

Article

Effectiveness Evaluation of Different IDSs Using Integrated Fuzzy MCDM Model

Hashem Alyami ¹, Md Tarique Jamal Ansari ², Abdullah Alharbi ³, Wael Alosaimi ³, Majid Alshammari ³, Dhirendra Pandey ², Alka Agrawal ², Rajeev Kumar ⁴ and Raees Ahmad Khan ^{2,*}

¹ Department of Computer Science, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; hyami@tu.edu.sa

² Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow 226025, Uttar Pradesh, India; tjtjansari@gmail.com (M.T.J.A.); prof.dhiren@gmail.com (D.P.); alka_csjmu@yahoo.co.in (A.A.)

³ Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; amharbi@tu.edu.sa (A.A.); w.osaimi@tu.edu.sa (W.A.); m.alshammari@tu.edu.sa (M.A.)

⁴ Department of Computer Science and Engineering, Babu Banarasi Das University, Lucknow 226028, Uttar Pradesh, India; rs0414@gmail.com

* Correspondence: khanraees@yahoo.com



Citation: Alyami, H.; Ansari, M.T.J.; Alharbi, A.; Alosaimi, W.; Alshammari, M.; Pandey, D.; Agrawal, A.; Kumar, R.; Khan, R.A. Effectiveness Evaluation of Different IDSs Using Integrated Fuzzy MCDM Model. *Electronics* **2022**, *11*, 859. <https://doi.org/10.3390/electronics11060859>

Academic Editors: Stavros Shiaeles, Bogdan Ghita and Nicholas Kolokotronis

Received: 3 February 2022

Accepted: 7 March 2022

Published: 9 March 2022

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



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Abstract: Cyber-attacks are becoming progressively complicated; hence, the functional issues of intrusion-detection systems (IDSs) present ever-growing challenges. Failing to detect intrusions may jeopardize the trustworthiness of security services, such as privacy preservation, authenticity, and accessibility. To fight these risks, different organizations nowadays use a variety of approaches, techniques, and technologies to safeguard the systems' credibility. Establishing policies and procedures, raising user awareness, implementing firewall and verification systems, controlling system access, and building computer-issue management groups are all examples of safeguarding methods. There is a lack of sufficient emphasis on the effectiveness of intrusion-detection systems. In enterprises, IDS is used to analyze the potentially dangerous activities taking place within the technological settings. The selection of efficient IDS is a challenging task for organizations. This research evaluates the impact of five popular IDSs for their efficiency and effectiveness in information security. The authors used the fuzzy analytical hierarchy process (AHP) and fuzzy technique for order performance by similarity to ideal solution (TOPSIS)-based integrated multi-criteria decision-making (MCDM) methodology to evaluate the efficacy of the popular IDSs. The findings of this research suggest that most of the IDSs appear to be highly potential tools. Even though Snort is extensively deployed, Suricata has a substantial advantage over Snort. Suricata uses multi-threading functionality in comparison to Snort to boost the processing performance.

Keywords: intrusion-detection systems; threat; cyber-attacks; MCDM; fuzzy logic

1. Introduction

Communication networks are an integral part of our lives in the digital age. They are a privilege to the digital world. They introduce the rest of the world relatively close to all of us. The challenge of intrusion became much more prevalent with the network. Hackers are always present in the virtual environment. Business organizations could be vulnerable to cyber-attacks. It is necessary to take significant action to analyze network attacks and return them to normal. As a result, intrusion-detection systems (IDS) are important in a network security solution. IDS is a solution that detects network attacks. IDS assists anyone in detecting network traffic. IDS can further initiate an immediate alert. This will assist the IT workforce in dealing with such challenges. However, it would not stop a threat from impacting system applications. It analyzes daily network activities by using

the guidelines. The security management system receives an alert through IDS in case any malicious activity is detected over the network. As a result, it is easier for the security expert to identify such suspected activities. The traffic information is moved in bulk and then analyzed for any unusual behavior in the data. The team explores threats by using known attack signatures, as well as trends [1–6].

IDS is a mechanism that detects discrepancies in capturing attackers before they cause serious damage to the network system. On the user's computer, a host-based IDS is installed. The network is monitored by a network-based IDS. During the normal assignment, IDSs search for signatures from attack patterns. These abnormalities are reported to the knowledge base and, after that, analyzed at the guidelines and application layers based on the policy and procedures. IDS could be used as software or as a network security device. Since the IDSs only need to identify the risks, these systems are positioned outside of band on the communications infrastructure, indicating that the transmitter and the recipient of data do not communicate in real-time. IDS systems commonly use a Test Access Point (TAP) or Switch Port Analyzer (SPAN) port for the analysis of a copy of the Inline Traffic Stream, so that IDS does not affect the performance of the Inline Network. This has been established initially by IDS, since the required intrusion analysis at the time cannot be conducted at a pace that is consistent with the elements on the network infrastructure's direct communication line [7–10]. Figure 1 shows the general architecture of IDS.

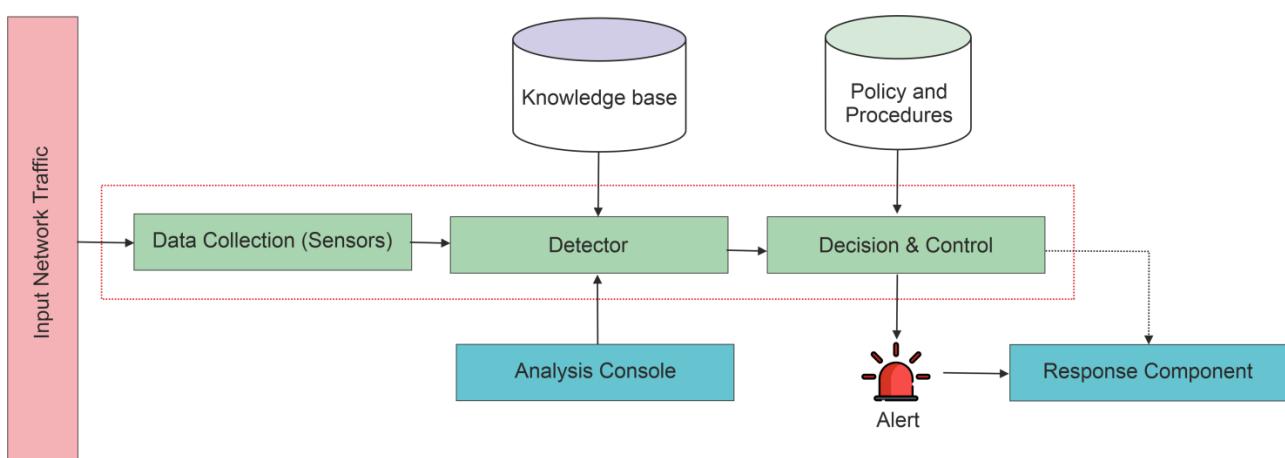


Figure 1. General architecture of intrusion-detection system (IDS).

An efficient IDS and mitigation systems are important for an organization's normal system functioning. Traditional defense technology has become increasingly inefficient as a result of attacker tactics, such as obfuscation techniques, metamorphism, and polymorphism, which increase malware's resistance. Discrepancies are detected by the IDSs to capture attackers that can cause significant harm to the organization. They could be a network or even a host. Due to new attacks developing almost daily, IDSs are crucial in identifying and responding to potential system intrusions. IDSs should change and continually adjust to all of these new threats and assault techniques. The challenge on which scholars have been researching for decades is how to construct effective, efficient, and responsive IDSs [11–15].

The evaluation of IDSs is a popular and challenging task in research at present. Choosing an efficient IDS to secure a business network must not be undertaken lightly, rapidly, or without a thorough grasp of the technology, solutions, and potential consequences. The decision-making process can be broken down into several stages, which include determining the requirement, gaining a broad awareness of IDSs, more in-depth knowledge of the network, and also determining policy and processes by evaluating various IDS solutions [16]. This paper evaluates the effectiveness of different IDSs, using the integrated fuzzy analytical hierarchy process (AHP) technique for order performance by similarity to the ideal solution (TOPSIS) model.

The remainder of this paper is structured as follows: The study outlines relevant research efforts in this domain in Section 2. Section 3 discusses the overview of several types of popular IDSs. Section 4 discusses the integrated fuzzy AHP-TOPSIS technique. Section 5 of this work contains the findings, comparisons of the findings, and a sensitivity analysis. Section 6 closes with the summary and conclusions.

2. Related Research Studies

Upendran and Gopinath [16] proposed an improved entropy-based TOPSIS approach to recommend one or more options from a large set of alternatives. To decrease the number of the network traffic sample, they applied five feature selection strategies. To measure the calculation time, as well as intrusion-detection time, classification techniques, such as Artificial Neural Network (ANN), Naive Bayes, and Support Vector Machine (SVM) are employed. Their suggested TOPSIS approach is used to monitor the effectiveness of feature selection in order to improve intrusion detection.

Hu et al. [17] evaluated two well-known open-source intrusion-detection systems, Snort and Suricata, as well as their comprehensive comparative standards, to develop a better understanding of drop rates, as well as identification efficiency on 100 Gb/s networks. Furthermore, they investigated critical parameters (such as system resource utilization, packet processing power, packet drop frequency, and identification accuracy) which constrain IDSs' application to high-speed networks. Moreover, they also discussed a complete investigation to demonstrate the effectiveness of IDSs utilizing various setups, traffic levels, and flows. They outlined the difficulties of utilizing open-source IDSs in strong networks, offered solutions to assist network managers in addressing identified concerns, and also presented some suggestions for establishing novel IDSs that may be employed in high-speed networking.

