnerability scans, vulnerability management, etc. The company was founded in 1988 and has received awards for its tool [47].

Greenbone: Greenbone is an open-source solution for vulnerability analysis and management. It identifies security risks in corporate IT, assesses their risk potential and recommends actions. The goal is to prevent attacks by targeting precautionary measures. The company provides a Source Edition, a Professional Edition and Cloud Services [48].

Qualys: Qualys provides products like Qualys Cloud Platform and Cloud Agent. The Qualys Web Application Scanner (WAS) scanner provides deep scans using Simple Object Access Protocol (SOAP) and Representational State Transfer (REST)-based Application Programming Interfaces (APIs). The scanner performs exhaustive testing using DevOps and Agile-based techniques to remove malware and other issues. WAS backed by the Cloud-based Platform and their Web App Firewall allows for comprehensive security solutions [49].

Nexpose: Nexpose is an on-premise vulnerability scanner offered by Rapid 7. The twenty-year-old organization offers many tools, among which the Nexpose can handle vulnerabilities very quickly in a rapidly changing environment. It is considered to be easy to use and points out the areas which need the most attention [50].

The opinions of three decision makers about the above-mentioned vulnerability scanners were collected through a questionnaire. The questionnaire was designed in such a way that the input of the decision maker was marked against each criteria's individual importance as well as the importance of the criteria in a particular scanner.

Thus, $m = 5$ denotes the alternatives, $n = 7$ denotes the 7 attributes discussed in the earlier section, and $L = 3$ denotes the 3 decision makers.

Step I. Determine the weights for each decision maker

The weightage assigned to decision makers is shown in the following Tab. 4.

Table 4: Decision maker's weight

Decision maker	Linguistic importance
DM1	Very important
DM2	Important
DM3	Medium

The linguistic terms for each decision maker as shown in Tab. 4 can be converted to intuitionistic fuzzy numbers using Tab. 2. Further, evaluating Eq. (5) gives us the corresponding weights for each decision maker as:

$$\lambda = [0.406176, 0.356295, 0.23753] \tag{24}$$

Step II. Create the aggregated intuitionistic fuzzy decision matrix

The input of each decision maker regarding the various attributes is shown in Tab. 5.

Table 5: Importance of each alternative

Alternative	Criteria	DM1	DM2	DM3
A1	X1	VVH	EH	VH
	X2	VH	VVH	EH
	X3	VVH	VVH	VH
	X4	VH	H	VH

(Continued)

Table 5: Continued

Alternative	Criteria	DM1	DM2	DM3
	X5	VH	VVH	VVH
	X6	VH	VH	VVH
	X7	VH	H	VH
A2	X1	VVH	EH	H
	X2	VH	VH	H
	X3	H	H	VH
	X4	H	H	H
	X5	H	VH	VH
	X6	VH	VH	H
	X7	VH	MH	MH
A3	X1	VVH	VVH	H
	X2	VH	VH	VH
	X3	VH	VVH	H
	X4	H	H	M
	X5	VH	VH	H
	X6	H	MH	VH
	X7	H	VH	H
A4	X1	VVH	EH	VH
	X2	VH	VVH	EH
	X3	VVH	VVH	VH
	X4	VH	VH	VH
	X5	EH	EH	VH
	X6	VVH	VVH	VVH
	X7	EH	VVH	VVH
A5	X1	VVH	EH	VH
	X2	VH	EH	VH
	X3	EH	VH	VH
	X4	VH	VVH	MH
	X5	EH	EH	VVH
	X6	VVH	VVH	VH
	X7	VH	VH	H

