sensors

MDPI

Article

An Optimization Model for Appraising Intrusion-Detection Systems for Network Security Communications: Applications, Challenges, and Solutions

Mohamed Abdel-Basset [1], Abduallah Gamal [1], Karam M. Sallam [2,*], Ibrahim Elgendi [2], Kumudu Munasinghe [2] and Abbas Jamalipour [3]

[1] Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt; mohamedbasset@ieee.org (M.A.-B.); abduallahgamal@fci.zu.edu.eg (A.G.)
[2] School of IT and Systems, University of Canberra, Canberra, ACT 2601, Australia; ibrahim.elgendi@canberra.edu.au (I.E.); kumudu.munasinghe@canberra.edu.au (K.M.)
[3] School of Electrical and Information Engineering, The University of Sydney, Sydney, NSW 2006, Australia; abbas.jamalipour@sydney.edu.au
* Correspondence: karam.sallam@canberra.edu.au

Abstract: Cyber-attacks are getting increasingly complex, and as a result, the functional concerns of intrusion-detection systems (IDSs) are becoming increasingly difficult to resolve. The credibility of security services, such as privacy preservation, authenticity, and accessibility, may be jeopardized if breaches are not detected. Different organizations currently utilize a variety of tactics, strategies, and technology to protect the systems' credibility in order to combat these dangers. Safeguarding approaches include establishing rules and procedures, developing user awareness, deploying firewall and verification systems, regulating system access, and forming computer-issue management groups. The effectiveness of intrusion-detection systems is not sufficiently recognized. IDS is used in businesses to examine possibly harmful tendencies occurring in technological environments. Determining an effective IDS is a complex task for organizations that require consideration of many key criteria and their sub-aspects. To deal with these multiple and interrelated criteria and their sub-aspects, a multi-criteria decision-making (MCMD) approach was applied. These criteria and their sub-aspects can also include some ambiguity and uncertainty, and thus they were treated using q-rung orthopair fuzzy sets (q-ROFS) and q-rung orthopair fuzzy numbers (q-ROFNs). Additionally, the problem of combining expert and specialist opinions was dealt with using the q-rung orthopair fuzzy weighted geometric (q-ROFWG). Initially, the entropy method was applied to assess the priorities of the key criteria and their sub-aspects. Then, the combined compromised solution (CoCoSo) method was applied to evaluate six IDSs according to their effectiveness and reliability. Afterward, comparative and sensitivity analyses were performed to confirm the stability, reliability, and performance of the proposed approach. The findings indicate that most of the IDSs appear to be systems with high potential. According to the results, Suricata is the best IDS that relies on multi-threading performance.

Keywords: cyber-attacks; intrusion-detection system; MCDM; q-rung orthopair fuzzy sets; q-ROFWG

Citation: Abdel-Basset, M.; Gamal, A.; Sallam, K.M.; Elgendi, I.; Munasinghe, K.; Jamalipour, A. An Optimization Model for Appraising Intrusion-Detection Systems for Network Security Communications: Applications, Challenges, and Solutions. *Sensors* **2022**, *22*, 4123. https://doi.org/10.3390/s22114123

Academic Editor: Peter Han Joo Chong

Received: 13 April 2022
Accepted: 25 May 2022
Published: 29 May 2022

1. Introduction

The continuous development of computer systems has led to the increasing dependence of companies, organizations, and people on computer networks in performing their functions and offering their services in modern ways [1]. However, at the same time, it has become vulnerable to penetration by attackers with the aim of making illegal gains by exploiting some security vulnerabilities, which led to an increase in interest in issues of protection and security of these systems. Today there are many methods used within this field, and there are many intrusion-detection systems (IDSs) available [2]. IDSs are a necessity for the stability of an organization's normal system performance. In this regard, traditional

intrusion-detection techniques are highly unrewarding and ineffective due to the multiplicity of attack methods and their different forms. Among the traditional methods used previously are obfuscation, transformation, and polymorphism techniques, which lead to malware resistance [3]. Despite the prominent role it plays, it still has some shortcomings. Therefore, there was a need to continue conducting research on intrusion-detection systems in order to reach an optimal structure that achieves a high protection rate.

The internet changed the concept of computing as we know it. The possibilities and opportunities available became unlimited, and with it, the risks and opportunities for breakthroughs increased. Computer security primarily focuses on protecting a specific source or valuable data and information within a single computer device. Security is defined as the reaction taken to security threats resulting from a harmful act by some people. The value of the data can be violated in three ways: privacy, integrity, and availability of information [4]. Computer protection is generally referred to by the term CIA, which is represented by the following three concepts:

- Confidentiality: Preventing unauthorized persons from disclosing or accessing information; i.e., accessing information only by authorized persons.
- Integrity: Maintaining information integrity by preventing unauthorized modification.
- Availability: It is the ability of a computer to work and provide the resources and services expected of it to legitimate people upon request.

Network security includes all actions or activities taken by organizations and companies in order to protect resources and ensure the integrity and continuity of operations across networks [5]. Security policies also define the permissions available to users in the way they use network components and resources. In order to build an effective network-protection strategy, all potential security threats must be identified, and then the most effective set of tools to combat them must be selected [6]. Preventing all exploits for vulnerabilities in networks and systems is not possible [7]. Network protection is achieved through the use of a set of components at several levels, with the aim of protecting organizations from internal attacks and external attacks as much as possible. A firewall is a component that achieves the most basic level of protection but is not sufficient on its own. Designing and implementing a completely secure system is very difficult in practice, but it is possible to detect intrusions and take appropriate measures to protect against them. This is what the IDS basically does, as it is used as an alert system, within the security and protection system, that gives an alert when it detects an attempt by someone to penetrate the computer system or network [8]. As a result, IDSs are important in a network security solution. The primary goal of IDSs is to detect an intrusion while it is occurring rather than after it has ended, and then alert the person responsible for the problem by sending an email or setting off an alert. It must be able to take any action to minimize harm to the system due to the hack. The second goal is to collect data from the system, record all important events, and determine the source of the attack, and these data are used for legal purposes as evidence or proof against the attacker.

IDSs must be placed in strategic places so that they are able to see network traffic in order to analyze it and thus achieve the maximum benefit from it [9]. In this regard, several ways to classify IDSs are described using different analysis and control methods. The most common way to classify intrusion-detection systems is to group them according to the location of the information source. Basic information sources are network packets captured from a network backbone or local network segments, operating systems, and critical files. Intrusion-detection systems can be classified into host-based detection-intrusion systems, network-based intrusion-detection systems, and hybrid systems. On the user's computer, a host-based intrusion-detection system (HIDS) is installed. HIDSs operate on information collected from within a single computer system [10]. HIDSs employ monitoring sensors, also called clients, on each host to be monitored. In general, the most common forms of information sources for HIDSs are operating system audit logs, system logs, and critical system files [10]. The customer checks these sources for unauthorized changes or patterns of suspicious activity. This allows HIDSs to reliably analyze activities, accurately identifying

which users and which processes are participating in a specific attack on the operating system. The most common form of IDSs is network-based intrusion-detection systems (NIDSs) [11]; also, most companies and organizations are often supported by NIDSs along with firewalls. These systems detect attacks by capturing and analyzing network packets by listening to network segments or switches [11]. In this case, the system is placed on an entire network segment and not on a single device within the network, or it is placed to monitor a gateway on the switch. Thus, it can monitor all mobile packets between groups of computers connected to the network, by matching one or more packets with the database of signatures of attacks, or by analyzing the traffic to detect anomalies. NIDSs can be taken advantage of by placing it outside of firewalls, thus alerting the responsible person to incoming packets that might circumvent the firewall. Both HIDSs and NIDSs have strengths and benefits that complement each other [12]. Figure 1 introduces the general architecture of an HIDS and NIDS. The next generation of IDSs must combine the two technologies in order to improve the network's resistance to attacks and abuse. In addition, they should enhance security policy and provide greater flexibility in application and deployment options. A hybrid IDS is a mixture of an HIDS and NIDS. It provides a combination of the strengths of the two methods. Their modus operandi varies from product to product, making it difficult to define and determine hybrid intrusion systems in a more accurate manner.

Afterward, detection methods are the basis of intrusion-detection techniques, which are the engine in detecting the malicious activities of the information source. Detection methods analyze the information they monitor and trigger alerts if malicious traffic is detected. Accordingly, IDSs can be categorized, according to the detection methods used, into anomaly-based intrusion-detection systems (AIDSs) [13] and signature-based intrusion-detection systems (SIDSs) [14]. In this regard, AIDSs operate on the assumption that malicious events are different from normal actions, and thus the differences are sought to detect the attack. These systems constitute profiles of historical data collected during a period of normal operation. It then collects event data to determine when the monitored activity deviates from normal behavior and triggers an alarm. SIDSs also are called signature-based detection because alerts are generated based on the signatures of specific attacks. This type of signature attack involves specific traffic or activity based on known hacking activity. It is also called misuse-based detection. The basic premise is the model that has been written to describe bad behavior, after which the system compares the sequence of information with this model to decide what is normal and what is malicious. These systems are accurate and emit fewer false alarms, but they do not detect a hack unless there is a predetermined model for it.

Nowadays, Internet networks are vulnerable to a wide range of threats and attacks, such as impersonation, privilege breaches, data loss, altered and fraudulent data units, and denial of connections [15]. Therefore, IDSs have an essential task to protect the normal system performance of an organization. It is, therefore, necessary to add new security requirements and additional networking measures to the network security requirements [16]. IDSs must constantly change and adapt to all these new threats and assault technologies. Therefore, the process of determining the best IDS for network protection, threat warning, and cyber-attacks is a very difficult task in light of the various criteria on which an IDS is developed. Thus, IDSs should not be chosen to quickly secure the network without a thorough understanding of the technology, solutions, and potential consequences.

In this study, a set of criteria were adopted to evaluate IDSs according to previous studies and expert opinions. The criteria that have been adopted were divided into four basic criteria—protected system, audit source location, alerts, and types—and each main criterion includes several sub-aspects. The set of sub-aspects are as follows: HIDS, NIDS, hybrids, host log files, network packets, application log files, IDS sensor application, network, host, open-source, closed source, and freeware. In order to solve such complex problems related to the evaluation of IDSs, multi-criteria decision-making (MCDM) has been proven to be one of the best tools for the effective evaluation of IDS [16]. MCDM is

popular in complex problems because it enables the decision-maker to take care of all the available criteria and take an appropriate decision as per the priority [17]. Since the ideal choice is governed by multiple criteria, a good decision-maker, in certain situations, may look for criteria of high impact on which to focus.

Consequently, due to the assessment of IDSs under multiple criteria and a pluralistic viewpoint, the assessment process is tainted by ambiguity and uncertainty, which is difficult to deal with in real numbers. Hence, the q-rung orthopair fuzzy sets (q-ROFSs) theory has been applied to deal with such complex problems [18]. The q-ROFS proved to be effective in solving ambiguous and uncertain problems as it came as a generalization of the intuitionistic fuzzy sets (IFSs) [19] and Pythagorean fuzzy sets (PFSs) theories [20].

Finally, to deal with the problem of evaluating the effectiveness of IDSs, a hybrid approach consisting of two multi-criteria decision-making methods, the entropy method [21] and the combined compromised solution (CoCoSo) method [22], was adopted. The proposed hybrid approach is presented under the q-rung orthopair fuzzy environment and by utilizing the q-rung orthopair fuzzy numbers (q-ROFNs) numbers. Firstly, the entropy method was adopted to evaluate the main and sub-aspects and to determine the final weights. Secondly, the CoCoSo method was applied to evaluate the available alternatives and determine the best alternative.