Imoize et al. [18] suggested an expansive and cost-based intrusion-detection system. Based on this approach, an objective metric driven by information theory is introduced, and a package for determining the intrusion-detection capabilities of an intrusion-detection system (IDS), given specified input parameters, is constructed in Java. For each operational IDS, the decision-making methodology is applied to evaluate the projected costs and the capacity to detect false-positive rates.

Saber et al. [19] developed a testing method to monitor the effectiveness of the IDS elements and their impacts on the whole system. The assessment is based on several tests. In addition, the effect of the implementation parameters of IDS was studied. They also developed the IDS SNORT on systems with various technical features, and they have constructed a network to produce a series of experiments to evaluate the performance of a higher bandwidth network deployment.

Shiaeles et al. [20] introduced a DDoS detection technique based on developing a fuzzy estimator for the mean packet inter-arrival rate. They separated the task into two concerns: the first was detecting the DDoS incident in progress, and the second was identifying the offender's IP addresses. They set strong real-time limits on the first assignment and more flexible restrictions on address recognition. They also demonstrated through practical assessment that the identification can be accomplished within better real-time restrictions and by utilizing fuzzy estimators rather than crisp statistical classifiers.

Schrötter et al. [21] developed a standard set for assessing intrusion-detection systems in IPv6 settings. This standard is used to compare the popular intrusion-detection systems, such as Snort, Zeek, and Suricata. Furthermore, an IPv6 Plugin Suite was also provided and assessed, which improved Snort by detecting stateful attacks. Their evaluation results indicated the current ability to identify IPv6 connection attacks.

As intrusion-detection systems are particularly built to function on specific systems and situations, they are challenging to implement. Therefore, there is a significant need to evaluate the effectiveness of different IDSs based on their approaches and rules that are present in the most recent version of the IDSs. This fundamental challenge is more succinctly expressed as the intrusion-detection-assessment challenge, and its solution is

typically dependent on a number of parameters in a hierarchical structure. Prior studies, however, suggested that no single model was ideal for all issues. Using a highly integrated fuzzy-based strategy may yield greater results than other approaches. To the extent of our knowledge, our work is the first study that examines several IDSs systematically employing an integrated fuzzy multi-criteria decision-making (MCDM)-based technique. The effectiveness of five major intrusion-detection systems, including Zeek, Suricata, Security Onion, OSSEC, and Snort, is examined in this research. The effectiveness is evaluated by using a hierarchical structure based on the MCDM solution.

3. Different Types of Intrusion-Detection Systems

3.1. Zeek

Zeek [22,23] is a network intrusion-detection system that runs on Unix (IDS). Zeek analyzes network traffic and recognizes intrusion attempts, depending on the type and substance of the traffic. Zeek IDS was previously known as Bro. Zeek identifies intrusions by matching network traffic to rules that describe undesirable events. These rules may define activities (for example, certain hosts interacting to specific services), what actions warrant alerting (for example, attempts to a particular number of distinct hosts constitute a “scan”), or signatures characterizing known attacks or exposure to security issues. If Zeek discovers anything of interest, the direction could be to either write a log entry or run an operating system function. Zeek is designed for high-speed (Gbps) and increased intrusion detection. Zeek IDS can perform competently while operating on commercially accessible PC hardware by intelligently exploiting packet filtering methods, and so can provide an economically efficient way of monitoring a site’s Internet communication.

3.2. Suricata

Suricata was designed in 2010 by the OISF (Open Information Security Foundation), with funding from the US Department of Homeland Security [24]. Suricata’s design is quite close to snort’s, except that, instead of using a single thread to process packets, Suricata uses many threads [25]. This enables Suricata’s distinctive feature, which is to maximize the capacity to obtain packets. Snort was single-threaded; therefore, when packets exceeded the capacity to obtain bandwidth, Snort disregarded them. Thus, multi-threading is a useful capability of Suricata. Suricata has many detection algorithm threads.

3.3. Security Onion

Security Onion [26] is a Linux-based intrusion-detection approach that includes several IDS that are both host-oriented (HIDS) and network-oriented (NIDS). Security Onion can collect and analyze an extensive range of data. This comprises information on the host, connection, session, resource, alerting, and standards. Security Onion can be deployed as a solo implementation with a server and detector, or with a master server and many detectors that allow the platform to be expanded as needed. Numerous gateways and tools are present for system management and information analysis, including Sguil, Snorby, Squert, and Enterprise Log Search and Archive (ELSA). It offers host-based identification in the form of OSSEC HIDS, as well as network-based detection via Snort, Suricata, and Zeek NIDS. Security Onion is particularly customizable because it may be set as a master server with numerous sensors or as an independent or hybrid installation. The information gathered by Security Onion is saved in log files and also in a Sguil database, which includes a new interface for recording and analysis.

3.4. OSSEC

OSSEC is an open-source intrusion-detection system built by Daniel B. Cid, who sold the product to Trend Micro in 2008 [27]; however, the project remained a free and open source. The most recent stable release is 2.9.3. It is made up of numerous services and modules, each of which has its own distinct set of intrusion-detection capabilities. HIDS has numerous elements, and OSSEC combines them all to provide certain fundamental

advantages. OSSEC ensures that security compliance standards are met. Many consumers, primarily corporate clients, demand that the companies with whom they do business have particular security compliances, including Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and so on. Analyzing logs and evaluating them for suspicious activity is a one-way OSSEC that helps firms comply with various security standards [28].

3.5. Snort

Snort fills an essential “ecological niche” in network security by serving as a cross-platform lightweight network intrusion-detection program that can be used to monitor tiny TCP/IP networks, as well as discover a wide range of abnormal network traffic and also explicit cyberattacks. It can offer controllers adequate information to make informed judgments on how to proceed in the event of suspicious behavior. Snort could also be quickly implemented to cover any gaps in a network’s protection measures, such as when a big threat occurs and corporate security companies take their time releasing new attack identification signatures. Snort is beneficial when it is not cost-effective to install commercial NIDS sensors. Current commercialized intrusion-detection systems cost thousands or tens of thousands, or perhaps even hundreds of thousands of dollars in extreme situations [29,30]. Snort was created to encounter the requirements of a typical compact network intrusion-detection system. It has progressed into a compact, versatile, and high-performing technology that is used on both large and small networks around the globe. It has met its initial design aims and is a perfectly capable solution to corporate intrusion-detection systems in locations where installing standard production systems would be prohibitively expensive.

Table 1 shows the comparison of the five popular intrusion-detection methods.

Table 1. Comparison of the five intrusion-detection methods.

IDS Techniques	Provider	Type	Operating System	License	Network Traffic
Zeek	Vern Paxson	NIDS	Unix/Linux/Mac	BSD License	IPv4
Suricata	OISF	NIDS	Win/Unix/Mac	GNU General Public License (version 2)	IPv4/IPv6
Security Onion	Security Onion Solutions, LLC	NIDS, HIDS	Linux	GNU General Public License (version 2)	IPv4/IPv6
OSSEC	Daniel B. Cid et al.	HIDS	Win/Unix/Linux/Mac	GNU General Public License (version 2)	IPv6
Snort	Cisco System	NIDS	Win/Unix/Linux	GNU General Public License (version 2)	IPv4/IPv6

4. Methods

4.1. Identification of Evaluation Criteria and Alternatives

MCDM is a discipline of combinatorial optimization in which the alternatives are evaluated to identify the best alternative that meets a set of various and frequently contradictory parameters. MCDM is a critical component of the decision-making principle and operational investigation. It is frequently regarded as trustworthy. It is a set of strategies and techniques for integrating various and contradictory parameters into a decision-making process. Furthermore, MCDM might be regarded as a systematic approach for evaluating and selecting between possibilities. It seeks to divide an issue into smaller components, analyze and evaluate each part, and then aggregate those components to determine the

appropriate reasonable alternative from a range of options based on a stated set of parameters. In uncertain, unclear, fuzzy, or risky contexts, MCDM tries to help decision-makers to tackle contradictory real-world statistical and/or qualitative subjective multi-criteria challenges, and to select best-fit options from a group of options. Figure 2 shows the hierarchy for the assessment of some popular intrusion-detection systems (IDS) in this research study. Based on an analysis of the relevant literature, as well as insight from seventy-seven security experts, the four considerable factors at level one, as well associated sub-factors at level two, in the current method that make a significant contribution to the assessment of multiple IDSs were evidently identified and designed. The four main criteria to evaluate the different popular IDSs are Types, Audit source location, Targets, and Protected system denoted as M1, M2, M3, and M4 respectively. The significant criterion Types contain the different types of IDSs. The IDSs may be open-source, closed-source, or freeware, denoted by M11, M12, and M13, respectively. Different IDSs are classified by the type of input data they evaluate at the audit source location. Audit procedures on a host log file, network packets, application log files, or sensor alerts denoted by M21, M22, M23, and M24, respectively, produced by other IDSs can all be used as input data. The targets' criterion shows the IDS capability to detect potential attacks against specific targets. These targets may be application, network, or host, as denoted by M31, M32, and M33, respectively. The protected system criteria show the approach of intrusion detection. It can be HIDS, NIDS, or hybrid types denoted by M41, M42, and M43, respectively. The five alternatives, namely Zeek, Suricata, Security Onion, OSSEC, and Snort, are represented by S1, S2, S3, S4, and S5, respectively.