Using the inputs from Tab. 5 and evaluating Eqs. (6)–(8), the aggregated intuitionistic fuzzy decision matrix is obtained as:

$$T = \begin{bmatrix} (1,0,0) & (1,0,0) & (0.882,0.1,0.018) & (0.769,0.128,0.103) & (0.867,0.1,0.033) & (0.830,0.1,0.07) & (0.769,0.128,0.103) \\ (1,0,0) & (0.78,0.118,0.102) & (0.728,0.17,0.103) & (0.7,0.2,0.1) & (0.764,0.133,0.103) & (0.78,0.118,0.102) & (0.698,0.192,0.110) \\ (0.87,0.118,0.012) & (0.8,0.1,0.1) & (0.828,0.118,0.054) & (0.661,0.236,0.103) & (0.78,0.118,0.102) & (0.698,0.196,0.106) & (0.74,0.156,0.103) \\ (1,0,0) & (1,0,0) & (0.882,0.1,0.018) & (0.8,0.1,0.1) & (1,0,0) & (0.9,0.1,0) & (1,0,0) \\ (1,0,0) & (1,0,0) & (1,0,0) & (0.816,0.13,0.054) & (1,0,0) & (0.882,0.1,0.018) & (0.78,0.118,0.102) \end{bmatrix}$$

Step III: Determine the weights of each criterion

To determine the importance of each criterion, the input of each decision maker was taken (Tab. 6) and an aggregated importance matrix was created with the use of Eqs. (10)–(12).

Table 6: Importance of each criterion

Criteria	DM1	DM2	DM3
X1	I	I	M
X2	I	M	I
X3	VI	VI	I
X4	M	I	M
X5	VI	VI	I
X6	I	I	VI
X7	M	M	I

Thus, the weight matrix W is:

$$W = [(0.719, 0.018, 0.263)\ (0.719, 0.018, 0.263)\ (0.393, 0.002, 0.606)\ (0.813, 0.041, 0.147)\ (0.393, 0.002, 0.606)\ (0.494, 0.004, 0.502)\ (0.813, 0.041, 0.147)]$$

Step IV: Create the aggregated weighted intuitionistic fuzzy decision matrix

The aggregated weighted intuitionistic fuzzy decision matrix is obtained using Eqs. (14)–(16) as:

$$T' = \begin{bmatrix} (0.719, 0.018, 0.263) & (0.719, 0.018, 0.263) & (0.346, 0.102, 0.552) & (0.625, 0.163, 0.212) & (0.34, 0.102, 0.558) & (0.41, 0.104, 0.486) & (0.625, 0.163, 0.212) \\ (0.719, 0.018, 0.263) & (0.56, 0.134, 0.306) & (0.286, 0.171, 0.543) & (0.569, 0.232, 0.199) & (0.3, 0.134, 0.566) & (0.385, 0.121, 0.494) & (0.567, 0.225, 0.208) \\ (0.625, 0.134, 0.241) & (0.575, 0.116, 0.309) & (0.325, 0.12, 0.555) & (0.537, 0.267, 0.196) & (0.306, 0.12, 0.574) & (0.345, 0.199, 0.456) & (0.602, 0.19, 0.208) \\ (0.719, 0.018, 0.263) & (0.719, 0.018, 0.263) & (0.346, 0.102, 0.552) & (0.65, 0.136, 0.214) & (0.393, 0.002, 0.606) & (0.444, 0.104, 0.452) & (0.813, 0.041, 0.147) \\ (0.719, 0.018, 0.263) & (0.719, 0.018, 0.263) & (0.393, 0.002, 0.606) & (0.663, 0.165, 0.172) & (0.393, 0.002, 0.606) & (0.436, 0.104, 0.461) & (0.634, 0.154, 0.213) \end{bmatrix}$$

Step V: Determine the distances from the intuitionistic fuzzy positive and negative ideal solution

The intuitionistic fuzzy positive ideal and intuitionistic fuzzy negative ideal solution have been obtained here with the help of Eqs. (17)–(20).