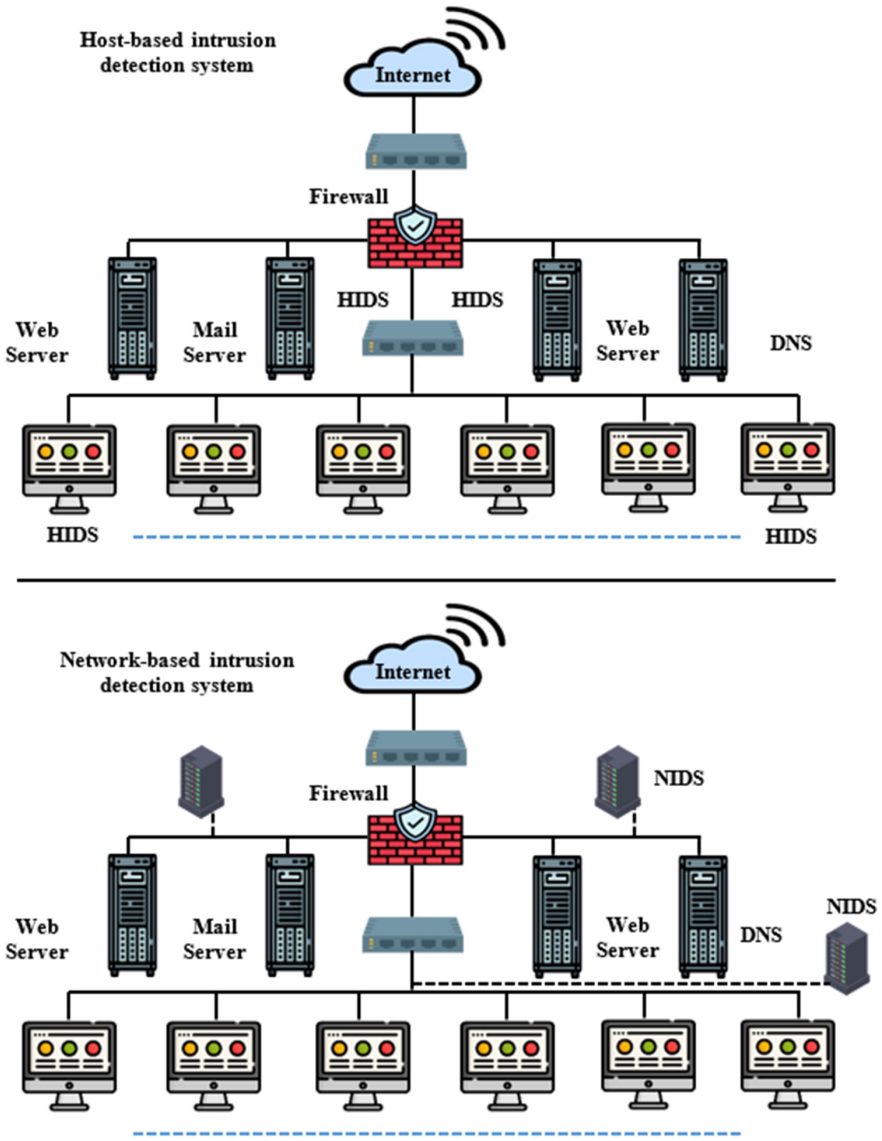

Figure 1. Comparison of the HIDS and NIDS structure [23].

The main contributions of this study can be listed as follows: (i) a novel hybrid MCDM approach is proposed for the evaluation of the IDS; (ii) this hybrid MCDM approach is named q-ROF entropy-CoCoSo, which give assessments of subjective and impartial expert insights; (iii) the q-ROFSs method is conducted to handle the uncertainty in experts' evaluations; (iv) a q-ROF entropy is utilized to compute the criteria weights; and (v) a q-ROF CoCoSo is suggested to evaluate the selected IDSs.

The article is organized as follows: Section 2 highlights the IDS and insights into MCDM; Section 3 introduces some preliminaries of q-ROFS and the proposed research approach; Section 4 illustrates the application of the MCDM approach in evaluating the IDS and discussion; and Section 5 contains the conclusions.

2. Background Information

This section provides basic knowledge about IDSs to enable a deeper understanding of this topic; also, some basic information related to MCDM is presented. Afterward, some studies related to q-ROF theory are introduced. Alyami et al. presented a study based on a hybrid MCDM approach consisting of the fuzzy analytical hierarchy process (AHP) and the fuzzy technique for order performance by similarity to ideal solution (TOPSIS) to evaluate the effectiveness of the IDSs [16]. In their study, they used four main criteria and thirteen sub-aspects to evaluate five IDSs. Their results indicate that Suricata is the most effective IDS. Their results also indicate that most of the IDSs that were evaluated in the study are effective and close in their results. Abushark et al. developed a study to evaluate the optimization of machine learning-based IDSs using a hybrid MCDM approach that comprises the AHP and TOPSIS in a fuzzy environment [24]. Their findings aim to identify attributes related to cyber security, allowing the design of more effective and efficient IDSs. Al-Harbi et al. presented a study for an optimal evaluation of machine learning-based IDSs using a hybrid MCDM model that includes AHP and TOPSIS under hesitant fuzzy conditions [8]. Their findings aim to identify features related to cyber security, allowing the design of more effective and IDSs. Almotiri presented an evaluation system to detect malicious traffic based on system performance [25]. They adopted an MCDM approach consisting of AHP–TOPSIS methods to rank the impact of alternatives according to their overall performance. Their study aims to be a reference for practitioners working in the field of evaluating and selecting the most effective traffic detection approach.

Afterward, some studies related to MCDM approaches and their applications in different fields were presented. Sharma and Kaul presented a study to deal with network performance delays and disruptions due to cluster-based communications that place a significant burden on the cluster head (CH) [26]. They used an MCDM approach including two AHP–TOPSIS methods to reduce the overburden on a single CH through a multi-CH scheme. Ogundoyin and Kamil presented a study to address security and privacy issues where fog servers can be used to process private and respond to time-sensitive information [27]. They applied the fuzzy AHP MCDM approach to determine and prioritize confidence parameters in fog computing. Their results indicate that quality of service is the best priority parameter that a service requester can use to evaluate the trusted standard of a service provider. Kumar et al. introduced a study to evaluate the impact of various malware analysis methods on the perspective of web applications [28]. They applied an MCDM approach that comprises AHP and TOPSIS methods under a fuzzy environment. Their results indicate that reverse engineering is the most effective method for analyzing complex malware.

There are many theories dealing with uncertainty, including the q-ROFS theory. Thus, we present some related studies as follows. Duane et al. introduced a study to deal with risks in information sharing and software piracy, which poses a threat to any system [29]. They applied the q-rung orthopair double hierarchy linguistic term set (q-RODHLTS) in the MCDM process. To prove the validity of their results, they applied the proposed approach to many information security systems. Panetikul et al. presented a study to analyze computer security threat analysis and control under a q-ROF environment [30].

They applied an approach based on the combination of the Heronian mean (HM) operator with complex q-ROFS is to initiate the complex q-rung orthopair fuzzy HM (Cq-ROFHM) operator. To prove the reliability and efficiency of the techniques used, some illustrative examples are introduced. Cheng et al. presented a study for evaluating sustainable enterprise risk management in manufacturing small and medium-sized enterprises [31]. They adopted a new extended Vlse Kriterijumska Optimizacija Kompromisno Resenje (VIKOR) approach using q-ROFSs. Peng et al. introduced a study for presenting a new score function of q-ROFN for solving the failure issues when comparing two q-ROFNs [32].

Finally, given the importance of IDSs and the importance of implementing them in a manner appropriate to their specific situation, choosing the most effective and appropriate one is a great challenge. Hence, there is an urgent and great need to evaluate IDSs. In this regard, a set of main and sub-criteria affecting the selection of the most effective IDS is identified; also, a set of alternatives are identified to be evaluated according to these criteria, using an MCDM approach and under a q-ROF environment.

3. Proposed Research Approach

3.1. Prelimianries

In this section, we list some concepts, procedures, and fundamental definitions related to IFSs, PFSs, and q-ROFSs.

3.1.1. Intuitionistic Fuzzy Sets

Atanassov developed IFSs as an extension of fuzzy set theory in 1986. IFSs are distinguished by the grade of membership and the grade of non-membership when their total is 1 or less than 1. It is explained as stated in Definition 1 [19].

Definition 1. *Let* X *a fixed set. An IFS* $\tilde{I}$ *in* X *is an entity having the form given by*

$$\tilde{I} = \{(\mathrm{x},\ \mu_{\tilde{I}}(\mathrm{x}),\ \upsilon_{\tilde{I}}(\mathrm{x}))|\ \mathrm{x} \in \mathrm{X}\} \tag{1}$$

where the function $\mu_{\tilde{I}}$*:* $\mathrm{X} \to$ *[0, 1] describes the grade of membership of an element to the sets* $\tilde{I}$ *and* $\upsilon_{\tilde{I}}$*:* $\mathrm{X} \to$ *[0, 1] describes the grade of non-membership of an element to the sets* $\tilde{I}$*, with the condition that*

$$0 \ \leq\ \mu_{\tilde{I}}(\mathrm{x}) + \upsilon_{\tilde{I}}(\mathrm{x}) \leq\ 1, \text{ for } \forall\ \mathrm{x} \in \mathrm{X} \tag{2}$$

The grade of hesitancy is computed as follows:

$$\Lambda\upsilon_{\tilde{I}}(\mathrm{x}) = 1 - \mu_{\tilde{I}}(\mathrm{x}) - \upsilon_{\tilde{I}}(\mathrm{x}) \tag{3}$$

Definition 2. *Let* $\widetilde{\mathbb{A}} = (\mu_{\widetilde{\mathbb{A}}}, \upsilon_{\widetilde{\mathbb{A}}})$ *and* $\widetilde{\mathbb{B}} = (\mu_{\widetilde{\mathbb{B}}}, \upsilon_{\widetilde{\mathbb{B}}})$ *be two intuitionistic fuzzy numbers (IFNs), then the addition and multiplication operations on these two IFNs as follows:*

$$\widetilde{\mathbb{A}} \oplus \mathbb{B} = (\mu_{\widetilde{\mathbb{A}}} + \widetilde{\mu_{\widetilde{\mathbb{B}}} - \mu_{\widetilde{\mathbb{A}}}\mu_{\widetilde{\mathbb{B}}}},\ \upsilon_{\widetilde{\mathbb{A}}}\upsilon_{\widetilde{\mathbb{B}}}) \tag{4}$$

$$\widetilde{\mathbb{A}} \otimes \widetilde{\mathbb{B}} = (\mu_{\widetilde{\mathbb{A}}}\mu_{\widetilde{\mathbb{B}}},\ \upsilon_{\widetilde{\mathbb{A}}} + \upsilon_{\widetilde{\mathbb{B}}} - \upsilon_{\widetilde{\mathbb{A}}}\upsilon_{\widetilde{\mathbb{B}}}) \tag{5}$$

3.1.2. Pythagorean Fuzzy Sets

Yager developed PFSs as an extension of the IFSs [20]. They are distinguished by two membership grades termed as membership and non-membership. The total membership and non-membership grades in PFSs are unlike in IFSs. In PFSs, the membership and non-membership grade may be more than 1, but the total of their squares has to be at most 1. It is explained as stated in Definition 3.