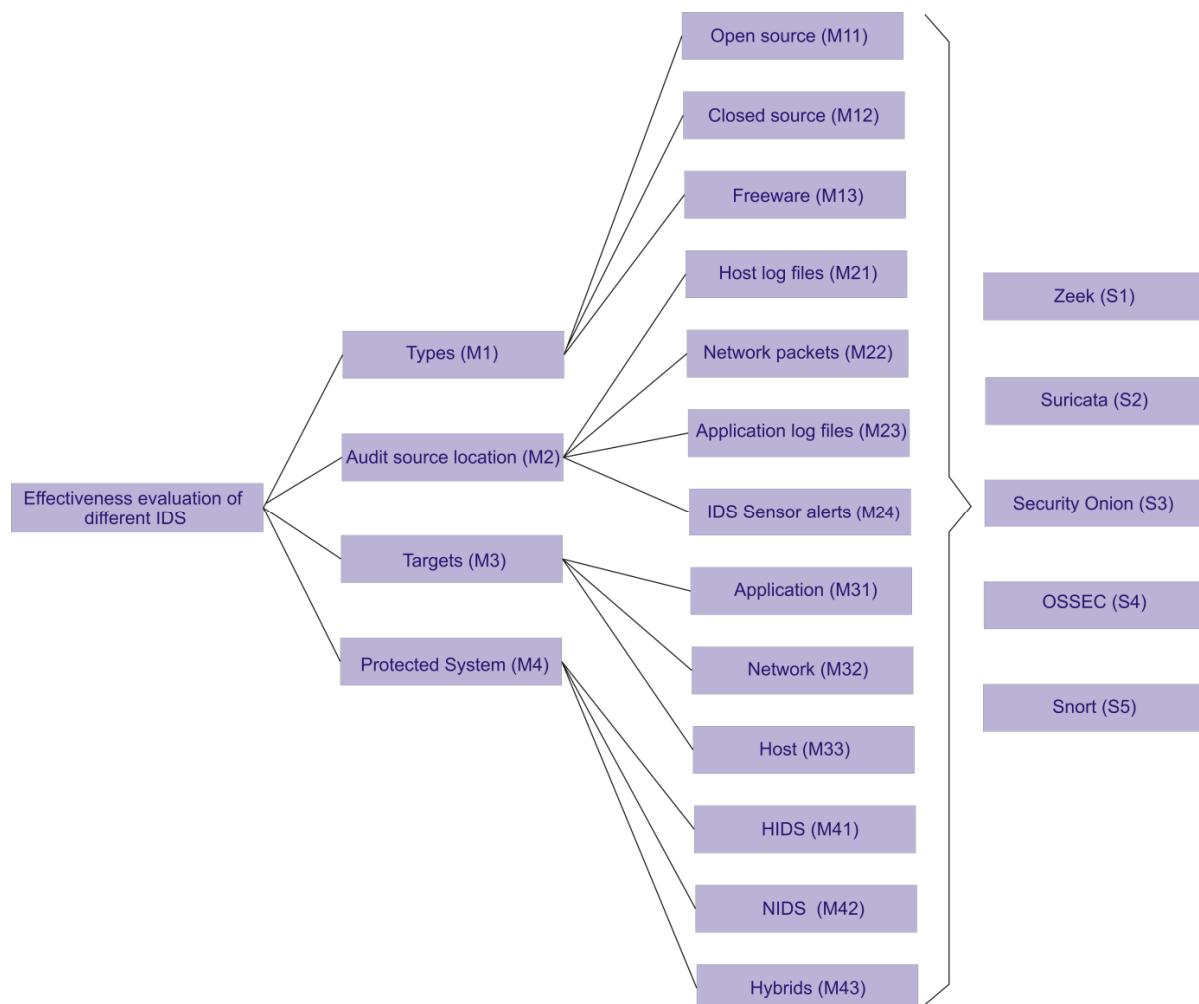


Figure 2. Hierarchy for the effectiveness evaluation of different IDSs.

4.2. Fuzzy AHP-TOPSIS Methodology

Problems with decision-making are likely a consequence of putting too much emphasis on analogical reasoning that has worked previously. When attempting to make a judgment or decision, researchers use a predictive model, which is a heuristic algorithm or guiding principle. These strategies can help in making better decisions by reducing our cognitive strain, and they can also lead to mistakes. However, AHP is unable to resolve the fundamental uncertainty and inaccuracies in a decision-maker's response to genuine statistical information. Because the real world is so indistinct, researchers noted that experts have combined the fuzzy theory with AHP to investigate obscure real-world problems [31–33]. Furthermore, while the AHP method is typically based on a highly volatile scale of decisions, the fuzzy AHP does have deficiencies [23,24]. As a result, a combined AHP and TOPSIS fuzzy method is a special process that could aid in the efficacious evaluation of options. Moreover, the fuzzy AHP-TOPSIS technique is as follows:

Fuzzy AHP: Fuzzy AHP is a popular methodology for resolving difficult selection challenges. Every complicated topic can be investigated by using remarkable categorized ranges of objectives, i.e., hierarchy. With the help of fuzzy AHP, the problem is differentiated into a tree form to describe it. Figure 2 shows how to make a tree shape. This tree shape was created with the help of experts' opinions [34]. The triangular fuzzy number (TFN) is then constructed from the hierarchical structure. A pair-wise comparison of each group of categorized goals is critical because of the impact of one criterion on other criteria.

Transforming linguistic numbers into crisp numbers, as well as TFN, is the next step. The TFN is used in this research, and it ranges from 0 to 1 [35]. The quantitative simplification of TFN membership functions, as well as their capabilities to handle with fuzzy data, is driving this implementation [23]. In addition, linguistic values are categorized as equally important or weakly important, and crisp values are categorized as 1, 2, ..., 9. Furthermore, if the membership functions of a fuzzy number M on F are recognized, it is referred to as TFN:

$$\mu_a(x) = a \rightarrow [0, 1] \quad (1)$$

$$\mu_a(x) = \begin{cases} \frac{x}{mi-l} & x \in [l, mi] \\ \frac{x}{mi-u} & x \in [mi, u] \end{cases} \quad (2)$$

In the triangular membership function, l , mi , and u represent the lower, middle, and upper limits, respectively. A TFN is shown in Figure 3.

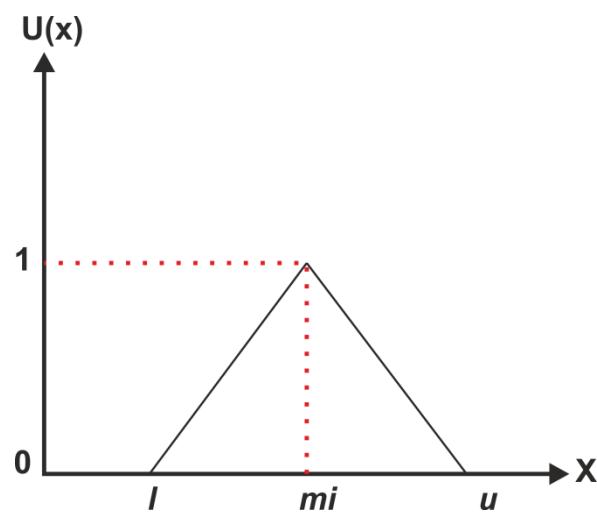


Figure 3. Triangular fuzzy numbers.

A TFN can be written as (l, mi, u) . Specialists assigned numerical scores to the elements that influence the values using a measure that is highlighted in Table 2.

Table 2. TFN scale.

Saaty Scale Definition	Fuzzy Triangle Scale
1	Equally important
3	Weakly important
5	Fairly important
7	Strongly important
9	Absolutely important
2	
4	Intermittent values between two adjacent scales
6	
8	

The numerical methods (3–6) are used to convert numeric values into TFNs that are identified as (l_{ij}, m_{ij}, u_{ij}) , where l_{ij} is lower significance, m_{ij} is middle significance, and u_{ij} is uppermost significance events. Moreover, TFN (Φ_{ij}) is represented as follows:

$$\Phi_{ij} = (l_{ij}, m_{ij}, u_{ij}) \quad (3)$$

where $l_{ij} \leq m_{ij} \leq u_{ij}$

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

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

$$\text{and } u_{ij} = \max(J_{ijd}) \quad (6)$$

In Equations (3)–(6), J_{ijd} specifies the proportional position of the values among two elements that is quantified by specialist d , where i and j indicate a pair of elements being decided by specialists. Φ_{ij} is calculated according to the geometric mean of a specialist's observations for a particular assessment. The geometric mean is capable of appropriately joining and demonstrating the consent of specialists and designates the lowest and highest marks, respectively, for the relative consequence among the two elements. Additionally, Equations (7)–(9) provide the joint TFN values. Take into account the two TFNs, M1 = (l_1, m_{i1}, u_1) and M2 = (l_2, m_{i2}, u_2) . The procedures of actions on them are as follows:

$$(l_1, m_{i1}, u_1) + (l_2, m_{i2}, u_2) = (l_1 + l_2, m_{i1} + m_{i2}, u_2 + u_2) \quad (7)$$

$$(l_1, m_{i1}, u_1) \times (l_2, m_{i2}, u_2) = (l_1 \times l_2, m_{i1} \times m_{i2}, u_1 \times u_2) \quad (8)$$

$$(l_1, m_{i1}, u_1)^{-1} = \left(\frac{1}{u_1}, \frac{1}{m_{i1}}, \frac{1}{l_1} \right) \quad (9)$$

With the support of the equation, a fuzzified pair-wise comparative matrix in the state of $n \times n$ matrix is formed after acquiring the TFN variables for every pair of comparisons (10).