The intuitionistic fuzzy positive ideal solution obtain is:

$$E^{+} = \{(0.719, 0.018, 0.263)\ , (0.719, 0.018, 0.263)\ , (0.393, 0.002, 0.606)\ , (0.663, 0.165, 0.172)\ ,$$
$$(0.393, 0.002, 0.606)\ , (0.444, 0.104, 0.452)\ , (0.813, 0.041, 0.147)\}$$

And the intuitionistic fuzzy negative ideal solution is:

$$E^{-} = \{(0.625, 0.134, 0.241)\ , (0.56, 0.134, 0.306)\ , (0.286, 0.171, 0.543)\ , (0.537, 0.267, 0.196)\ ,$$
$$(0.3, 0.134, 0.566)\ , (0.345, 0.199, 0.456)\ , (0.567, 0.225, 0.208)\}$$

Step VI: Calculate the separation measures

The separation measures can be obtained using Eqs. (21)–(22) and the values are shown in following Tab. 7:

Table 7: Separation measures for the alternatives

Alternative/separation measure	D^{+}	D^{-}
E1	0.080123	0.090334
E2	0.127998	0.049189

(Continued)

Table 7: Continued

Alternative/separation measure	D^+	D^-
E3	0.123829	0.023261
E4	0.035525	0.132556
E5	0.059341	0.115901

Step VII: Determine the relative proximity coefficient to the intuitionistic ideal solution

The relative proximity P_{i+} is shown in the second row of Tab. 8.

Table 8: Ranking and proximity co-efficient of the alternatives

Alternative	E1	E2	E3	E4	E5
P_{i+}	0.529952	0.2776103	0.158143	0.788646	0.661377
Rank	3	4	5	1	2
Product name	Nessus	Fsecure radar	Greenbone	Qualys	Nexpose

Step VIII: Rank the alternatives

Since the proximity coefficient is highest for Qualys, it is ranked as the best and is followed by Nexpose and Nessus.

Thus, a ranking for the five considered alternatives based on the opinion of the expert group could be obtained.

5 Discussion

5.1 Research Contribution

As can be seen from the results obtained in the earlier section, a comprehensive ranking of the considered scanners could be obtained. IFS TOPSIS was able to consider the opinions of various decision makers and obtain a collective decision. The relative importance of each decision maker was also given relevant weightage. The technique was further able to consider various attributes and consider their relative importance. According to the results obtained here, Qualys is the best vulnerability scanner followed by Nexpose, Nessus, Fsecure Radar and Greenbone. This contrasts with the report discussed earlier wherein Nessus topped the list and was followed by Qualys. This shows that the results can vary as per the attributes under consideration and hence a mathematical model is a better fit in such a situation.

5.2 Limitations and Future Research Directions

The current analysis has been carried out based on the inputs received from three decision makers who have worked on multiple vulnerability scanners. The decision makers were asked to express their views regarding five vulnerability scanners. The number of decision makers is usually considered small in such group-based decision-making approaches. The number of products analyzed can be extended depending on the problem under consideration. It can be further seen that the results obtained here are based on the opinion of the decision makers. Different views of the decision makers or the administrators might lead to a different outcome. Hence, this research work is scale-independent and

can be implemented by a single firm, by a group of organizations, or by the whole software industry to determine the benchmark. Detailed enumeration of the steps with discussions will facilitate the easy application to the problem and hence obtain a tailor-fit solution each time. The technique can also be used to analyze and rank other aspects of vulnerability management and improve software security.

6 Conclusion

Security is a major concern for any software whether it is an application, an operating system, or a network. Vulnerabilities crop up in software when there are loopholes and can be exploited for wrongful gains. Vulnerability Scanning Software help in detecting vulnerabilities automatically in a web-based application and network. But due to the numerous vulnerability scanners available in the market, each with its unique features, choosing the right scanner becomes a precarious decision. For this, a multi-criteria group decision making approach i.e., Intuitionistic Fuzzy Set TOPSIS has been used to select the best scanner and also provide a ranking to different scanners. To assess the vulnerability scanner, the study identified seven parameters whose presence is essential in good quality software. A highlighting feature of IFS TOPSIS is that it can cater to different importance assigned to different things in a group and yet make a group decision. Different members of the decision-making group can hold varying levels of importance. Similarly, the criteria of judging a scanner can hold a varying level of importance for a particular firm/individual or in a particular scanner. This group decision making approach can combine the varying perspectives and present a joint outcome. To demonstrate the working of the discussed technique, the analysis was carried out on five vulnerability scanners based on inputs from a group of three decision makers. The technique was able to successfully rank the scanners.