Definition 3. *Let be* X *a fixed set. A PFS* $\widetilde{P}$ *in* X *is an entity having the form given by*

$$\widetilde{\mathrm{P}} = \{(\mathrm{x},\ \mu_{\widetilde{\mathrm{P}}}(\mathrm{x}),\ \upsilon_{\widetilde{\mathrm{P}}}(\mathrm{x})) \mid \mathrm{x} \in \mathrm{X}\} \tag{6}$$

where the function $\mu_{\widetilde{\mathrm{P}}}$: X → *[0, 1] describes the grade of membership of an element* x ∈ X *to the sets* $\widetilde{\mathrm{P}}$ *and* $\upsilon_{\widetilde{\mathrm{P}}}$: X → *[0, 1] describes the grade of non-membership of an element* x ∈ X *to the sets* $\widetilde{\mathrm{P}}$*, with the condition that*

$$0 \leq (\mu_{\widetilde{\mathrm{P}}}(\mathrm{x}))^2 + (\upsilon_{\widetilde{\mathrm{P}}}(\mathrm{x}))^2 \leq 1, \text{ for } \forall\ \mathrm{x} \in \mathrm{X} \tag{7}$$

The grade of uncertainty is computed as follows:

$$\pi_{\widetilde{\mathrm{P}}}(\mathrm{x}) = \sqrt{1 - \mu_{\widetilde{\mathrm{P}}}(\mathrm{x})^2 - \upsilon_{\widetilde{\mathrm{P}}}(\mathrm{x})^2} \tag{8}$$

Definition 4. *Let* $\widetilde{\mathrm{P}}_1 = (\mu_{\widetilde{\mathrm{P}}_1}, \upsilon_{\widetilde{\mathrm{P}}_1})$ *and* $\widetilde{\mathrm{P}}_2 = (\mu_{\widetilde{\mathrm{P}}_2}, \upsilon_{\widetilde{\mathrm{P}}_2})$ *be two Pythagorean fuzzy numbers (PFNs), then the addition and multiplication operations on these two PFNs as follows:*

$$\widetilde{\mathrm{P}}_1 \oplus \widetilde{\mathrm{P}}_2 = \left(\sqrt{{\mu_{\widetilde{\mathrm{P}}_1}}^2 + {\mu_{\widetilde{\mathrm{P}}_2}}^2 - {\mu_{\widetilde{\mathrm{P}}_1}}^2 {\mu_{\widetilde{\mathrm{P}}_2}}^2}, \upsilon_{\widetilde{\mathrm{P}}_1} \upsilon_{\widetilde{\mathrm{P}}_2}\right) \tag{9}$$

$$\widetilde{\mathrm{P}}_1 \otimes \widetilde{\mathrm{P}}_2 = \left(\mu_{\widetilde{\mathrm{P}}_1} \mu_{\widetilde{\mathrm{P}}_2}, \sqrt{{\upsilon_{\widetilde{\mathrm{P}}_1}}^2 + {\upsilon_{\widetilde{\mathrm{P}}_2}}^2 - {\upsilon_{\widetilde{\mathrm{P}}_1}}^2 {\upsilon_{\widetilde{\mathrm{P}}_2}}^2}\right) \tag{10}$$

3.1.3. Q-Rung Orthopair Fuzzy Sets

Yager presented q-ROFSs in 2018 with the grade of membership and non-membership. In q-ROFSs, the total of the qth power of the membership and non-membership grades should be at most equal to 1 [18]. In Figure 2, it is readily noted that q-ROFSs have a reasonable membership degree extent greater than that of the IFSs and PFSs. q-ROFSs are explained as stated in Definition 5.

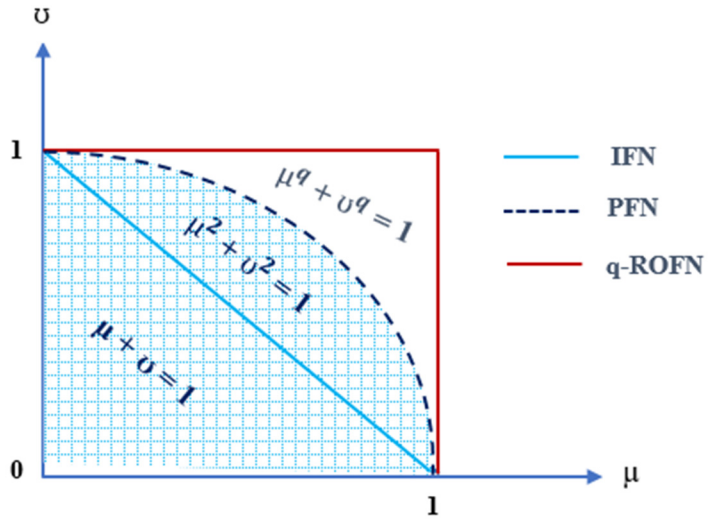

Figure 2. Comparison of the geometric area of various fuzzy membership degrees: IFNs, PFNs, and q-ROFNs.

Definition 5. *A q-ROFS* $\breve{\mathfrak{Q}}$ *in a finite universe of discourse* X = $x_1, x_2, \ldots, x_n$ *is defined by Yager as follows [18]:*

$$\breve{\mathfrak{Q}} = \{(\mathrm{x},\ \mu_{\breve{\mathfrak{Q}}}(\mathrm{x}), \upsilon_{\breve{\mathfrak{Q}}}(\mathrm{x})) \mid \mathrm{x} \in \mathrm{X}\} \tag{11}$$

where the function $\mu_{\widetilde{\mathfrak{Q}}}$: $X \rightarrow [0, 1]$ *defines the grade of membership of an element* $x \in X$ *to the sets* $\widetilde{\mathfrak{Q}}$ *and* $\upsilon_{\widetilde{\mathfrak{Q}}}$: $X \rightarrow [0, 1]$ *defines the grade of non-membership of an element* $x \in X$ *to the sets* $\widetilde{\mathfrak{Q}}$, *with the condition that*

$$0 \leq \mu_{\widetilde{\mathfrak{Q}}}(x)^q + \upsilon_{\widetilde{\mathfrak{Q}}}(x)^q \leq 1, \text{ for } \forall\, x \in X \tag{12}$$

The grade of uncertainty is computed as follows

$$\pi_{\widetilde{\mathfrak{Q}}}(x) = \sqrt[q]{1 - \mu_{\widetilde{\mathfrak{Q}}}(x)^q - \upsilon_{\widetilde{\mathfrak{Q}}}(x)^q} \tag{13}$$

Definition 6. *Let* $\breve{\mathfrak{Q}} = (\mu_{\widetilde{\mathfrak{Q}}}, \upsilon_{\widetilde{\mathfrak{Q}}})$, $\breve{\mathfrak{Q}}_1 = (\mu_{\widetilde{\mathfrak{Q}}_1}, \upsilon_{\widetilde{\mathfrak{Q}}_1})$, $\breve{\mathfrak{Q}}_2 = (\mu_{\widetilde{\mathfrak{Q}}_2}, \upsilon_{\widetilde{\mathfrak{Q}}_2})$, *be three q-ROFNs, then their procedures can be well-defined as follows [18]:*

$$\breve{\mathfrak{Q}}_1 \cap \breve{\mathfrak{Q}}_2 = (\min\{\mu_{\widetilde{\mathfrak{Q}}_1}, \mu_{\widetilde{\mathfrak{Q}}_2}\}, \max\{\upsilon_{\widetilde{\mathfrak{Q}}_1}, \upsilon_{\widetilde{\mathfrak{Q}}_2}\}) \tag{14}$$

$$\breve{\mathfrak{Q}}_1 \cup \breve{\mathfrak{Q}}_2 = (\max\{\mu_{\widetilde{\mathfrak{Q}}_1}, \mu_{\widetilde{\mathfrak{Q}}_2}\}, \min\{\upsilon_{\widetilde{\mathfrak{Q}}_1}, \upsilon_{\widetilde{\mathfrak{Q}}_2}\}) \tag{15}$$

$$\breve{\mathfrak{Q}}_1 \oplus \breve{\mathfrak{Q}}_2 = \left(\left(\mu_{\widetilde{\mathfrak{Q}}_1}{}^q + \mu_{\widetilde{\mathfrak{Q}}_2}{}^q - \mu_{\widetilde{\mathfrak{Q}}_1}{}^q \mu_{\widetilde{\mathfrak{Q}}_2}{}^q\right)^{\frac{1}{q}}, \upsilon_{\widetilde{\mathfrak{Q}}_1} \upsilon_{\widetilde{\mathfrak{Q}}_2}\right) \tag{16}$$

$$\breve{\mathfrak{Q}}_1 \otimes \breve{\mathfrak{Q}}_2 = \left(\mu_{\widetilde{\mathfrak{Q}}_1} \mu_{\widetilde{\mathfrak{Q}}_2}, \left(\upsilon_{\widetilde{\mathfrak{Q}}_1}{}^q + \upsilon_{\widetilde{\mathfrak{Q}}_2}{}^q - \upsilon_{\widetilde{\mathfrak{Q}}_1}{}^q \upsilon_{\widetilde{\mathfrak{Q}}_2}{}^q\right)^{\frac{1}{q}}\right) \tag{17}$$

$$\lambda\breve{\mathfrak{Q}} = \left((1 - (1 - \mu_{\breve{\mathfrak{Q}}}{}^q)^\lambda)^{\frac{1}{q}}, \upsilon_{\breve{\mathfrak{Q}}}{}^\lambda\right), \ \lambda > 0 \tag{18}$$

$$\breve{\mathfrak{Q}}^\lambda = \left(\mu_{\breve{\mathfrak{Q}}}{}^\lambda, (1 - (1 - \upsilon_{\breve{\mathfrak{Q}}}{}^q)^\lambda)^{\frac{1}{q}}\right), \ \lambda > 0 \tag{19}$$

Definition 7. *Let* $\breve{\mathfrak{Q}} = (\mu_{\widetilde{\mathfrak{Q}}}, \upsilon_{\widetilde{\mathfrak{Q}}})$ *be a q-ROFN; the score function* $S(\breve{\mathfrak{Q}})$ *of* $\breve{\mathfrak{Q}}$ *can be expressed as in [33], and the accuracy function* $A(\breve{\mathfrak{Q}})$ *of* $\breve{\mathfrak{Q}}$ *can be well defined, as in [34], shown by Equations (20) and (21), respectively.*

$$S(\breve{\mathfrak{Q}}) = \frac{1}{2}(1 + \mu_{\breve{\mathfrak{Q}}}{}^q - \upsilon_{\breve{\mathfrak{Q}}}{}^q) \tag{20}$$

$$A(\breve{\mathfrak{Q}}) = \mu_{\breve{\mathfrak{Q}}}{}^q + \mathfrak{Q}_{\breve{\mathfrak{Q}}}{}^q \tag{21}$$

Definition 8. *Let* $\breve{\mathfrak{Q}}_i = (\mu_{\widetilde{\mathfrak{Q}}_i}, \upsilon_{\widetilde{\mathfrak{Q}}_i})$ *(i = 1, 2, … n) be set of q-ROFNs and* $W = (w_1, w_2, \ldots, w_n)^T$ *be weight vector of* $\breve{\mathfrak{Q}}_i$ *with* $\sum_{i=1}^n W_i = 1$ *and* $W_i \in [0, 1]$. *Q-rung orthopair fuzzy weighted average (q-ROFWA) and q-rung orthopair fuzzy weighted geometric (q-ROFWG) operators can be expressed as in [34], shown by Equations (22) and (23), respectively.*

$$\text{q-ROFWA}\left(\breve{\mathfrak{Q}}_1, \breve{\mathfrak{Q}}_2, \ldots, \breve{\mathfrak{Q}}_n\right) = \left(\left(1 - \prod_{i=1}^n \left(1 - \mu_{\widetilde{\mathfrak{Q}}_i}{}^q\right)^{w_i}\right)^{\frac{1}{q}}, \prod_{i=1}^n \upsilon_{\widetilde{\mathfrak{Q}}_i}{}^{w_i}\right) \tag{22}$$

$$\text{q-ROFWA}\left(\breve{\mathfrak{Q}}_1, \breve{\mathfrak{Q}}_2, \ldots, \breve{\mathfrak{Q}}_n\right) = \left(\prod_{i=1}^n \mu_{\widetilde{\mathfrak{Q}}_i}{}^{W_i}, \left(1 - \prod_{i=1}^n \left(1 - \upsilon_{\widetilde{\mathfrak{Q}}_i}{}^q\right)^{W_i}\right)^{\frac{1}{q}}\right) \tag{23}$$