$$\widetilde{A}^d = [\widetilde{k}_{11}^d \widetilde{k}_{12}^d \dots \widetilde{k}_{1n}^d \widetilde{k}_{21}^d \widetilde{k}_{22}^d \dots \widetilde{k}_{2n}^d \dots \dots \dots \widetilde{k}_{n1}^d \widetilde{k}_{n2}^d \dots \widetilde{k}_{nn}^d] \quad (10)$$

where \widetilde{k}_{ij}^d symbolizes the d th decision-makers' priority of the i th standards over the j th criteria. If more than one responsible party is prevalent, the equation is used to calculate the average of every judgment-maker's priorities (11).

$$\widetilde{k}_{ij} = \sum_{d=1}^d \widetilde{k}_{ij}^d \quad (11)$$

The next step is to use the equation to modify the pair-wise comparative matrixes for all elements in the hierarchical order based on the averaged priorities (12).

$$\tilde{A} = \left[\begin{array}{cccccc} \widetilde{k_{11}} & \dots & \widetilde{k_{1n}} & \dots & \ddots & \dots & \widetilde{k_{n1}} & \dots & \widetilde{k_{nn}} \end{array} \right] \quad (12)$$

The fuzzy geometrical mean and fuzzy weights of each element are then described by using the geometrical mean method, as demonstrated in Equation (13).

$$\tilde{p}_i = \left(\prod_{j=1}^n \widetilde{k_{ij}} \right)^{\frac{1}{n}}, i = 1, 2, 3, \dots, n \quad (13)$$

The next step is to use the equation to calculate the identified element's fuzzy weight (14).

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

Equations are also used to determine the average and normalized weight criteria (15–16).

$$M_i = \frac{\tilde{w}_1 \oplus \tilde{w}_2 \dots \oplus \tilde{w}_n}{n} \quad (15)$$

$$Nr_i = \frac{M_i}{M_1 \oplus M_2 \oplus \dots \oplus M_n} \quad (16)$$

Additionally, the Centre of Area (COA) method is used to estimate the BNP (best non-fuzzy performance) number of the fuzzy weights of each quantity with the support of Equation (17).

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

Fuzzy TOPSIS: TOPSIS sees multi-standard decision-making problems, with m options as a geometrical configuration with m points inside the n -dimensional problem area. The strategy used in this article for TOPSIS is principally founded on the notion that a designated possibility is the relatively short and farthest range from the positive-ideal solution, as well as the negative-ideal solution, correspondingly, for best possible and lowest ideal solutions [36]. Specialists have a difficult time assigning a particular performance rating to an alternative based on criteria. TOPSIS uses fuzzy numbers rather than precise numerals to demonstrate the relative importance of criteria in order to be consistent with the actual fuzzy situation. Furthermore, the fuzzy AHP-TOPSIS method is most suitable for handling group decision-making issues in fuzzy settings. The following is the fuzzy AHP-TOPSIS methodology:

The first step is to determine the weights of the evaluation criteria. With the support of equations, this research utilized fuzzy AHP to arrive at fuzzy choice weights (1–16). Moreover, with support of Equation (18), as well as Table 3, the researcher designed the fuzzy decision matrix and selected the best linguistic aspects as criteria possibilities.

$$C_1 \dots C_n \tilde{K} = \begin{matrix} A_1 \\ \dots \\ A_m \end{matrix} \left[\begin{array}{ccc} \tilde{x}_{11} & \dots & \tilde{x}_{1n} \\ \dots & \ddots & \dots \\ \tilde{x}_{m1} & \dots & \tilde{x}_{mn} \end{array} \right] \quad (18)$$

where $\tilde{x}_{ij} = \frac{1}{D} (\tilde{x}_{ij}^1 \dots \oplus \tilde{x}_{ij}^d \oplus \dots \tilde{x}_{ij}^D)$, and \tilde{x}_{ij}^d is the assessment of the alternative A_i in terms of factor C_j effectiveness estimated by the d th specialist, as well as $\tilde{x}_{ij}^d = (l_{ij}^d, m_{ij}^d, u_{ij}^d)$.

Table 3. Linguistic scales for the rating.

Linguistic Variable	Corresponding Triangular Fuzzy Number
Very poor (VP)	(0, 1, 3)
Poor (P)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Good (G)	(5, 7, 9)
Very good (VG)	(7, 9, 10)

The subsequent step is to use an expression to normalize the fuzzy decision matrix (19). The normalized fuzzy assessment matrix denoted by \tilde{P} is represented as follows.

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

After that, using equations, one may complete the normalizing procedure by using Equation (20).

$$\tilde{p}_{ij} = \left(\frac{l_{ij}}{u_j^+}, \frac{m_{ij}}{u_j^+}, \frac{u_{ij}}{u_j^+} \right), u_j^+ = \max\{u_{ij}, i = 1, 2, 3 \dots, n\} \quad (20)$$

Otherwise, we can establish the highest anticipated level, u_j^+ , and $j = 1, 2, \dots, n$ is equivalent to 1; or else, the worst is 0. Furthermore, the normalized \tilde{p}_{ij} remains to be TFNs. For TFNs, the normalization procedure can be achieved in an analogous way. The subjective fuzzy normalized assessment matrix (\tilde{Q}) is measured with the support of Equation (21).

$$\tilde{Q} = [\tilde{q}_{ij}]_{m \times n} \quad i = 1, 2, \dots, m; j = 1, 2, 3 \dots, n \quad (21)$$

where $\tilde{q}_{ij} = \tilde{p}_{ij} \otimes \tilde{w}_{ij}$ also, at that point, describes the Fuzzy Positive-Ideal Solution (FPIS), as well as Fuzzy Negative-Ideal Solution (FNIS). The subjective normalized fuzzy assessment matrix specifies that the components \tilde{q}_{ij} are normalized positive TFN and their choices fit in to the closed interval [0, 1]. Afterward, we can designate the FPIS A^+ (aspiration levels) and FNIS A^- (the worst levels), as presented in Equations (22) and (23).

$$A^+ = (\tilde{q}_1^*, \dots, \tilde{q}_j^*, \dots, \tilde{q}_n^*) \quad (22)$$

$$A^- = (\tilde{q}_1^*, \dots, \tilde{q}_j^*, \dots, \tilde{q}_n^*) \quad (23)$$

where $\tilde{q}_1^* = (1, 1, 1) \otimes \tilde{w}_{ij} = (Lw_j, Mw_j, Hw_j)$ and $\tilde{q}_{ij}^- = (0, 0, 0)$, $j = 1, 2, 3 \dots, n$. For computing the space of every alternative solution from FPIS, as well as FNIS, the spaces (\tilde{d}_i^+ and \tilde{d}_i^-) of every alternative solution from A^+ and A^- can be assessed with the area compensation procedure, as presented in Equations (24) and (25).

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

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

The next stage is to identify the closeness coefficients (absolute gaps' degree) and construct the alternative solutions for achieving the aspiration degrees in each element. Ying-Chyi Chou et al. recommended that $\tilde{C}\tilde{C}_i$ is cleared to estimate the point of the fuzzy gap based on the fuzzy closeness coefficients to increase the alternatives solution [37]. Once the \tilde{d}_i^+ and \tilde{d}_i^- of every alternative solution is assessed, the comparisons to the ideal

clarification are computed. This procedure resolves the equation's similarity to the best choice (26).

$$C\tilde{C}_i = \frac{\tilde{k}_i^-}{\tilde{k}_i^+ + \tilde{k}_i^-} = 1 - \frac{\tilde{k}_i^+}{\tilde{k}_i^+ + k_i^-}, i = 1, 2, \dots, m \quad (26)$$

where $\frac{\tilde{k}_i^-}{\tilde{k}_i^+ + \tilde{k}_i^-}$ is demarcated as the fuzzy satisfaction amount in the i th alternative solution, and $\frac{\tilde{k}_i^+}{\tilde{k}_i^+ + k_i^-}$ is the fuzzy-gap amount in the i th alternative solution. Based on the ranks of alternatives, the solution is accomplished. The subsequent step is to evaluate the various IDSs by using their contributing qualities.

5. Numerical Data Analysis

5.1. Statistical Findings

It should be necessary to evaluate the effectiveness of different intrusion-detection systems [33,34]. A condition that is hard to ascertain is unsuitable for the job. Prohibitively expensive evaluations still would not yield the anticipated outcomes. The gap of cost-benefit analysis is advantageous toward a better assessment, as long as it includes the necessary standards for reliability and bias. A common method for estimating effectiveness is to evaluate the IDS numerous times and then determine a "significance level of measurement". An independent evaluation is better than one that is biased. Measuring bias, on the other hand, is challenging. In this research, we used an integrated fuzzy AHP-TOPSIS based methodology to evaluate the different popular IDSs. First, seventy-seven researchers and cybersecurity specialists with different IDS experiences were consulted for each parameter set and relevant technologies. These 77 decision-makers are composed of 30 cybersecurity specialists with more than 12 years of experience and 47 researchers from various security organizations with 10 years of IDS research experience. The specialists were required to submit and assess their viewpoints in a collaborative online setting, and they were given information on the degree of the variables in relation to the various groups, as well as linguistic standards. To begin, the decision-maker creates a pair-wise comparison matrix containing the parameters. The decisions are considered valid, since the consistency ratio (CR) is less than 0.1 or near to it. Table 4 demonstrates the combined fuzzify pair-wise assessment matrix at the initial first level. The fuzzy-aggregated pair-wise comparison matrix at the second level for Types, Audit Source Location, Targets, and Protected System is presented in Tables 5–8. For every second-level phase, the global weights were calculated. The statistical findings were tabularized in Tables 9–13. Table 14 shows the overall weights and ranking of different factors. Table 15 shows the evaluators' subjective intelligence findings in linguistic terminology, and Table 16 shows the fuzzy-decision matrix with normalized decisions. Furthermore, Table 17 demonstrates the fuzzy-decision matrix with weighted normalization. In addition, with the support of the hierarchical structure, Table 18 and Figure 4 illustrate the comprehensive and the ultimate relative closeness of the different alternatives.