Acknowledgement: The authors would like to thank Mr. Lokesh Tiwari, Information Security Engineer at Intel Tech. India Private Limited, Bangalore, India; and his team members who helped us in filling questionnaire regarding our study.

Funding Statement: The authors received no specific funding for this study.

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

References

[1] S. Carielli, A. DeMartine, M. Bongarzone and P. Dostie, "The state of application security," 2020. [Online] Available: https://www.forrester.com/report/The+State+Of+Application+Security+2020/-/E-RES159057, (Accessed 5 November 2021).

[2] Gartner, Gartner Peer Insights "Voice of the customer: Vulnerability assessment," 2021. [Online] Available: https://www.gartner.com/en/documents/4008853-gartner-peer-insights-voice-of-the-customer-vulnerability-assessment, (Accessed 10 December 2021).

[3] G2 business software and reviews, compare BurpSuite, IBM security QRadar, and Nessus, 2022. [Online] Available: https://www.g2.com/compare/burpsuite-vs-ibm-security-qradar-vs-nessus, (Accessed 2 November 2021).

[4] Nessus, 2022. [Online] Available: https://www.tenable.com/products/nessus/nessus-professional, (Accessed 5 November 2021).

[5] Tenable, Cybersecurity insiders 2018 application security report, 2018. [Online] Available: https://www.tenable.com/whitepapers/cybersecurity-insiders-2018-application-security-report, 2022 (Accessed 5 November 2021).

[6] A. Mardani, A. Jusoh, K. Nor, Z. Khalifah, N. Zakwan *et al.,* "Multiple criteria decision-making techniques and their applications–a review of the literature from 2000 to 2014." *Economic Research-Ekonomska Istraživanja*, vol. 28, no. 1, pp. 516–571, 2015.
[7] C. L. Hwang and K. Yoon, "Methods for multiple attribute decision making," in *Multiple Attribute Decision Making-Methods and Applications: A State-of-the-Art Survey*, 1st ed. Berlin, Heidelberg: Springer, pp. 58–191, 1981.
[8] K. T. Atanassov, "Intuitionistic fuzzy sets," VII ITKR session, Sofia, 20-23 June 1983, deposed in centr. Sci.-Techn. library of the Bulgarian academy of science, 1697/84. *Reprinted: International Journal of Bioautomation*, vol. 20, no. S1, pp. S1–S6, 2016.
[9] S. W. Woo, O. H. Alhazmi and Y. K. Malaiya, "An analysis of the vulnerability discovery process in web browsers," in *Proc. of 10th Int. Association of Science and Technology for Development: Software Engineering and Applications (IASTED SEA)*, Dallas, TX, USA, pp. 13–15, 2006.
[10] O. H. Alhazmi, Y. K. Malaiya and I. Ray, "Measuring, analyzing, and predicting security vulnerabilities in software systems," *Computers & Security*, vol. 26, no. 3, pp. 219–228, 2007.
[11] O. H. Alhazmi and Y. K. Malaiya, "Application of vulnerability discovery models to major operating systems," *IEEE Transactions on Reliability*, vol. 57, no. 1, pp. 14–22, 2008.