Definition 9. *Darko and Liang developed an operator named the weighted q-rung orthopair fuzzy Hamacher average (Wq-ROFHA) [35] as in Equations (24) and (25). Let* $\breve{\mathfrak{Q}}_i = (\mu_{\widetilde{\mathfrak{Q}}_i}, \upsilon_{\widetilde{\mathfrak{Q}}_i})$ *(i = 1, 2,*

... n) be set of q-ROFNs and $\mathrm{W} = (\mathrm{w}_1, \mathrm{w}_2, \ldots, \mathrm{w}_n)^T$ *be a weight vector of* $\breve{\mathfrak{Q}}_i$ *with* $\sum_{i=1}^{n} \mathrm{W}_i = 1$ *and* $\mathrm{W}_i \in [0, 1]$.

$$\text{Wq-ROFHA}(\breve{\mathfrak{Q}}_1, \breve{\mathfrak{Q}}_2, \ldots, \breve{\mathfrak{Q}}_n) = \mathrm{w}_1(\breve{\mathfrak{Q}}_1) \oplus \mathrm{w}_2(\breve{\mathfrak{Q}}_2) \oplus \ldots \oplus \mathrm{w}_n(\breve{\mathfrak{Q}}_n) = \bigoplus_{i=1}^{n} \mathrm{w}_i(\breve{\mathfrak{Q}}_i) \tag{24}$$

$$\text{Wq-ROFHA}(\breve{\mathfrak{Q}}_1, \breve{\mathfrak{Q}}_2, \ldots, \breve{\mathfrak{Q}}_n) = \left(\sqrt[q]{\frac{\prod_{i=1}^{n}\left(1+(\gamma-1)\left(\mu_{\breve{\mathfrak{Q}}_i}\right)^q\right)^{\mathrm{W}_i} - \prod_{i=1}^{n}\left(1-\left(\mu_{\breve{\mathfrak{Q}}_i}\right)^q\right)^{\mathrm{W}_i}}{\prod_{i=1}^{n}\left(1+(\gamma-1)\left(\mu_{\breve{\mathfrak{Q}}_i}\right)^q\right)^{\mathrm{W}_i} + (\gamma-1)\prod_{i=1}^{n}\left(1-\left(\mu_{\breve{\mathfrak{Q}}_i}\right)^q\right)^{\mathrm{W}_i}}} \; \frac{\sqrt[q]{\gamma}\prod_{i=1}^{n}\left(\upsilon_{\tilde{\mathfrak{Q}}_i}\right)^{\mathrm{W}_i}}{\sqrt[q]{\prod_{i=1}^{n}\left(1+(\gamma-1)\left(1-\left(\upsilon_{\tilde{\mathfrak{Q}}_i}\right)^q\right)\right)^{\mathrm{W}_i} + (\gamma-1)\prod_{i=1}^{n}\left(\upsilon_{\tilde{\mathfrak{Q}}_i}\right)^{q\mathrm{W}_i}}} \right) \tag{25}$$

where $\gamma > 0$, $q \geq 0$.

Definition 10. *Darko and Liang presented an operator named the weighted q-rung orthopair fuzzy Hamacher geometric mean (Wq-ROFHGM) [35], as in Equations (26) and (27). Let* $\breve{\mathfrak{Q}}_i = (\mu_{\tilde{\mathfrak{Q}}_i}, \upsilon_{\tilde{\mathfrak{Q}}_i})$ *(i = 1, 2, ... n) be set of q-ROFNs and* $\mathrm{W} = (\mathrm{w}_1, \mathrm{w}_2, \ldots, \mathrm{w}_n)^T$ *be the weight vector of* $\breve{\mathfrak{Q}}_i$ *with* $\sum_{i=1}^{n} \mathrm{W}_i = 1$ *and* $\mathrm{W}_i \in [0, 1]$.

$$\text{Wq-ROFHGM}(\breve{\mathfrak{Q}}_1, \breve{\mathfrak{Q}}_2, \ldots, \breve{\mathfrak{Q}}_n) = \mathrm{w}_1(\breve{\mathfrak{Q}}_1) \oplus \mathrm{w}_2(\breve{\mathfrak{Q}}_2) \oplus \ldots \oplus \mathrm{w}_n(\breve{\mathfrak{Q}}_n) = \bigoplus_{i=1}^{n} \mathrm{w}_i(\breve{\mathfrak{Q}}_i) \tag{26}$$

$$\text{Wq-ROFHGM}(\breve{\mathfrak{Q}}_1, \breve{\mathfrak{Q}}_2, \ldots, \breve{\mathfrak{Q}}_n) = \left(\frac{\sqrt[q]{\gamma}\prod_{i=1}^{n}\left(\mu_{\tilde{\mathfrak{Q}}_i}\right)^{\mathrm{W}_i}}{\sqrt[q]{\prod_{i=1}^{n}\left(1+(\gamma-1)\left(1-\left(\mu_{\tilde{\mathfrak{Q}}_i}\right)^q\right)\right)^{\mathrm{W}_i} + (\gamma-1)\prod_{i=1}^{n}\left(\mu_{\tilde{\mathfrak{Q}}_i}\right)^{q\mathrm{W}_i}}} \; \sqrt[q]{\frac{\prod_{i=1}^{n}\left(1+(\gamma-1)\left(\upsilon_{\breve{\mathfrak{Q}}_i}\right)^q\right)^{\mathrm{W}_i} - \prod_{i=1}^{n}\left(1-\left(\upsilon_{\breve{\mathfrak{Q}}_i}\right)^q\right)^{\mathrm{W}_i}}{\prod_{i=1}^{n}\left(1+(\gamma-1)\left(\upsilon_{\breve{\mathfrak{Q}}_i}\right)^q\right)^{\mathrm{W}_i} + (\gamma-1)\prod_{i=1}^{n}\left(1-\left(\upsilon_{\breve{\mathfrak{Q}}_i}\right)^q\right)^{\mathrm{W}_i}}} \right) \tag{27}$$

where $\gamma > 0$, $q \geq 0$.

3.2. Suggested Approach

In this part, a sequential multi-step approach is presented to evaluate several intrusion-detection systems by combining two MCDM methods, namely, Entropy-CoCoSo. The proposed approach was performed under the q-rung orthopair fuzzy environment and by using q-ROFNs. The proposed approach was divided into three main parts. The data aggregation part includes identifying experts, selecting the criteria used, and determining the IDSs alternatives available. Then, the criteria evaluation part assesses the selected criteria using the q-ROF Entropy method. After that, the alternatives evaluation part assesses the available IDSs using the q-ROF CoCoSo method. The steps of the proposed approach are shown in Figure 3. Consequently, the steps of the suggested approach used are presented in detail as follows:

Step 1. The problem was studied and its main and sub-aspects were identified. The basic criteria for selecting the participating experts also were established. The criteria for selecting experts were determined as follows: the participants should have sufficient experience in the field of cyber security and the field of information security in general; also, their experience in the field of information security should not be less than 10 years. In addition, the participants should have practical experience in the field of information security technology and in the academic field. Next, the number of experts ($\mathrm{EX_s}$) participating in the study was considered. After that, the participating experts were divided into several groups and the appropriate weight for each group was determined according to the measure of experience. Finally, the most appropriate means of communication with the participating experts were determined.

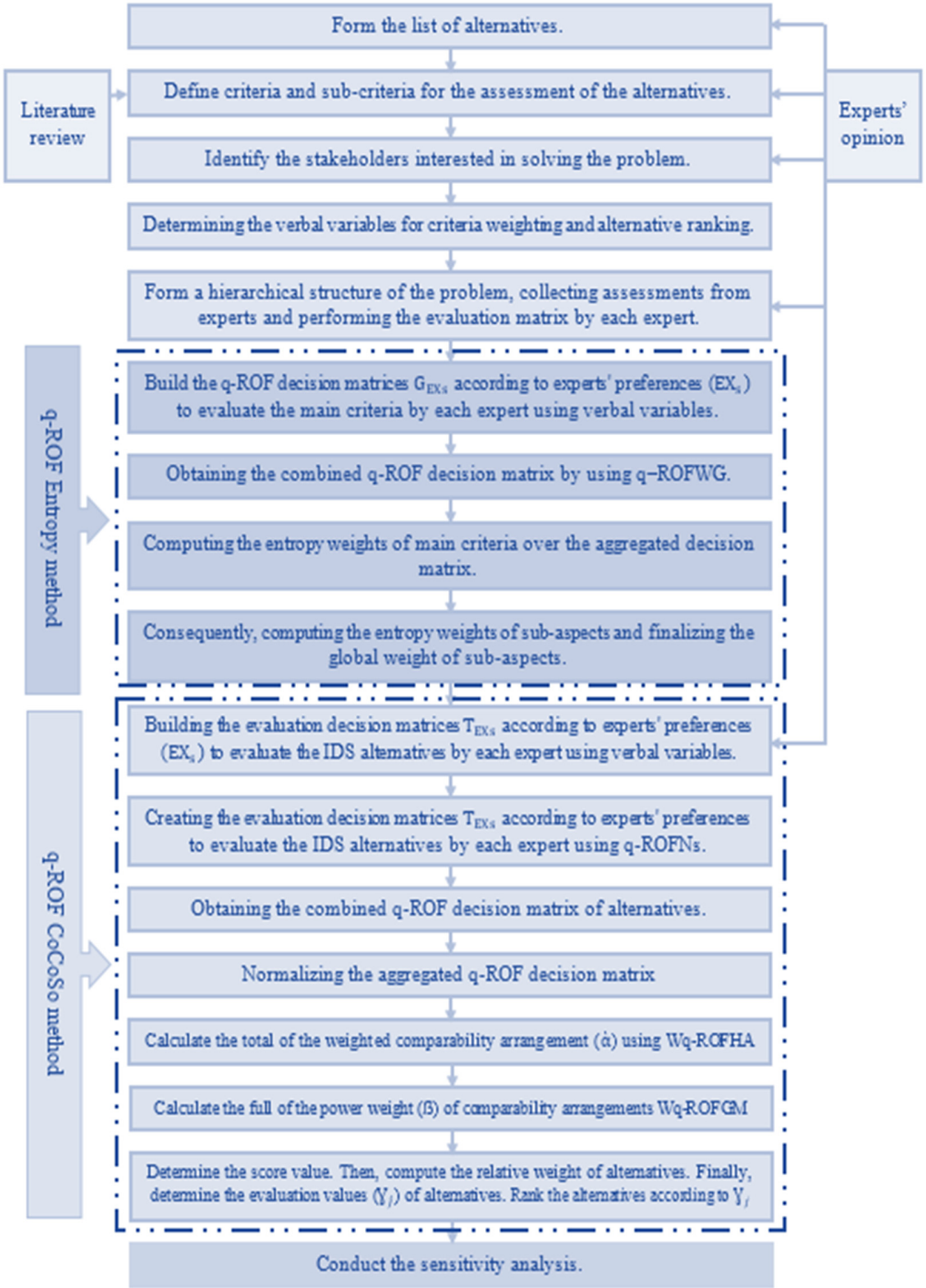

Figure 3. Decision framework for IDS evaluation.