Table 4. Level 1 fuzzify consolidated pair-wise comparative matrix.

	M1	M2	M3	M4
M1	1.000000, 1.000000, 1.000000	1.000000, 1.515700, 1.933100	0.489600, 0.637200, 1.000000	0.415200, 0.574300, 1.000000
	-	1.000000, 1.000000, 1.000000	0.574300, 0.665700, 0.802200	0.303900, 0.393600, 0.566100
M2	-	-	1.000000, 1.000000, 1.000000	1.000000, 1.319500, 1.551800
	-	-	-	1.000000, 1.000000, 1.000000
M3	-	-	-	-
	-	-	-	-
M4	-	-	-	-
	-	-	-	-

Table 5. Pair-wise fuzzy multi-criteria decision comparative matrix for types.

	M11	M12	M13
M11	1.000000, 1.000000, 1.000000	0.237552, 0.287963, 0.367526	0.342154, 0.447785, 0.824763
M12	-	1.000000, 1.000000, 1.000000	0.661454, 1.172563, 1.693686
M13	-	-	1.000000, 1.000000, 1.000000

Table 6. Pair-wise fuzzy multi-criteria decision comparative matrix for audit source location.

	M21	M22	M23	M24
M21	1.000000, 1.000000, 1.000000	0.694154, 0.895356, 1.112485	0.234596, 0.287864, 0.364168	0.711256, 0.954163, 1.351257
M22	-	1.000000, 1.000000, 1.000000	0.493154, 0.642362, 1.241435	0.271354, 0.351565, 0.521635
M23	-	-	1.000000, 1.000000, 1.000000	1.085484, 1.329762, 1.558235
M24	-	-	-	1.000000, 1.000000, 1.000000

Table 7. Pair-wise fuzzy multi-criteria decision comparative matrix for targets.

	M31	M32	M33
M31	1.000000, 1.000000, 1.000000	0.665365, 1.172384, 1.697465	1.157663, 1.447254, 1.704365
M32	-	1.000000, 1.000000, 1.000000	1.007762, 1.524765, 1.934368
M33	-	-	1.000000, 1.000000, 1.000000

Table 8. Pair-wise fuzzy multi-criteria decision comparative matrix for protected system.

	M41	M42	M43
M41	1.000000, 1.000000, 1.000000	1.197856, 1.588385, 2.156465	0.491541, 0.642285, 1.009958
M42	-	1.000000, 1.000000, 1.000000	0.224165, 0.295684, 0.427969
M43	-	-	1.000000, 1.000000, 1.000000

Table 9. Pair-wise comparative matrix with defuzzification and local weight of parameters at level 1.

	M1	M2	M3	M4	Weights
M1	1.000000	1.491200	0.691000	0.641000	0.214422
M2	0.670600	1.000000	0.677000	0.414300	0.159049
M3	1.447200	1.477100	1.000000	1.297700	0.312280
M4	1.560100	2.413700	0.770600	1.000000	0.314249
					C.R.= 0.015241

Table 10. Defuzzified pair-wise comparative matrix with parameter local weight for types.

	M11	M12	M13	Weights
M11	1.000000	1.173540	0.494564	0.275854
M12	0.852550	1.000000	1.172547	0.328627
M13	2.024340	0.853545	1.000000	0.395519
				C.R. = 0.0488003

Table 11. Defuzzified pair-wise comparative matrix with parameter local weight for audit source location.

	M21	M22	M23	M24	Weights
M21	1.000000	0.892654	1.173554	0.994547	0.246313
M22	1.121242	1.000000	0.691526	0.372546	0.182575
M23	0.852562	1.447256	1.000000	1.298541	0.272112
M24	1.006624	2.688354	0.770435	1.000000	0.299000
					C.R. = 0.034904

Table 12. Defuzzified pair-wise comparative matrix with parameter local weight for targets.

	M31	M32	M33	Weights
M31	1.000000	1.172541	1.363652	0.388975
M32	0.853345	1.000000	1.491224	0.355978
M33	0.733754	0.670725	1.000000	0.255047
				C.R. = 0.002506

Table 13. Defuzzified pair-wise comparative matrix with parameter local weight for protected system.

	M41	M42	M43	Weights
M41	1.000000	1.633244	0.691844	0.322565
M42	0.612477	1.000000	0.303457	0.356224
M43	1.447247	3.300347	1.000000	0.321211
				C.R. = 0.0052045

Table 14. Overall weights and level of different factors.

Level 1 Methods	Local Weights of Level 1	Level 2 Methods	Local Weights of Level 2	Overall Weights	Overall Ranks
M1	0.214422	M11	0.275854	0.059149	9
		M12	0.328627	0.070465	8
		M13	0.395519	0.084808	6
		M21	0.246313	0.039176	12
M2	0.159049	M22	0.182575	0.029038	13
		M23	0.272112	0.043279	11
		M24	0.299000	0.047556	10
		M31	0.388975	0.121469	1
M3	0.312280	M32	0.355978	0.111165	3
		M33	0.255047	0.079646	7
		M41	0.322565	0.101366	4
		M42	0.356224	0.111943	2
M4	0.314249	M43	0.321211	0.100940	5

Table 15. Evaluators' subjective intelligence findings in linguistic terminology.

	S1	S2	S3	S4	S5
M11	5.3600, 7.3006, 8.7300	5.5500, 7.5500, 8.9100	0.6400, 2.2700, 4.2700	5.3600, 7.3600, 8.7300	4.1800, 6.0900, 7.6400
	3.7300,	4.4500,	1.6400,	3.5500,	5.0000,
M12	5.5500, 7.2700	6.4500, 8.1800	3.5500, 5.5500	5.5500, 7.3600	7.0000, 8.4500
	2.3600,	5.3600,	5.5500,	0.6400,	5.3600,
M13	4.2700, 6.2700	7.3006, 8.7300	7.5500, 8.9100	2.2700, 4.2700	7.3600, 8.7300
	4.8200,	3.7300,	4.4500,	1.6400,	3.5500,
M21	6.8200, 8.5500	5.5500, 7.2700	6.4500, 8.1800	3.5500, 5.5500	5.5500, 7.3600
	5.5500,	2.3600,	2.4500,	1.3600,	4.4500,
M22	7.5005, 9.2700	4.2700, 6.2700	4.2700, 6.2700	3.3600, 5.3600	6.4500, 8.1800

Table 15. Cont.

	S1	S2	S3	S4	S5
M23	4.2700, 6.2700, 8.1800	4.8200, 6.8200, 8.5500	4.6400, 6.6400, 8.5500	0.8200, 2.6400, 4.6400	4.4500, 6.4500, 8.2700
M24	5.3600, 7.3006, 8.7300	5.5500, 7.5500, 8.9100	0.6400, 2.2700, 4.2700	5.3600, 7.3600, 8.7300	5.7300, 7.7300, 9.2700
M31	3.7300, 5.5500, 7.2700	5.3600, 7.3006, 8.7300	5.5500, 7.5500, 8.9100	0.6400, 2.2700, 4.2700	5.3600, 7.3600, 8.7300
M32	2.3600, 4.2700, 6.2700	3.7300, 5.5500, 7.2700	4.4500, 6.4500, 8.1800	1.6400, 3.5500, 5.5500	3.5500, 5.5500, 7.3600
M33	5.3600, 7.3006, 8.7300	5.5500, 7.5500, 8.9100	0.6400, 2.2700, 4.2700	5.3600, 7.3600, 8.7300	4.4500, 6.4500, 8.1800
M41	3.7300, 5.5500, 7.2700	4.4500, 6.4500, 8.1800	1.6400, 3.5500, 5.5500	3.5500, 5.5500, 7.3600	4.4500, 6.4500, 8.2700
M42	2.3600, 4.2700, 6.2700	2.4500, 4.2700, 6.2700	1.3600, 3.3600, 5.3600	4.4500, 6.4500, 8.1800	5.7300, 7.7300, 9.2700
M43	4.8200, 6.8200, 8.5500	4.6400, 6.6400, 8.5500	0.8200, 2.6400, 4.6400	4.4500, 6.4500, 8.2700	5.1800, 7.1800, 8.8200

Table 16. Fuzzy decision matrix with normalized decisions.