[12] A. Anand, P. Gupta, Y. Klochkov and V. S. S. Yadavalli, "Modeling software fault removal and vulnerability detection and related patch release policy," in *System Reliability Management: Solutions and Technologies*, 1st ed. CRC Press, pp. 19, 2018.
[13] N. Bhatt, A. Anand, V. S. S. Yadavalli and V. Kumar, "Modeling and characterizing software vulnerabilities," *International Journal of Mathematical, Engineering and Management Sciences*, vol. 2, no. 4, pp. 288–299, 2017.
[14] N. Bhatt, A. Anand and V. S. S. Yadavalli, "Exploitability prediction of software vulnerabilities," *Quality and Reliability Engineering International*, vol. 37, no. 2, pp. 648–663, 2020.
[15] A., Anand, N. Bhatt and O. H. Alhazmi, "Modeling software vulnerability discovery process inculcating the impact of reporters," *Information Systems Frontiers*, vol. 23, no. 3, pp. 709–722, 2021.
[16] M. A. Williams, R. C. Barranco, S. M. Naim, S. Dey, M. S. Hossain *et al.,* "Vulnerability analysis and prediction framework," *Computers & Security*, vol. 92, pp. 101751, 2020.
[17] E. Yasasin, J. Prester, G. Wagner and G. Schryen, "Forecasting IT security vulnerabilities–an empirical analysis," *Computers & Security*, vol. 88, pp. 101610, 2020.
[18] A. Anand, N. Bhatt, J. Kaur and Y. Tamura, "Time lag-based modelling for software vulnerability exploitation process," *Journal of Cyber Security and Mobility*, vol. 10, no. 4, pp. 663–678, 2021.
[19] A. Anand, M. Agrawal, N. Bhatt and M. Ram, "Software patch scheduling policy incorporating functional safety standards," in *Advances in System Reliability Engineering*, Academic Press, USA, pp. 267–279, 2019.
[20] F. D. Nembhard, M. M. Carvalho and T. C. Eskridge, "Towards the application of recommender systems to secure coding," *European Association for Signal Processing (EURASIP) Journal on Information Security*, vol. 24, no. 1, pp. 267–279, 2019.
[21] A. Anand, N. Bhatt and D. Aggrawal, "Modeling software patch management based on vulnerabilities discovered," *International Journal of Reliability, Quality and Safety Engineering*, vol. 27, no. 2, pp. 2040003, 2020.
[22] A. Anand, J. Kaur, A. A. Gokhale and M. Ram, "Impact of available resources on software patch management," in *Systems Performance Modeling*, vol. 4, Walter de Gruyter GmbH & Co KG, pp. 1–11, 2020.
[23] J. Kaur, A. Anand and O. Singh, "Modeling software vulnerability correction/fixation process incorporating time lag," in *Recent Advancements in Software Reliability Assurance*, Boca Raton, FL: CRC Press, pp. 39–58, 2019.
[24] G. Spanos, A. Sioziou and L. Angelis, "WIVSS: A new methodology for scoring information systems vulnerabilities," in *Proc. of 17th Panhellenic Conf. on Informatics*, Thessaloniki, Greece, pp. 83–90, 2013.
[25] G. Spanos and L. Angelis, "Impact metrics of security vulnerabilities: Analysis and weighing," *Information Security Journal: A Global Perspective*, vol. 24, no. 1-3, pp. 57–71, 2015.