Step 2. The main criteria and their sub-aspects used in the study were determined based on an analysis of the relevant literature, as well as insight from the participating experts. $C_j = \{C_1, C_2, \ldots, C_n\}$, with $j = 1, 2 \ldots n$. Let $W = (w_1, w_2, \ldots, w_n)$ be the vector set utilized for determining the criteria weights, where $w_j > 0$ and $\sum_{j=1}^{n} w_j = 1$.

Step 3. After studying the problem and its details and identifying the most important criteria, the available alternatives were determined to be used in the study. After that, experts' opinions were taken on the selected alternatives and a final list of alternatives to be used in the evaluation process was prepared. The set $A_i = \{A_1, A_2, \ldots, A_m\}$, having

i = 1, 2,..,m alternatives, was evaluated by n decision criteria of set $C_j = \{C_1, C_2, \ldots, C_n\}$, with j = 1, 2, . . . , n.

Step 4. After defining the main criteria and their sub-aspects and adopting a set of final alternatives, all these aspects were organized in the form of a hierarchical structure. This hierarchy shows the main objective of the problem, the criteria used, and the alternatives determined.

Step 5.Verbal variants and their equivalent q-ROFNs were identified. These variables were used in the evaluation process to assist the participating experts. These variants were divided into two parts in the same table. The first part refers to the variables that are used in evaluating the main criteria and their sub-aspects. The second part refers to the variables that are used in evaluating the available alternatives, as shown in Table 1.

Table 1. Verbal variables and their corresponding q-ROFNs for the weighting criteria and ranking alternatives.

Verbal Variables for Criteria	Abbreviations for Criteria	Verbal Variables for Alternatives	Abbreviations for Alternatives	q-ROFNs	
				μ	υ
Extremely poor	ELP	Extremely low	EXO	0.11	0.99
Very poor	VPO	Very low	VLO	0.22	0.88
Poor	POO	Low	LLO	0.33	0.77
Medium poor	MDP	Medium low	MEL	0.44	0.66
Fair	FAR	Medium	MED	0.55	0.55
Medium good	MDG	Medium high	MEH	0.66	0.44
Good	GOO	High	HGH	0.77	0.33
Very good	VGO	Very high	VEH	0.88	0.22
Extremely good	EXG	Extremely high	EXH	0.99	0.11

Step 6. Build the q-ROF decision matrices, G_{EXs}, according to experts' preferences (EX_s) to evaluate the criteria by each expert using verbal variables in Table 1, and then by using q-rung orthopair fuzzy scale q-ROFNs, as shown in Table 2.

Table 2. The evaluation matrix for criteria based on q-ROFN with respect to experts.

Criteria	Experts			
	Ex_1	Ex_2	Ex_3	Ex_4
C_1	$[\mu_{1Ex_1}, \upsilon_{1Ex_1}]$	$[\mu_{1Ex_2}, \upsilon_{1Ex_2}]$	$[\mu_{1Ex_3}, \upsilon_{1Ex_3}]$	$[\mu_{1Ex_4}, \upsilon_{1Ex_4}]$
C_2	$[\mu_{2Ex_1}, \upsilon_{2Ex_1}]$	$[\mu_{2Ex_2}, \upsilon_{2Ex_2}]$	$[\mu_{2Ex_3}, \upsilon_{2Ex_3}]$	$[\mu_{2Ex_4}, \upsilon_{2Ex_4}]$
⋮	⋮	⋮	⋮	⋮
C_n	$[\mu_{nEx_1}, \upsilon_{nEx_1}]$	$[\mu_{nEx_2}, \upsilon_{nEx_2}]$	$[\mu_{nEx_3}, \upsilon_{nEx_3}]$	$[\mu_{nEx_4}, \upsilon_{nEx_4}]$

Step 7. Aggregate the evaluations on criteria weights. The individual expert evaluations are collected by using q−ROFWG given in Equation (23). Here $(w_j)_{1\times n}$, presents the q-ROF weight of the *j*th criterion.

Step 8. The steps of the entropy method based on q-ROFSs are applied to evaluate and weight the main criteria and their sub-aspects [36]. Compute the entropy values of each q-ROFN of the aggregated experts' evaluations by applying Equations (28) and (29).

$$KE_{q,ij}(x) = \frac{1}{\sqrt{2}} \sqrt{((\mu(x))^q)^2 + ((\upsilon(x))^q)^2 + ((\mu(x))^q + (\upsilon(x))^q)^2} \quad (28)$$

$$EN_{q,ij}(x) = 1 - KE_{q,ij}(x) = 1 - \frac{1}{\sqrt{2}} \sqrt{((\mu(x))^q)^2 + ((\upsilon(x))^q)^2 + ((\mu(x))^q + (\upsilon(x))^q)^2} \quad (29)$$

Step 9. The main criteria weights are calculated based on the entropy values using Equation (30).

$$\mathrm{w_j} = \frac{1-\mathcal{E}_\mathrm{j}}{\sum_{j=1}^{n}(1-\mathcal{E}_\mathrm{j})};\ \mathrm{j} = 1,\ 2, \ldots\ \mathrm{n} \tag{30}$$

where $\mathcal{E}_\mathrm{j} = \frac{\sum_{i=1}^{m} \mathrm{EN_{q,ij}}}{\sum_{i=1}^{m}\sum_{j=1}^{n}.\mathrm{EN_{q,ij}}}$ refers to the q-ROF entropy value.

Step 10. In the same way, the weights of the sub-aspects of the main criteria are calculated as in Steps 6–9.

Step 11. A q-ROF evaluation decision matrix (T_{EX}) is generated by each expert (EX) individually among the selected sub-aspects and alternatives to determine the best intrusion-detection system through the use of verbal variables, as shown in Table 1, and then by using the q-ROFNs in Table 1, as shown in Table 3. Here, $\check{T}_{EX} = \left(\check{t}_{ijEX}\right)_{n\times m}$, in which $\check{t}_{ijEX} = \left[\mu_{ijEX}, \upsilon_{ijEX}\right]$ is created by applying the verbal variables in Table 1. Consequently, $\check{t}_{ijEX}$ refers the performance of intrusion-detection systems (alternatives) $\mathrm{A_i}$ according to criteria $\mathrm{C_j}$ of the $\mathrm{EX^{th}}$ expert.

Table 3. Decision evaluation matrix for alternatives in terms of criteria based on q-ROFN.

Criteria	**Alternatives (Intrusion-Detection Systems)**			
	$\mathbf{A_1}$	$\mathbf{A_2}$	...	$\mathbf{A_m}$
$\mathrm{C_1}$	$[\mu_{11\mathrm{Ex}}, \upsilon_{11\mathrm{Ex}}]$	$[\mu_{12\mathrm{Ex}}, \upsilon_{12\mathrm{Ex}}]$	...	$[\mu_{1\mathrm{mEx}}, \upsilon_{1\mathrm{mEx}}]$
$\mathrm{C_2}$	$[\mu_{21\mathrm{Ex}}, \upsilon_{21\mathrm{Ex}}]$	$[\mu_{22\mathrm{Ex}}, \upsilon_{22\mathrm{Ex}}]$	...	$[\mu_{2\mathrm{mEx}}, \upsilon_{2\mathrm{mEx}}]$
⋮	⋮	⋮	⋱	⋮
$\mathrm{C_n}$	$[\mu_{n1\mathrm{Ex}}, \upsilon_{n1\mathrm{Ex}}]$	$[\mu_{n2\mathrm{Ex}}, \upsilon_{n2\mathrm{Ex}}]$	...	$[\mu_{\mathrm{nmEx}}, \upsilon_{\mathrm{nmEx}}]$

Step 12. After the q-ROF evaluation decision matrix (T_{EX}) is generated by each expert (EX) between the sub-aspects and the available alternatives by all experts, the q-ROF evaluation decision matrices (T_{EXs}) were aggregated into one matrix by utilizing q−ROFWG, as presented in Equation (23). A combined q-ROF evaluation decision matrix ($\check{T}$) was created as in Table 4. Accordingly, $\check{T} = \left(\check{t}_{ij}\right)_{n\times m}$ in which $\check{t}_{ij} = \left[\mu_{ij}, \upsilon_{ij}\right]$ is utilized to refer to the combined q-ROFN of the ith substitute with regard to the jth criteria.

Table 4. Combined evaluation matrix for alternatives in terms of the criteria based on q-ROFN.

Criteria	**Alternatives (Intrusion-Detection Systems)**			
	$\mathbf{A_1}$	$\mathbf{A_2}$	**...**	$\mathbf{A_m}$
$\mathrm{C_1}$	$[\mu_{11}, \upsilon_{11}]$	$[\mu_{12}, \upsilon_{12}]$	...	$[\mu_{1\mathrm{m}}, \upsilon_{1\mathrm{m}}]$
$\mathrm{C_2}$	$[\mu_{21}, \upsilon_{21}]$	$[\mu_{22}, \upsilon_{22}]$	...	$[\mu_{2\mathrm{m}}, \upsilon_{2\mathrm{m}}]$
⋮	⋮	⋮	⋱	⋮
C_n	$[\mu_{n1}, \upsilon_{n1}]$	$[\mu_{n2}, \upsilon_{n2}]$	...	$[\mu_{\mathrm{nm}}, \upsilon_{\mathrm{nm}}]$

Step 13. Compute the normalized aggregated q-ROF evaluation decision matrix ($\check{H}$) by applying Equation (31).

$$\check{H} = \left(\check{h}_{ij}\right)_{m\times n} = \left[\breve{\mu}_{ij}, \breve{\upsilon}_{ij}\right] = \begin{cases} \left(\breve{\mu}_{ij}, \breve{\upsilon}_{ij}\right) if\ i\ \in \mathbb{B} \\ \left(\breve{\upsilon}_{ij}, \breve{\mu}_{ij}\right) if\ i\ \in \mathbb{C} \end{cases} \tag{31}$$

where $\mathbb{B}$ refers to the set of benefit criteria and $\mathbb{C}$ refers to the set of cost criteria.

Step 14. Calculate the total of the weighted comparability arrangement ($\acute{\alpha}$) for all substitutes by applying the Wq-ROFHA operator as presented in Equations (24) and (25).

Step 15. Calculate the full of the power weight (ß) of comparability arrangements for all substitutes by applying the Wq-ROFHGM operator as exhibited in Equations (26) and (27).

Step 16. Determine the score values of the substitutes by applying the values of values of the Wq-ROFHA and Wq-ROFHGM operators for each substitute by applying Equation (20).

Step 17. Calculate the proportional weight of the substitutes with the assistance of Equations (32)–(34).

$$\gamma_{ja} = \frac{\acute{\alpha}_j + ß_j}{\sum_{j=1}^{n}(\acute{\alpha}_j + ß_j)} \tag{32}$$

$$\gamma_{jb} = \frac{\acute{\alpha}_j}{\min(\acute{\alpha}_j)} + \frac{ß_j}{\min(ß_j)} \tag{33}$$

$$\gamma_{jc} = \frac{\Psi\acute{\alpha}_j + (1-\Psi)ß_j}{\Psi\max(\acute{\alpha}_j) + (1-\Psi)\max(ß_j)}; 0 \le \Psi \le 1 \tag{34}$$

where γ_{ja} refers to the arithmetic mean of sums of the weighted sum method (WSM) and weighted product model (WPM) scores. Then, γ_{jb} indicates the sum of proportional scores of WSM and WPM. γ_{jc} also refers to the stable adjustment of the WSM and WPM models scores.