	S1	S2	S3	S4	S5
M11	0.3800, 0.6000, 0.8000	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9300	0.4200, 0.6900, 0.9900	0.5200, 0.7400, 0.9400
M12	0.5200, 0.7400, 0.9400	0.3800, 0.6000, 0.8000	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9300	0.4200, 0.6900, 0.9900
M13	0.3800, 0.6000, 0.8000	0.5200, 0.7400, 0.9400	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9200	0.2000, 0.4700, 0.7700
M21	0.3800, 0.6000, 0.8000	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9300	0.4200, 0.6900, 0.9900	0.5400, 0.7500, 0.9400
M22	0.5200, 0.7400, 0.9400	0.3800, 0.6000, 0.8000	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9300	0.4200, 0.6900, 0.9900
M23	0.3800, 0.6000, 0.8000	0.5200, 0.7400, 0.9400	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9200	0.2000, 0.4700, 0.7700
M24	0.3800, 0.6000, 0.8000	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9300	0.4200, 0.6900, 0.9900	0.5400, 0.7500, 0.9400
M31	0.5200, 0.7400, 0.9400	0.3800, 0.6000, 0.8000	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9300	0.4200, 0.6900, 0.9900
M32	0.3800, 0.6000, 0.8000	0.5200, 0.7400, 0.9400	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9200	0.2000, 0.4700, 0.7700
M33	0.3800, 0.6000, 0.8000	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9300	0.4200, 0.6900, 0.9900	0.5400, 0.7500, 0.9400
M41	0.5200, 0.7400, 0.9400	0.3800, 0.7500, 0.9200	0.3800, 0.6000, 0.8000	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9300
M42	0.3800, 0.6000, 0.8000	0.3500, 0.5800, 0.8100	0.5200, 0.7400, 0.9400	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9200
M43	0.5200, 0.7400, 0.9200	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.3500, 0.5800, 0.8100	0.4200, 0.6900, 0.9900

Table 17. Fuzzy decision matrix with weighted normalization.

	S1	S2	S3	S4	S5
M11	0.00000,	0.00200,	0.00200,	0.00100,	0.00300,
	0.00200,	0.00700,	0.00700,	0.00500,	0.01100,
	0.00900	0.02200	0.02400	0.01800	0.03600
M12	0.00300,	0.00000,	0.00200,	0.00200,	0.00100,
	0.01200,	0.00200,	0.00700,	0.00700,	0.00500,
	0.04100	0.00900	0.02200	0.02400	0.01800
M13	0.00300,	0.00300,	0.00300,	0.00500,	0.00500,
	0.01200,	0.01200,	0.01200,	0.01600,	0.01600,
	0.04200	0.04100	0.04100	0.04800	0.04900
M21	0.00000,	0.00200,	0.00200,	0.00100,	0.00200,
	0.00200,	0.00700,	0.00700,	0.00500,	0.00900,
	0.00900	0.02200	0.02400	0.01800	0.03800
M22	0.00300,	0.00000,	0.00200,	0.00200,	0.00100,
	0.01200,	0.00200,	0.00700,	0.00700,	0.00500,
	0.04100	0.00900	0.02200	0.02400	0.01800
M23	0.00300,	0.00300,	0.00300,	0.00500,	0.00500,
	0.01200,	0.01200,	0.01200,	0.01600,	0.01600,
	0.04200	0.04100	0.04100	0.04800	0.04900
M24	0.00000,	0.00000,	0.00200,	0.00200,	0.00100,
	0.00200,	0.00200,	0.00700,	0.00700,	0.00500,
	0.00900	0.00900	0.02200	0.02400	0.01800
M31	0.00300,	0.00300,	0.00300,	0.00500,	0.00500,
	0.01200,	0.01200,	0.01200,	0.01600,	0.01600,
	0.04100	0.04100	0.04100	0.04800	0.04900
M32	0.00000,	0.00000,	0.00200,	0.00200,	0.00100,
	0.00200,	0.00200,	0.00700,	0.00700,	0.00500,
	0.00900	0.00900	0.02200	0.02400	0.01800
M33	0.00300,	0.00300,	0.00300,	0.00500,	0.00500,
	0.01200,	0.01200,	0.01200,	0.01600,	0.01600,
	0.04100	0.04100	0.04100	0.04800	0.04900
M41	0.00000,	0.00200,	0.00200,	0.00100,	0.00200,
	0.00200,	0.00700,	0.00700,	0.00500,	0.00900,
	0.00900	0.02200	0.02400	0.01800	0.03800
M42	0.00300,	0.00300,	0.00500,	0.00500,	0.00100,
	0.01200,	0.01200,	0.01600,	0.01600,	0.00500,
	0.04100	0.04100	0.04800	0.04900	0.01800
M43	0.00300,	0.00300,	0.00200,	0.00200,	0.00100,
	0.01200,	0.01200,	0.01000,	0.00900,	0.00500,
	0.04200	0.04200	0.03700	0.03800	0.01800

Table 18. Coefficients of closeness to the aspired level throughout the alternatives.

Alternatives	d + i	d - i	Gap	Degree of CC+i	Satisfaction Degree of CC-i
Alternative 1	S1	0.0452564	0.0556547	0.6235652	0.3954740
Alternative 2	S2	0.0564554	0.0353625	0.3655474	0.6586950
Alternative 3	S3	0.0475458	0.0555474	0.5695857	0.4585660
Alternative 4	S4	0.0453567	0.0463562	0.4685745	0.4458570
Alternative 5	S5	0.0452265	0.0425555	0.4536652	0.4695850

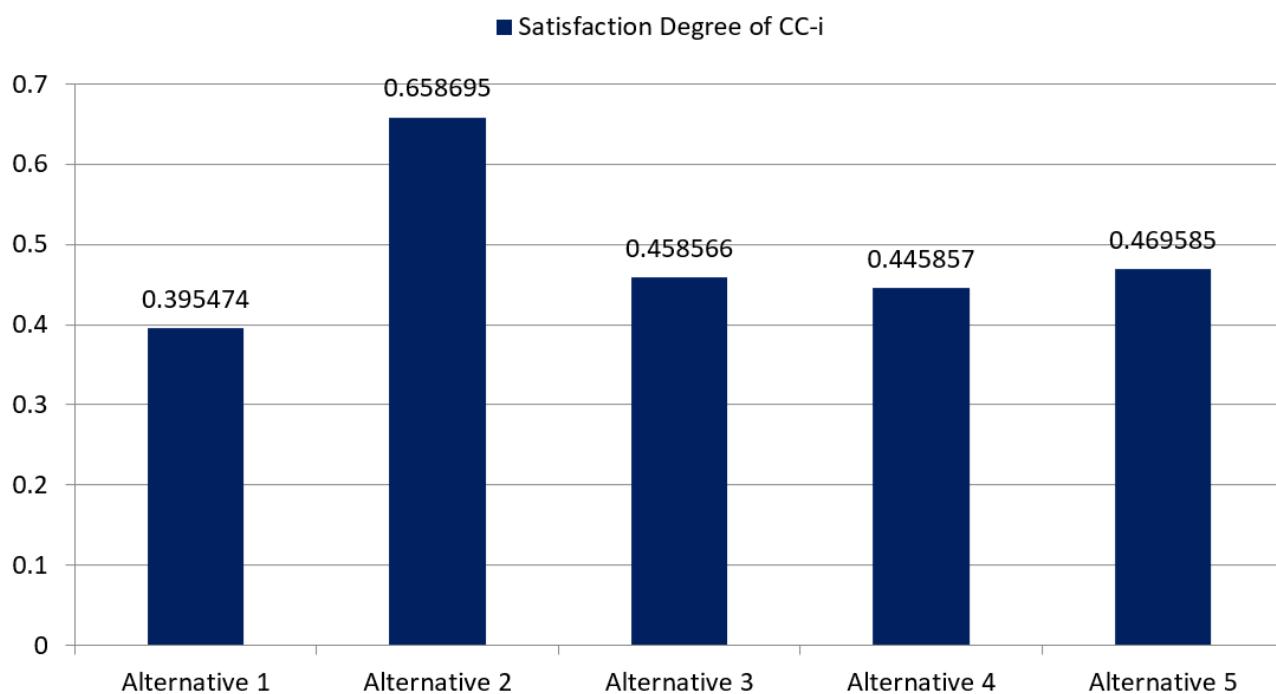


Figure 4. Satisfaction Degree of CC-i.

Depending upon the value of satisfaction degree shown in Figure 4, it is concluded that the initial ranking of the efficient IDS using the integrated fuzzy AHP-TOPSIS approach is $S_2 > S_5 > S_3 > S_4 > S_1$ ($>$ means “higher to”). Therefore, S_2 , which is Suricata, is considered the preferable and effective IDS.

5.2. Comparative Analysis

The use of multiple techniques on almost the same data delivers contradictory conclusions. The investigators use a variety of complementary ways to test the correctness of the research outcome. In this investigation, the researcher applied a hybrid fuzzy AHP-TOPSIS-based approach to evaluate the effectiveness of different alternatives. The data-acquisition and -assessment process for that sample in fuzzy AHP-TOPSIS is similar to the traditional AHP-TOPSIS approach. As a result, fuzzification and defuzzification are required for the fuzzy-AHP-TOPSIS. Furthermore, the data for fuzzy AHP-TOPSIS are captured in their initial statistical values and afterward transformed into fuzzy value sets. The outcomes obtained through the traditional method were well correlated with those obtained by using the fuzzy procedure. The comparison analysis' results were not highly different and varied from each other, but the accuracy of the outcomes was varied. The traditional approaches for the effectiveness evaluation of different IDSs are insufficient for working with the inaccurate or ambiguous quality of linguistic evaluations. Therefore, integrated fuzzy multi-criteria decision-making strategies are developed to tackle this challenge. Moreover, the fuzzy approach confirms the findings of the classic strategy, thus enhancing the validity of the ranking among the five methods. Table 19 and Figure 5 show the comparison of outcomes with the fuzzy and traditional AHP-TOPSIS approach.

Table 19. Comparison of the results of classical and fuzzy AHP-TOPSIS methods.