[26] S. Khan and S. Parkinson, "Review into state of the art of vulnerability assessment using Artificial Intelligence," in *Guide to Vulnerability Analysis for Computer Networks and Systems*, Cham, Springer, pp. 3–32, 2018.
[27] X. Tian and D. Tang, "A distributed vulnerability scanning on machine learning," in *Proc. of 6th Int. Conf. on Information Science and Control Engineering (ICISCE)*, IEEE, Shanghai, China, pp. 32–35, 2019.
[28] J. Fonseca, M. Vieira and H. Madeira, "Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks," in *Proc. of 13th Pacific Rim Int. Symposium on Dependable Computing (PRDC 2007)*, IEEE, Melbourne, VIC, Australia, pp. 365–372, 2007.
[29] J. Bau, E. Bursztein, D. Gupta and J. Mitchell, "State of the art: automated black-box web application vulnerability testing," in *Proc. IEEE Symposium on Security and Privacy*, Oakland, California, USA, pp. 332–345, 2010.
[30] H. Holm, T. Sommestad, J. Almroth and M. Persson, "A quantitative evaluation of vulnerability scanning," *Information Management & Computer Security*, vol. 19, no. 4, pp. 231–247, 2011.
[31] N. I. Daud, K. A. A. Bakar and M. S. M. Hasan, "A case study on web application vulnerability scanning tools," in *Proc. Science and Information Conf.*, London, UK, pp. 595–600, 2014.
[32] Y. Makino and V. Klyuev, "Evaluation of web vulnerability scanners.," in *Proc. Int. Conf. on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, Warsaw, Poland, pp. 399–402, 2015.
[33] M. Alsaleh, N. Alomar, M. Alshreef, A. Alarifi and A. Al-Salman, "Performance-based comparative assessment of open-source web vulnerability scanners," *Security and Communication Networks*, Article ID: 6158107, 2017.
[34] D. Esposito, M. Rennhard, L. Ruf and A. Wagner, "Exploiting the potential of web application vulnerability scanning," in *Proc. Int. Conf. on Internet Monitoring and Protection*, Barcelona, Spain, pp. 22–29, 2018.
[35] M. Rennhard, D. Esposito, L. Ruf and A. Wagner, "Improving the effectiveness of web application vulnerability scanning," *International Journal on Advances in Internet Technology*, vol. 12, no. 1/2, pp. 12–27, 2019.
[36] E. Roszkowska, "Multi-criteria decision-making models by applying the TOPSIS method to crisp and interval data," *Multiple Criteria Decision Making/University of Economics in Katowice*, vol. 6, pp. 200–230, 2011.
[37] E. K. Zavadskas, A. Mardani, Z. Turskis, A. Jusoh and K. M. Nor, "Development of TOPSIS method to solve complicated decision-making problems - An overview on developments from 2000 to 2015," *International Journal of Information Technology & Decision Making*, vol. 15, no. 3, pp. 645–682, 2016.
[38] S. Avikal, R. Singhal, R. Sajwan, R. K. Tiwari and R. Singh, "Selection of best power supply source for telecom towers in remote areas," *International Journal of Mathematical, Engineering and Management Sciences*, vol. 5, no. 5, pp. 913–925, 2020.
[39] F. E. Boran, S. Genç, M. Kurt and D. Akay, "A Multi-criteria intuitionistic fuzzy group decision making for supplier selection with TOPSIS method," *Expert Systems with Applications*, vol. 36, no. 8, pp. 11363–11368, 2009.
[40] F. E. Boran, K. Boran and T. Menlik, "The evaluation of renewable energy technologies for electricity generation in Turkey using intuitionistic fuzzy TOPSIS," *Energy Sources, Part B: Economics, Planning, and Policy*, vol. 7, no. 1, pp. 81–90, 2012.
[41] G. Büyüközkan and S. Güleryüz, "Multi criteria group decision making approach for smart phone selection using intuitionistic fuzzy TOPSIS," *International Journal of Computational Intelligence Systems*, vol. 9, no. 4, pp. 709–725, 2016.
[42] N. Sachdeva, O. Singh, P. K. Kapur and D. Galar, "Multi-criteria intuitionistic fuzzy group decision analysis with TOPSIS method for selecting appropriate cloud solution to manage big data projects," *International Journal of System Assurance Engineering and Management*, vol. 7, no. 3, pp. 316–324, 2016.
[43] P. Gupta, A. Anand and M. Ram, "Reliability as key software quality metric: A multi-criterion intuitionistic fuzzy-TOPSIS based analysis," *International Journal of Reliability, Quality and Safety Engineering*, vol. 28, no. 6, pp. 2140003, 2021.

[44] F. Shen, X. Ma, Z. Li, Z. Xu and D. Cai, "An extended intuitionistic fuzzy TOPSIS method based on a new distance measure with an application to credit risk evaluation," *Information Sciences*, vol. 428, pp. 105–119, 2018.
[45] OWASP, 2022. [Online] Available: https://owasp.org/www-community/Vulnerability_Scanning_Tools, (Accessed 5 November 2021).
[46] Z. Xu, "Intuitionistic fuzzy aggregation operators," *IEEE Transactions on Fuzzy Systems*, vol. 15, no. 6, pp. 1179–1187, 2007.
[47] FSECURE, 2022. [Online] Available: https://www.f-secure.com/en, (Accessed 5 November 2021).
[48] Greenbone, 2022. [Online] Available: https://www.greenbone.net/, (Accessed 5 November 2021).
[49] Qualys, 2022. [Online] Available: https://www.qualys.com, (Accessed 5 November 2021).
[50] Rapid7, [Online] Available: https://www.rapid7.com/products/nexpose/. (Accessed 5 November 2021).