Step 18. Determine the evaluation values (γ_j) of the substitutes by applying Equation (35). Then, rank the available intrusion-detection systems according to the most possible value of the evaluation values (γ_j).

$$\gamma_j = \sqrt[3]{\gamma_{ja}\gamma_{jb}\gamma_{jc}} + \frac{\gamma_{ja} + \gamma_{jb} + \gamma_{jc}}{3} \tag{35}$$

4. Empirical Results and Interpretation

In this section, the steps of the proposed multistep hybrid MCDM approach consisting of Entropy-CoCoSo methods are applied to evaluate the efficiency and reliability of some IDSs. The proposed approach was applied under the q-rung orthopair fuzzy environment and by using q-ROFNs. In this regard, the process of evaluating intrusion-detection systems and selecting the most effective and reliable one is necessary and inevitable in light of the recent cyber-attacks and intrusion methods. In this regard, the intrusion-detection systems are revealed in the next sub-section.

4.1. Description of Intrusion-Detection Systems

In this subsection, a brief description of the intrusion-detection systems are considered; also, Figure 4 demonstrates the general structure of the network and IDS.

- **Suricata (IDS_1):** Suricata was developed by the Open Information Security Foundation in 2010. Suricata is the main alternative to Snort because the design of Suricata is very close to that of Snort [37]. Suricata has an advantage over Snort, which is that it collects data at the application layer. Suricata consists of so-called threads, thread units, and queues. Suricata is a multi-threaded program, so there will be multiple threads running at the same time [37]. Thread units are divided according to functions; for example, one unit is used to analyze data packets, and the other unit is used to discover data packets. Each data packet can be processed by several different threads, and the queue is used to transfer the data packet from one thread to another. At the same time, a thread can contain several thread units, but only one unit runs at a given time.

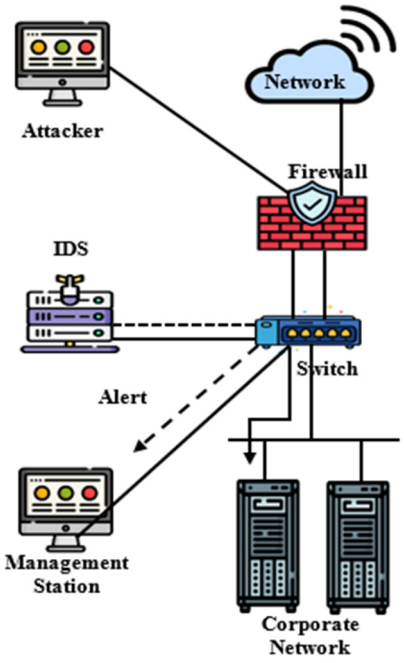

Figure 4. The general structure of the network and IDS.

- **Zeek (IDS_2):** Zeek (previously known as Bro until 2019) is a network intrusion-detection system that is compatible with Linux, Unix, and Mac OS [38]. Zeek uses network-based intrusion-detection methods by tracking the network and searching for malicious activities. The Zeek intrusion detection function is realized in two stages: traffic logging, and analysis. As with Suricata, Zeek has a significant advantage over Snort in that its analysis runs at the application layer, resulting in a broader analysis of network protocol activity.
- **Security onion (IDS_3):** Security Onion is a Linux-based IDS that is a mixture of several IDS that are both HIDS and NIDS solutions [16]. Although Security Onion is classified as NIDS, it includes HIDS functionality as well. It monitors log and configuration files for suspicious activity and checks those files for any unexpected changes. One of the downsides to Security Onion's comprehensive network monitoring system is its complexity. Thus, the Security Onion analysis engine is where things get complicated because there are so many different tools with different operating procedures that most of them may end up being overlooked.
- **Snort (IDS_4):** Snort is a Linux-based lightweight cross-platform network intrusion-detection system that can be used to monitor TCP/IP networks [39]. Snort is easy to deploy and can be configured to monitor network traffic for intrusion attempts, log intrusion behavior, and perform specific actions when intrusion attempts are detected. It is one of the most widely deployed IDS tools and can also be used as an intrusion-prevention system. Snort can be traced back to 1998, and there are still no signs of disappearing. There are some active communities that offer good help and support. The high level of personalization that Snort provides makes it a good choice for many different organizations.
- **Wazuh (IDS_5):** Wazuh is an IDS used to detect security and monitor compliance with security rules. Wazuh is an open-source intrusion-detection system project. It was developed as a fork part of OSSEC HIDS and was later integrated with Elastic Stack and Opens CAP. It relies on a cross-platform approach that redirects system data such as log messages, file tables, and detected anomalies to a central manager, where it is further analyzed and processed, resulting in security alerts. It monitors the file system and identifies changes in content, permissions, ownership, and file properties that

need to be monitored. It monitors configuration files to ensure that they comply with security policies, standards, or hardening guides.

- **OSSEC (IDS_6):** OSSEC is an open source IDS developed by Daniel B. Cid, who had sold the system to Trend Micro in 2008 [39]. Its detection methods are based on checking log files, making it a host-based IDS. OSSEC works on Unix, Linux, Mac OS, and Windows. There is no front end for this tool, but you can connect with Kibana or Graylog. OSSEC disclosure rules are called 'Policies'. You can write your own policies or get packages of them for free from the user community. It is also possible to define actions that should be performed automatically when specific warnings appear.

4.2. Application of the Proposed Approach

In this sub-section, the steps for evaluating the selected intrusion-detection systems through the Entropy-CoCoSo approach are presented as follows:

Step 1. Initially, a set of standards was identified to select the experts involved with the researchers in the study to evaluate the IDSs. The standards were as follows: the number of years of experience should not be less than 10 years in the field of cyber security and the field of information security in general; also, the scientific degree of the participating experts must not be lower than M.Sc. Accordingly, 60 experts were selected to participate in the IDSs evaluation process. After that, the participating experts were divided into four groups. Each group included a certain number of experts. The first and fourth groups included 12 experts. Whereas, the second and third groups included 18 experts. Accordingly, the appropriate weight was assigned to each group according to the years of experience and the number of experts. So, the first, second, third, and fourth groups had weights of 0.20, 0.30, 0.30, and 0.20, respectively. In addition, a leader was assigned to each group to express the final opinion in the evaluation process. Finally, the experts were contacted online.

Step 2. Based on the literature analysis and expert review, a set of main and sub-criteria were defined to evaluate the effectiveness and reliability of the IDSs. Initially, four main criteria were defined, which are as follows: protected system, PSC_1; audit source location, ASC_2; targets, TGC_3; and types, TPC_4. The main criteria also contained several sub-criteria, as follows: HIDS (HIC_{1_1}), NIDS (NIC_{1_2}), hybrids (HYC_{1_3}), host log files (HLC_{2_1}), network packets (NPC_{2_2}), application log files (ALC_{2_3}), IDS sensors alerts (ISC_{2_4}), applications (APC_{3_1}), network (NEC_{3_2}), host (HOC_{3_3}), open source (OSC_{4_1}), closed source (CSC_{4_2}), and freeware (CSC_{4_2}).

Step 3. A definitive list of available IDSs for use was prepared, as follows: Suricata (IDS_1), Zeek (IDS_2), Security onion (IDS_3), Snort (IDS_4), Wazuh (IDS_5), and OSSEC (IDS_6).

Step 4. A final hierarchical form of the problem was prepared, defining the main objective of the study, which was to evaluate the effectiveness of several IDSs, as shown in Figure 5; this in addition to regulating the relationship between the basic criteria and their sub-aspects, with the IDSs used as alternatives.

Step 5. A set of verbal variants and their equivalent q-ROFNs were prepared by reviewing the previous literature and expert opinions. Verbal variants were divided into two parts. The first part of the verbal variants is presented in Table 1, to assess the main criteria and their sub-aspects. The second part of the verbal variants is presented in Table 1, to evaluate the alternatives used.

Step 6. The decision matrix was built with the help of Table 2 by the four experts to assess the main criteria using the verbal variables as shown in Table 5.

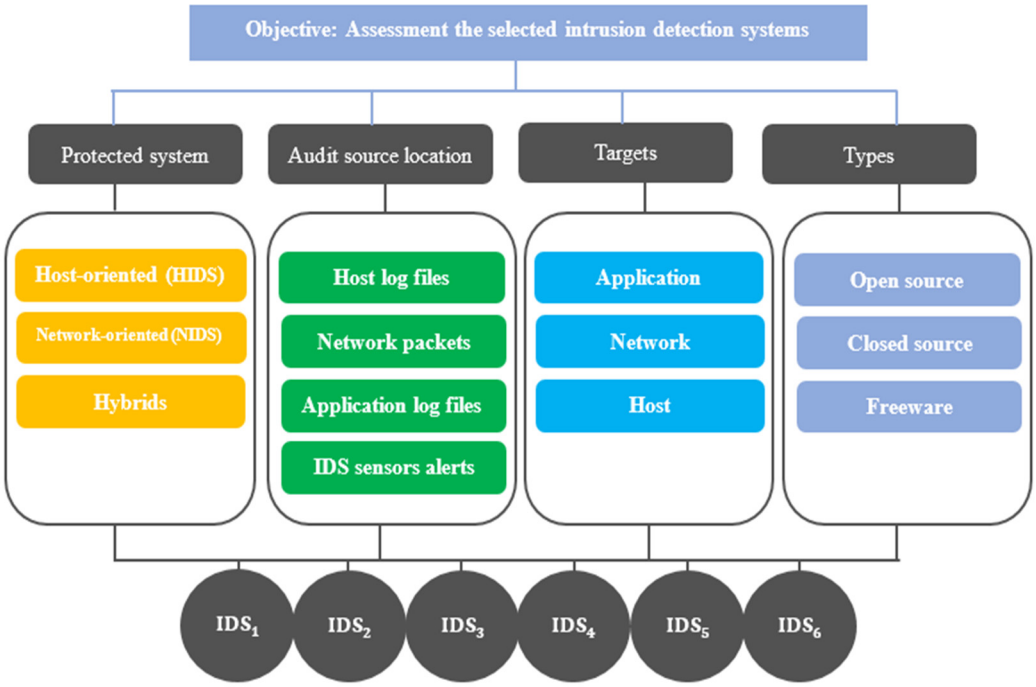

Figure 5. The hierarchy structure of the problem.

Table 5. Verbal evaluations of the main criteria by each expert and the aggregated main criteria weights.

Main Criteria	Ex_1	Ex_2	Ex_3	Ex_4	Aggregated Results	$KE_{q,ij}$ (x)	$EN_{q,ij}$ (x)	ε_j	w_j
PSC_1	GOO	VGO	EXG	VGO	[0.887, 0.253]	0.549576	0.450424	0.166067	0.278
ASC_2	FAR	MDG	MDG	GOO	[0.656, 0.461]	0.133121	0.866879	0.319610	0.226
TGC_3	GOO	VGO	VGO	VGO	[0.856, 0.260]	0.460183	0.539817	0.199025	0.266
TPC_4	MDG	POO	VGO	MDP	[0.538, 0.651]	0.144820	0.855180	0.315296	0.230

Step 7. Individual expert evaluations of the main criteria were compiled using a q-ROFWG operator in Equation (23), and using the weights assigned to the four experts, namely, 0.2, 0.3, 0.3, and 0.2, respectively, as exhibited in Table 5. The parameter was determined in a discretionary manner to reflect the position of the experts in terms of optimism and pessimism. In this case, q = 5 was introduced for a stronger illustration of the uncertainty.

Step 8. The entropy method was applied to calculate the entropy values for each q-ROFN from the aggregated experts' evaluations by applying Equations (28) and (29), as shown in Table 5.