Methods/Alternatives	S1	S2	S3	S4	S5
Fuzzy-AHP-TOPSIS	0.3954740	0.6586950	0.4585660	0.4458570	0.4695850
Traditional-AHP-TOPSIS	0.3785410	0.6453520	0.4445860	0.4324550	0.4585700

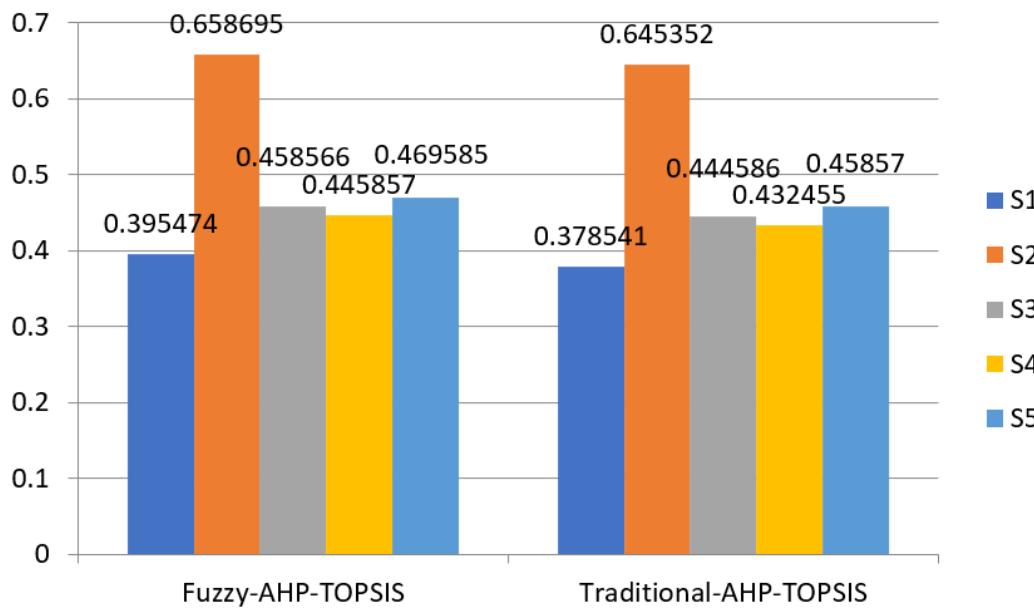


Figure 5. Comparison of the results with traditional approach.

5.3. Sensitivity Analysis

The responsiveness was evaluated by altering the parameters to test the validity of the gathered data. During the same statistical analysis, the sensitivity of the obtained weights (factors involved) was evaluated. Throughout the investigation, at the final (second) step, 13 variables were picked so that sensitivities can be investigated by using 12 experiments. In each trial, the degree of satisfaction (CC-i) was found by adjusting the weights of every parameter, while the weight of the other element remained stable, using the Fuzzy-AHP-TOPSIS approach. Reported consequences are shown in Table 20 and Figure 6.

Table 20. Sensitivity analysis.

Experiments	Weights/ Alternatives	S1	S2	S3	S4	S5
Experiment-0	Original Weights	0.3954740	0.6586950	0.4585660	0.4458570	0.4695850
Experiment-1	M11	0.4354254	0.6012524	0.4895685	0.4775474	0.4956526
Experiment-2	M12	0.4765285	0.7025652	0.5285657	0.5245412	0.5346525
Experiment-3	M13	0.5225365	0.5345474	0.3952653	0.3457425	0.3858547
Experiment-4	M21	0.3412524	0.3855268	0.4245623	0.3756352	0.4152334
Experiment-5	M22	0.3778569	0.4184759	0.5212542	0.5526354	0.5348549
Experiment-6	M23	0.3645256	0.3832654	0.3452635	0.3965875	0.3856368
Experiment-7	M24	0.4800215	0.4976965	0.3776538	0.4236587	0.4165365
Experiment-8	M31	0.3285452	0.5563598	0.3685659	0.5252635	0.5363524
Experiment-9	M32	0.5256356	0.5332654	0.4856965	0.3452635	0.3863897
Experiment-10	M33	0.3436352	0.3853652	0.4276566	0.3753416	0.4163526
Experiment-11	M41	0.3785695	0.4183265	0.3965235	0.3535277	0.3863524
Experiment-12	M42	0.3645758	0.3852653	0.3838574	0.4965352	0.4963564
Experiment-13	M43	0.4856365	0.4963526	0.5485684	0.5254291	0.5458473

Table 18 represents the real weights of this research investigation in the first row. Taking the performances into account, we see that the alternative (S2) has a high level of satisfaction (CC-i). Twelve experiments were carried out. The results reveal that, after twelve tests, Alternative-2 (S2) consistently retains a high level of satisfaction (CC-i). The performance results demonstrate that the rankings of the alternatives are weight-dependent.

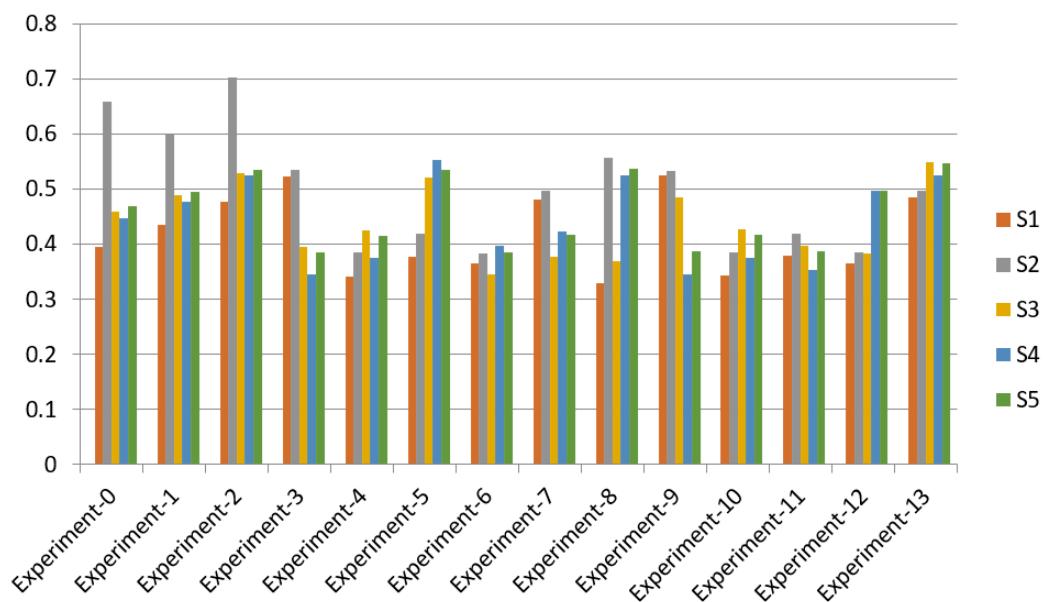


Figure 6. Sensitivity analysis.

6. Conclusions

In today's modern environment, network security is significant for small, as well as large, organizations. Modern security challenges that are increasingly complex and advanced are always being developed. Online security issues are becoming more prevalent, and an IDS can assist in defending your organization from malicious activities. An IDS simply analyzes network traffic and notifies the system administrator if any suspicious activity is detected. This paper discusses the five most widely used intrusion-detection systems. Thereafter, the functionality of these five popularly used intrusion-detection systems, including Zeek, Suricata, Security Onion, OSSEC, and Snort, are effectively compared with the help of a hybrid fuzzy-logic-based approach and discussed in this study. All of the IDSs appear to be highly potential tools. Even though Snort is extensively deployed, it is important to note that Suricata is the new-generation multi-threaded application with a broader range of features. Suricata also has a significant benefit over Snort in that it does not need many processes to handle an upsurge in network traffic. The type of connection or attack to be monitored will determine the implementation of a multispectral IDS. The recommendation to network administrators is based on a generic network design and frequent network obstructions; however, this may vary depending on the network infrastructure of the business entity. The target for future research work is to deploy similar research with other MCDM models. The real-world dataset would be reviewed, and final assessments would be easily measured without the assistance of any other third entity.

Author Contributions: Conceptualization, H.A., M.T.J.A., A.A. (Abdullah Alharbi), W.A. and M.A.; methodology, H.A., M.T.J.A., A.A. (Abdullah Alharbi), A.A. (Alka Agrawal) and R.K.; software, M.T.J.A., A.A. (Alka Agrawal) and R.K.; validation, M.T.J.A., A.A. (Abdullah Alharbi), A.A. (Alka Agrawal) and R.K.; formal analysis, H.A., M.T.J.A., A.A. (Alka Agrawal) and R.A.K.; investigation, H.A., M.T.J.A., A.A. (Abdullah Alharbi), W.A., M.A., D.P., A.A. (Alka Agrawal), R.K. and R.A.K.; resources, H.A., M.T.J.A., A.A. (Abdullah Alharbi), W.A. and M.A.; data curation, M.T.J.A., A.A. (Abdullah Alharbi), A.A. (Alka Agrawal) and R.K.; writing—original draft preparation, M.T.J.A., A.A. (Abdullah Alharbi), W.A., M.A., D.P., A.A. (Alka Agrawal) and R.A.K.; writing—review and editing, M.T.J.A., A.A. (Abdullah Alharbi), W.A., D.P., A.A. (Alka Agrawal) and M.A.; visualization, M.T.J.A., A.A. (Abdullah Alharbi), W.A., M.A., D.P. and R.A.K.; supervision, H.A., M.T.J.A., A.A. (Alka Agrawal) and R.A.K.; project administration, H.A., A.A. (Abdullah Alharbi), W.A. and R.A.K.; funding acquisition, H.A., A.A. (Abdullah Alharbi), W.A. and R.A.K. All authors have read and agreed to the published version of the manuscript.