Step 9. The weights of the main criteria were calculated based on the entropy values using Equation (30), as presented in Table 5.

Step 10. Likewise, the weights of the sub-aspects of the main criteria were calculated, as presented in Tables 6–9. Accordingly, the global weights of the sub-aspects were calculated, as in Table 10.

Table 6. Verbal evaluations of the protected system's criteria and aggregated main criteria weights.

Sub-Criteria	Ex_1	Ex_2	Ex_3	Ex_4	Aggregated Results	$KE_{q,ij}$ (x)	$EN_{q,ij}$ (x)	ε_j	w_j
HIC_{1_1}	MDP	FAR	VPO	EXG	[0.449, 0.748]	0.243794	0.756206	0.360331	0.319
NIC_{1_2}	ELP	VGO	MDP	MDG	[0.445, 0.862]	0.484883	0.515117	0.245452	0.377
HYC_{1_3}	VGO	GOO	GOO	POO	[0.667, 0.576]	0.172681	0.827319	0.394216	0.304

Table 7. Verbal evaluations of the audit source location's criteria and aggregated main criteria weights.

Sub-Criteria	Ex_1	Ex_2	Ex_3	Ex_4	Aggregated Results	$KE_{q,ij}$ (x)	$EN_{q,ij}$ (x)	ε_j	w_j
HLC_{2_1}	VPO	EXG	MDP	FAR	[0.510, 0.922]	0.684180	0.315820	0.151557	0.282
NPC_{2_2}	ELP	VGO	MDP	MDG	[0.445, 0.862]	0.484883	0.515117	0.247197	0.251
ALC_{2_3}	VGO	MDG	MDG	POO	[0.609, 0.588]	0.133588	0.866412	0.415779	0.196
ISC_{2_4}	VGO	MDP	ELP	MDG	[0.361, 0.906]	0.613525	0.386475	0.185464	0.271

Table 8. Verbal evaluations of the targets' criteria and aggregated main criteria weights.

Sub-Criteria	Ex_1	Ex_2	Ex_3	Ex_4	Aggregated Results	$KE_{q,ij}$ (x)	$EN_{q,ij}$ (x)	ε_j	w_j
APC_{3_1}	FAR	MDG	MDG	GOO	[0.656, 0.461]	0.133121	0.866879	0.431377	0.284
NEC_{3_2}	VGO	MDP	ELP	MDG	[0.361, 0.906]	0.613525	0.386475	0.192318	0.404
HOC_{3_3}	MDP	FAR	VPO	EXG	[0.449, 0.748]	0.243794	0.756206	0.376304	0.312

Table 9. Verbal evaluations of the types' criteria and aggregated main criteria weights.

Sub-Criteria	Ex_1	Ex_2	Ex_3	Ex_4	Aggregated Results	$KE_{q,ij}$ (x)	$EN_{q,ij}$ (x)	ε_j	w_j
OSC_{4_1}	MDP	FAR	VPO	GOO	[0.427, 0.748]	0.241568	0.758432	0.356283	0.322
CSC_{4_2}	MDG	POO	VGO	MDP	[0.538, 0.651]	0.144820	0.855180	0.401732	0.299
FRC_{4_3}	ELP	VGO	MDP	MDG	[0.445, 0.862]	0.484883	0.515117	0.241983	0.379

Table 10. The global weights of the sub criteria for evaluating intrusion-detection systems.

Main Criteria	**PSC_1 (0.278)**			**ASC_2 (0.226)**			
Sub-criteria	HIC_{1_1}	NIC_{1_2}	HYC_{1_3}	HLC_{2_1}	NPC_{2_2}	ALC_{2_3}	ISC_{2_4}
Local weights	0.319	0.377	0.304	0.282	0.251	0.196	0.271
Global weights	0.089	0.105	0.085	0.064	0.056	0.045	0.061
Main Criteria	**TGC_3 (0.266)**			**TPC_4 (0.230)**			
Sub-criteria	APC_{3_1}	NEC_{3_2}	HOC_{3_3}	OSC_{4_1}	CSC_{4_2}	FRC_{4_3}	
Local weights	0.284	0.404	0.312	0.322	0.299	0.379	
Global weights	0.075	0.107	0.083	0.074	0.069	0.087	

Step 11. An evaluation decision matrix was established to evaluate the IDSs according to the sub-aspects by the four experts and with the assistance of Table 3, as presented in Table 11.

Step 12. Individual expert evaluations of the alternatives between the sub-aspects and the available alternatives were compiled using the q-ROFWG operator in Equation (23), and using the weights assigned to the four experts, namely, 0.2, 0.3, 0.3, and 0.2, respectively, as exhibited in Table 12. The parameter also was determined in a discretionary manner to reflect the position of the experts in terms of optimism and pessimism. In this case, q = 5 and γ =1 were introduced for a stronger illustration of the uncertainty.

Table 11. Evaluations of the IDSs in terms of criteria.

IDS	Ex_s	HIC_{1_1}	NIC_{1_2}	HYC_{1_3}	HLC_{2_1}	NPC_{2_2}	ALC_{2_3}	ISC_{2_4}	APC_{3_1}	NEC_{3_2}	HOC_{3_3}	OSC_{4_1}	CSC_{4_2}	FRC_{4_3}
IDS_1	Ex_1	VEH	VEH	VEH	VEH	MEH	MEH	HGH	HGH	HGH	VLO	VLO	VLO	HGH
	Ex_2	VEH	VEH	VEH	HGH	VEH	HGH	HGH	VEH	VEH	MEL	HGH	HGH	MED
	Ex_3	HGH	HGH	HGH	HGH	HGH	HGH	HGH	VEH	VEH	MED	MEL	MEL	MED
	Ex_4	HGH	HGH	HGH	VEH	EXH	HGH	HGH	EXH	VEH	HGH	VLO	HGH	MED
	Ex_s	HIC_{1_1}	NIC_{1_2}	HYC_{1_3}	HLC_{2_1}	NPC_{2_2}	ALC_{2_3}	ISC_{2_4}	APC_{3_1}	NEC_{3_2}	HOC_{3_3}	OSC_{4_1}	CSC_{4_2}	FRC_{4_3}
IDS_2	Ex_1	HGH	LLO	EXO	VEH	LLO	MEL	HGH	VEH	VEH	VLO	VLO	VLO	VEH
	Ex_2	VEH	LLO	EXO	HGH	HGH	MEH	VEH	VEH	VEH	MEL	HGH	HGH	VLO
	Ex_3	HGH	LLO	EXO	HGH	MEL	MED	HGH	VEH	VEH	MED	MEL	MEL	MED
	Ex_4	HGH	LLO	EXO	EXH	VEH	MED	HGH	EXH	VEH	HGH	VLO	HGH	LLO
	Ex_s	HIC_{1_1}	NIC_{1_2}	HYC_{1_3}	HLC_{2_1}	NPC_{2_2}	ALC_{2_3}	ISC_{2_4}	APC_{3_1}	NEC_{3_2}	HOC_{3_3}	OSC_{4_1}	CSC_{4_2}	FRC_{4_3}
IDS_3	Ex_1	HGH	VEH	VEH	VEH	HGH	MED	HGH	VEH	MEL	VLO	VLO	VLO	EXO
	Ex_2	VEH	VEH	VEH	HGH	EXH	VEH	VEH	VEH	MEL	MEL	HGH	HGH	EXO
	Ex_3	HGH	HGH	HGH	HGH	VEH	MEH	HGH	VEH	MEL	MED	MEL	MEL	EXO
	Ex_4	HGH	HGH	HGH	VEH	EXH	HGH	HGH	VEH	MEL	HGH	VLO	HGH	EXO
	Ex_s	HIC_{1_1}	NIC_{1_2}	HYC_{1_3}	HLC_{2_1}	NPC_{2_2}	ALC_{2_3}	ISC_{2_4}	APC_{3_1}	NEC_{3_2}	HOC_{3_3}	OSC_{4_1}	CSC_{4_2}	FRC_{4_3}
IDS_4	Ex_1	VEH	VEH	VEH	VEH	LLO	MEL	HGH	HGH	MED	VLO	VLO	VLO	MEL
	Ex_2	VEH	VEH	VEH	HGH	HGH	MEH	VEH	HGH	MED	MEL	HGH	HGH	MEL
	Ex_3	HGH	HGH	HGH	HGH	MEL	MED	HGH	HGH	MED	MED	MEL	MEL	MEL
	Ex_4	HGH	HGH	HGH	EXH	VEH	MED	HGH	HGH	MED	HGH	VLO	HGH	MEL
	Ex_s	HIC_{1_1}	NIC_{1_2}	HYC_{1_3}	HLC_{2_1}	NPC_{2_2}	ALC_{2_3}	ISC_{2_4}	APC_{3_1}	NEC_{3_2}	HOC_{3_3}	OSC_{4_1}	CSC_{4_2}	FRC_{4_3}
IDS_5	Ex_1	HGH	VEH	VLO	VEH	HGH	MED	HGH	VLO	VEH	VLO	VLO	VLO	HGH
	Ex_2	VEH	VEH	HGH	HGH	EXH	VEH	VEH	VLO	VEH	MEL	HGH	HGH	MED
	Ex_3	HGH	HGH	MEL	HGH	VEH	MEH	HGH	VLO	VEH	MED	MEL	MEL	MED
	Ex_4	HGH	HGH	VLO	VEH	EXH	HGH	HGH	VLO	VEH	HGH	VLO	HGH	MED
	Ex_s	HIC_{1_1}	NIC_{1_2}	HYC_{1_3}	HLC_{2_1}	NPC_{2_2}	ALC_{2_3}	ISC_{2_4}	APC_{3_1}	NEC_{3_2}	HOC_{3_3}	OSC_{4_1}	CSC_{4_2}	FRC_{4_3}
IDS_6	Ex_1	HGH	VEH	VEH	VEH	HGH	MED	HGH	VEH	MEH	VLO	VLO	VLO	VLO
	Ex_2	VEH	VEH	VEH	HGH	EXH	VEH	VEH	VEH	MEH	MEL	HGH	HGH	VLO
	Ex_3	HGH	HGH	HGH	HGH	VEH	MEH	HGH	VEH	MEH	MED	MEL	MEL	VLO
	Ex_4	HGH	HGH	HGH	VEH	EXH	HGH	HGH	VEH	MEH	HGH	VLO	HGH	VLO

Table 12. The aggregated evaluations matrix of the IDSs.