Funding: The project was funded by Researchers Supporting project number (TURSP-2020/306), Taif University, Taif, Saudi Arabia.

Acknowledgments: This research was supported by Taif University Researchers Supporting Project number (TURSP-2020/306), Taif University, Taif, Saudi Arabia.

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

References

1. Sen, S. A survey of intrusion detection systems using evolutionary computation. In *Bio-Inspired Computation in Telecommunications*; Morgan Kaufmann: Burlington, MA, USA, 2015; pp. 73–94.
2. Ansari, M.T.J.; Pandey, D.; Alenezi, M. STORE: Security threat oriented requirements engineering methodology. *J. King Saud Univ.-Comput. Inf. Sci.* **2018**, *34*, 191–203. [[CrossRef](#)]
3. Ali, M.; Shaeles, S.; Bendiab, G.; Ghita, B. MALGRA: Machine learning and N-gram malware feature extraction and detection system. *Electronics* **2020**, *9*, 1777. [[CrossRef](#)]
4. Swann, M.; Rose, J.; Bendiab, G.; Shaeles, S.; Savage, N. A comparative study of traffic generators: Applicability for malware detection testbeds. *J. Internet Technol. Secur. Trans.* **2021**, *8*, 705–713. [[CrossRef](#)]
5. Shaeles, S.N.; Papadaki, M. FHSD: An improved IP spoof detection method for web DDoS attacks. *Comput. J.* **2015**, *58*, 892–903. [[CrossRef](#)]
6. Ansari, T.J.; Pandey, D. An Integration of Threat Modeling with Attack Pattern and Misuse Case for Effective Security Requirement Elicitation. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 16–20.
7. Ansari, M.T.J.; Baz, A.; Alhakami, H.; Alhakami, W.; Kumar, R.; Khan, R.A. P-STORE: Extension of STORE methodology to elicit privacy requirements. *Arab. J. Sci. Eng.* **2021**, *46*, 8287–8310. [[CrossRef](#)]
8. Alosaimi, W.; Ansari, M.T.J.; Alharbi, A.; Alyami, H.; Seh, A.H.; Pandey, A.K.; Agrawal, A.; Khan, R.A. Evaluating the Impact of Different Symmetrical Models of Ambient Assisted Living Systems. *Symmetry* **2021**, *13*, 450. [[CrossRef](#)]
9. Ji, H.; Wang, Y.; Qin, H.; Wang, Y.; Li, H. Comparative performance evaluation of intrusion detection methods for in-vehicle networks. *IEEE Access* **2018**, *6*, 37523–37532. [[CrossRef](#)]
10. Magán-Carrión, R.; Urda, D.; Díaz-Cano, I.; Dorronsoro, B. Towards a reliable comparison and evaluation of network intrusion detection systems based on machine learning approaches. *Appl. Sci.* **2020**, *10*, 1775. [[CrossRef](#)]
11. Hussein, S.M. Performance evaluation of intrusion detection system using anomaly and signature based algorithms to reduction false alarm rate and detect unknown attacks. In Proceedings of the 2016 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 15–17 December 2016; pp. 1064–1069.
12. Nikolopoulos, K.; Punia, S.; Schäfers, A.; Tsinopoulos, C.; Vasilakis, C. Forecasting and planning during a pandemic: COVID-19 growth rates, supply chain disruptions, and governmental decisions. *Eur. J. Oper. Res.* **2021**, *290*, 99–115. [[CrossRef](#)]
13. Alhakami, W.; Binmahfoudh, A.; Baz, A.; Alhakami, H.; Ansari, M.T.J.; Khan, R.A. Atrocious Impinging of COVID-19 Pandemic on Software Development Industries. *Comput. Syst. Eng.* **2021**, *36*, 323–338. [[CrossRef](#)]
14. Ansari, M.T.J.; Khan, N.A. Worldwide COVID-19 Vaccines Sentiment Analysis through Twitter Content. *Electron. J. Gen. Med.* **2021**, *18*, em329. [[CrossRef](#)]
15. Attaallah, A.; Ahmad, M.; Ansari, M.T.J.; Pandey, A.K.; Kumar, R.; Khan, R.A. Device security assessment of Internet of healthcare things. *Intell. Autom. Soft Comput.* **2020**, *27*, 593–603. [[CrossRef](#)]
16. Upendran, V.; Gopinath, R. Feature selection based on multi-criteria decision making for intrusion detection system. *Management* **2021**. [[CrossRef](#)]
17. Hu, Q.; Yu, S.Y.; Asghar, M.R. Analysing performance issues of open-source intrusion detection systems in high-speed networks. *J. Inf. Secur. Appl.* **2020**, *51*, 102426. [[CrossRef](#)]
18. Imoize, A.L.; Oyedare, T.; Otuokere, M.E.; Shetty, S. Software intrusion detection evaluation system: A cost-based evaluation of intrusion detection capability. *Commun. Netw.* **2018**, *10*, 211–229. [[CrossRef](#)]
19. Saber, M.; Belkasmi, M.G.; Chadli, S.; Emharraf, M.; El Farissi, I. Implementation and Performance Evaluation of Intrusion Detection Systems under high-speed networks. In Proceedings of the 2nd International Conference on Big Data, Cloud and Applications, Tetouan, Morocco, 29–30 March 2017; pp. 1–6.
20. Shaeles, S.N.; Katos, V.; Karakos, A.S.; Papadopoulos, B.K. Real time DDoS detection using fuzzy estimators. *Comput. Secur.* **2012**, *31*, 782–790. [[CrossRef](#)]
21. Schrötter, M.; Scheffler, T.; Schnor, B. Evaluation of Intrusion Detection Systems in IPv6 Networks. In Proceedings of the 16th International Joint Conference on e-Business and Telecommunications (ICETE 2019), Prague, Czech Republic, 26–28 July 2019; pp. 408–416.
22. Haas, S.; Sommer, R.; Fischer, M. Zeek-osquery: Host-network correlation for advanced monitoring and intrusion detection. In *IFIP International Conference on ICT Systems Security and Privacy Protection*; Springer: Cham, Switzerland, 2020; pp. 248–262.
23. Paxson, V. Bro: A system for detecting network intruders in real-time. *Comput. Netw.* **1999**, *31*, 2435–2463. [[CrossRef](#)]
24. Garcia-Teodoro, P.; Diaz-Verdejo, J.; Maciá-Fernández, G.; Vázquez, E. Anomaly-based network intrusion detection: Techniques, systems and challenges. *Comput. Secur.* **2009**, *28*, 18–28. [[CrossRef](#)]

25. Park, W.; Ahn, S. Performance comparison and detection analysis in snort and suricata environment. *Wirel. Pers. Commun.* **2017**, *94*, 241–252. [[CrossRef](#)]
26. Burks, D. Security Onion. 2012. Available online: Securityonion.blogspot.com (accessed on 17 January 2022).
27. Cid, D.B. Log Analysis Using OSSEC. 2017. Available online: http://www.academia.edu/8343225/Log_Analysis_using_OSSEC (accessed on 17 January 2022).
28. Anafcheh, A. Intrusion Detection with OSSEC. 2018. Available online: <https://www.theseus.fi/bitstream/handle/10024/150030/ali-anafcheh-thesis.pdf?sequence=1> (accessed on 17 January 2022).
29. Roesch, M. Snort: Lightweight intrusion detection for networks. In Proceedings of the LISA '99: 13th Systems Administration Conference, Seattle, WA, USA, 7–12 November 1999; Volume 99, pp. 229–238.
30. Saaty, T.L. How to make a decision: The analytic hierarchy process. *Eur. J. Oper. Res.* **1990**, *48*, 9–26. [[CrossRef](#)]
31. Hwang, C.L.; Yoon, K. Methods for multiple attribute decision making. In *Multiple Attribute Decision Making*; Springer: Berlin/Heidelberg, Germany, 1981; pp. 58–191.
32. Chen, S.J.; Hwang, C.L. Fuzzy multiple attribute decision making methods. *Fuzzy Mult. Attrib. Decis. Mak.* **1992**, *375*, 289–486.
33. Ansari, M.T.J.; Al-Zahrani, F.A.; Pandey, D.; Agrawal, A. A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 236. [[CrossRef](#)] [[PubMed](#)]
34. Rose, J.R.; Swann, M.; Bendiab, G.; Shiaeles, S.; Kolokotronis, N. Intrusion Detection using Network Traffic Profiling and Machine Learning for IoT. In Proceedings of the 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), Tokyo, Japan, 28 June–2 July 2021; pp. 409–415. [[CrossRef](#)]
35. Kumar, R.; Khan, A.I.; Abushark, Y.B.; Alam, M.M.; Agrawal, A.; Khan, R.A. An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications. *IEEE Access* **2020**, *8*, 50944–50957. [[CrossRef](#)]
36. Kumar, R.; Khan, A.I.; Abushark, Y.B.; Alam, M.M.; Agrawal, A.; Khan, R.A. A knowledge-based integrated system of hesitant fuzzy set, ahp and topsis for evaluating security-durability of web applications. *IEEE Access* **2020**, *8*, 48870–48885. [[CrossRef](#)]
37. Abushark, Y.B.; Khan, A.I.; Alsolami, F.J.; Almalawi, A.; Alam, M.M.; Agrawal, A.; Kumar, R.; Khan, R.A. Usability Evaluation through Fuzzy AHP-TOPSIS Approach: Security Requirement Perspective. *CMC-Comput. Mater. Contin.* **2021**, *68*, 1203–1218. [[CrossRef](#)]