IDS	HIC_{1_1}	NIC_{1_2}	HYC_{1_3}	HLC_{2_1}	NPC_{2_2}	ALC_{2_3}	ISC_{2_4}
IDS_1	[0.823, 0.295]	[0.823, 0.295]	[0.823, 0.295]	[0.823, 0.295]	[0.817, 0.342]	[0.747, 0.365]	[0.770, 0.330]
IDS_2	[0.801, 0.318]	[0.330, 0.770]	[0.110, 0.990]	[0.832, 0.301]	[0.564, 0.630]	[0.555, 0.562]	[0.801, 0.311]
IDS_3	[0.801, 0.318]	[0.823, 0.295]	[0.823, 0.295]	[0.832, 0.301]	[0.909, 0.248]	[0.715, 0.438]	[0.801, 0.311]
IDS_4	[0.823, 0.295]	[0.823, 0.295]	[0.823, 0.295]	[0.832, 0.301]	[0.817, 0.342]	[0.555, 0.562]	[0.801, 0.311]
IDS_5	[0.801, 0.318]	[0.823, 0.295]	[0.394, 0.780]	[0.812, 0.303]	[0.909, 0.284]	[0.715, 0.438]	[0.801, 0.318]
IDS_6	[0.801, 0.318]	[0.823, 0.295]	[0.823, 0.295]	[0.812, 0.303]	[0.909, 0.284]	[0.715, 0.438]	[0.801, 0.318]

IDS	APC_{3_1}	NEC_{3_2}	HOC_{3_3}	OSC_{4_1}	CSC_{4_2}	FRC_{4_3}
IDS_1	[0.877, 0.259]	[0.857, 0.260]	[0.458, 0.713]	[0.394, 0.780]	[0.507, 0.704]	[0.588, 0.528]
IDS_2	[0.901, 0.211]	[0.880, 0.220]	[0.458, 0.715]	[0.441, 0.661]	[0.507, 0.706]	[0.414, 0.765]
IDS_3	[0.880, 0.220]	[0.440, 0.660]	[0.458, 0.714]	[0.394, 0.780]	[0.507, 0.705]	[0.110, 0.990]
IDS_4	[0.770, 0.330]	[0.550, 0.550]	[0.458, 0.714]	[0.394, 0.780]	[0.507, 0.705]	[0.440, 0.432]
IDS_5	[0.220, 0.880]	[0.880, 0.220]	[0.458, 0.714]	[0.394, 0.780]	[0.507, 0.705]	[0.588, 0.528]
IDS_6	[0.880, 0.220]	[0.660, 0.440]	[0.458, 0.714]	[0.394, 0.780]	[0.507, 0.705]	[0.220, 0.880]

Step 13. The normalized aggregated q-ROF evaluation decision matrix was calculated by applying Equation (31), as presented in Table 13.

Table 13. The normalized evaluation matrix of the IDSs.

IDS	HIC_{1_1}	NIC_{1_2}	HYC_{1_3}	HLC_{2_1}	NPC_{2_2}	ALC_{2_3}	ISC_{2_4}
IDS_1	[0.823, 0.295]	[0.823, 0.295]	[0.823, 0.295]	[0.823, 0.295]	[0.817, 0.342]	[0.747, 0.365]	[0.770, 0.330]
IDS_2	[0.801, 0.318]	[0.330, 0.770]	[0.110, 0.990]	[0.832, 0.301]	[0.564, 0.630]	[0.555, 0.562]	[0.801, 0.311]
IDS_3	[0.801, 0.318]	[0.823, 0.295]	[0.823, 0.295]	[0.832, 0.301]	[0.909, 0.248]	[0.715, 0.438]	[0.801, 0.311]
IDS_4	[0.823, 0.295]	[0.823, 0.295]	[0.823, 0.295]	[0.832, 0.301]	[0.817, 0.342]	[0.555, 0.562]	[0.801, 0.311]
IDS_5	[0.801, 0.318]	[0.823, 0.295]	[0.394, 0.780]	[0.812, 0.303]	[0.909, 0.284]	[0.715, 0.438]	[0.801, 0.318]
IDS_6	[0.801, 0.318]	[0.823, 0.295]	[0.823, 0.295]	[0.812, 0.303]	[0.909, 0.284]	[0.715, 0.438]	[0.801, 0.318]
IDS	APC_{3_1}	NEC_{3_2}	HOC_{3_3}	OSC_{4_1}	CSC_{4_2}	FRC_{4_3}	
IDS_1	[0.877, 0.259]	[0.857, 0.260]	[0.458, 0.713]	[0.394, 0.780]	[0.507, 0.704]	[0.588, 0.528]	
IDS_2	[0.901, 0.211]	[0.880, 0.220]	[0.458, 0.715]	[0.441, 0.661]	[0.507, 0.706]	[0.414, 0.765]	
IDS_3	[0.880, 0.220]	[0.440, 0.660]	[0.458, 0.714]	[0.394, 0.780]	[0.507, 0.705]	[0.110, 0.990]	
IDS_4	[0.770, 0.330]	[0.550, 0.550]	[0.458, 0.714]	[0.394, 0.780]	[0.507, 0.705]	[0.440, 0.432]	
IDS_5	[0.220, 0.880]	[0.880, 0.220]	[0.458, 0.714]	[0.394, 0.780]	[0.507, 0.705]	[0.588, 0.528]	
IDS_6	[0.880, 0.220]	[0.660, 0.440]	[0.458, 0.714]	[0.394, 0.780]	[0.507, 0.705]	[0.220, 0.880]	

Step 14. Calculate the total of the weighted comparability arrangement for all alternatives by applying the Wq-ROFHA operator, as presented in Equations (24) and (25), and as exhibited in Table 14.

Table 14. The $\acute{\alpha}_j$ and $ß_j$ values of the IDSs.

IDSs	Wq-ROFHA Operator		Wq-ROFHGM Operator	
	$\acute{\alpha}$	ß	$\acute{\alpha}$	ß
IDS_1	0.784	0.382	0.139	0.567
IDS_2	0.741	0.489	0.102	0.789
IDS_3	0.767	0.438	0.113	0.777
IDS_4	0.741	0.421	0.127	0.578
IDS_5	0.760	0.483	0.119	0.671
IDS_6	0.771	0.419	0.125	0.651

Step 15. Calculate the full power weight of the comparability arrangements for all alternatives by applying the Wq-ROFHGM operator, as exhibited in Equations (26) and (27), and as exhibited in Table 14.

Step 16. The score values of the all alternatives are computed by applying the values of the Wq-ROFHA and Wq-ROFHGM operators for each alternative by applying Equation (20), as presented in Table 15.

Table 15. The score values of the IDSs for $\acute{\alpha}_j$ and $ß_j$.

IDS	$\acute{\alpha}_j$	$ß_j$
IDS_1	0.701	0.286
IDS_2	0.626	0.156
IDS_3	0.665	0.168
IDS_4	0.660	0.275
IDS_5	0.639	0.224
IDS_6	0.676	0.237

Step 17. The proportional weight of the alternatives is calculated with the assistance of Equations (32)–(34), as shown in Table 16.

Table 16. The proportional importance and the final ranking of the IDSs.

IDS	γ_{ja}	γ_{jb}	γ_{jc}	γ_j	Rank
IDS_1	0.186	2.952	1.000	2.398	1
IDS_2	0.147	2.000	0.792	1.595	6
IDS_3	0.157	2.136	0.843	1.701	5
IDS_4	0.176	2.814	0.947	2.089	2
IDS_5	0.162	2.455	0.874	1.867	4
IDS_6	0.172	2.597	0.925	1.976	3

Step 18. The evaluation values (γ_j) of the alternatives are identified by applying Equation (35). Then, the six intrusion-detection systems are rated according to the most possible value of the evaluation values (γ_j), as presented in Table 16 and in Figure 6.

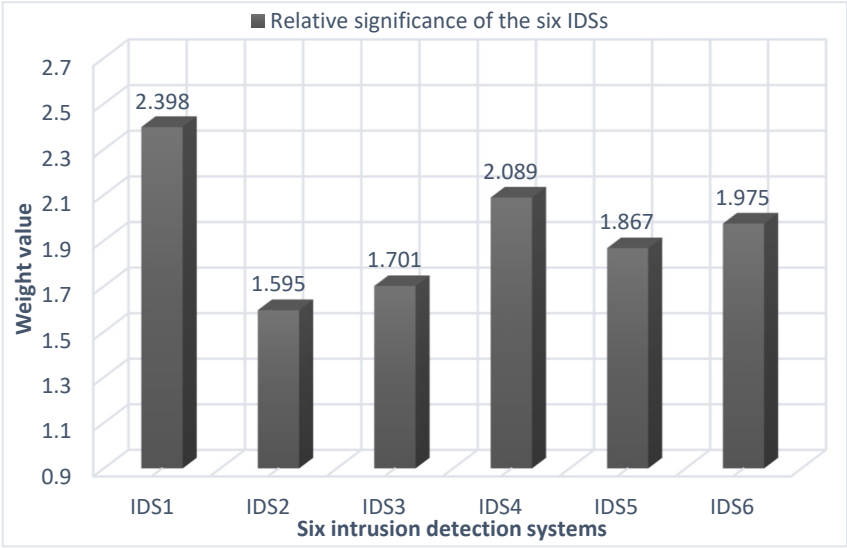

Figure 6. Ranking of the IDSs using the CoCoSo method.

4.3. Results Interpretation

In this subsection, some interpretations are introduced of the results obtained from applying the proposed approach, Entropy-CoCoSo, under a q-rung orthopair fuzzy environment. The results obtained are divided into two parts. The first part relates to the results of the main criteria weights and their sub-aspects. The second part relates to the results of the intrusion-detection systems evaluation used in the study. Initially, the four main criteria were evaluated by the participating experts. The results obtained indicate that the PSC_1 criterion has the highest weight, with a weight of 0.278, followed by the TGC_3 criterion with a weight of 0.266. Whereas, the ASC_2 criterion has the lowest weight, 0.226, and occupies the last rank in the ranking of the main criteria. Accordingly, the sub-criteria related to each main criterion were evaluated. Thus, the sub-criteria related to the PSC_1 criterion were evaluated as follows: the NIC_{1_2} criterion has the top weight with a weight of 0.377, followed by the HIC_{1_1} criterion with a weight of 0.319; the HYC_{1_3} criterion has the lowest weight, 0.304. The sub-criteria related to the ASC_2 criterion were calculated as follows: the HLC_{2_1} criterion has the maximum weight, with a weight of 0.282, followed by the ISC_{2_4} criterion, with a weight of 0.271; the ALC_{2_3} criterion has the minimum weight, 0.196. In addition, the sub-criteria related to the TGC_3 criterion were estimated as follows: the NEC_{3_2} criterion has the highest weight, with a weight of 0.404, followed by the HOC_{3_3} criterion with a weight of 0.312; the APC_{3_1} criterion has the lowest weight, 0.284. Afterward, the sub-criteria related to the TPC_4 criterion were assessed as follows:

the FRC_{4_3} criterion has the largest weight, with a weight of 0.379, followed by the OSC_{4_1} criterion with a weight of 0.322; the CSC_{4_2} criterion has the smallest weight, 0.299.

In the end, the results of the intrusion-detection systems used in the evaluation process were revealed as follows: Suricata (IDS_1) has the top rank with a weight of 2.398 followed by Snort (IDS_4) with a weight of 2.089. In turn, Zeek (IDS_2) has the lowest rank with a weight of 1.595.

4.4. Comparative Analysis

In this sub-section, a comparative analysis is demonstrated to test and verify the effectiveness of the developed approach, q-ROF Entropy-CoCoSo. Consequently, the assessment results were compared with Alyami et al.'s [16] fuzzy AHP–TOPSIS approach. In this regard, the same weights of the main criteria and sub-aspects obtained by applying the proposed approach were used, as shown in Table 10. Accordingly, the results of ranking the alternatives used in the study using the two approaches are presented in Table 17 and in Figure 7. The results of the comparison show that IDS_1 is the best alternative according to the results of the two approaches. IDS_2 is the least alternative in the order. According to the results, it can be seen that there are some changes in the order of some alternatives, such as IDS_3, IDS_4, IDS_5, and IDS_6. The presence of some differences in the order of the alternatives can be explained by the difference in the mathematical basis for each approach. Finally, the results of the comparative analysis and the reliability of the proposed approach can be verified by the experts.

Table 17. Comparative analysis with other approach for ranking the IDSs.

Approaches	IDS_1	IDS_2	IDS_3	IDS_4	IDS_5	IDS_6
q-ROF Entropy-CoCoSo	2.398	1.595	1.701	2.089	1.867	1.976
Ranking	1	6	5	2	4	3
Fuzzy AHP-TOPSIS	0.927	0.287	0.582	0.675	0.497	0.723
Ranking	1	6	4	3	5	2

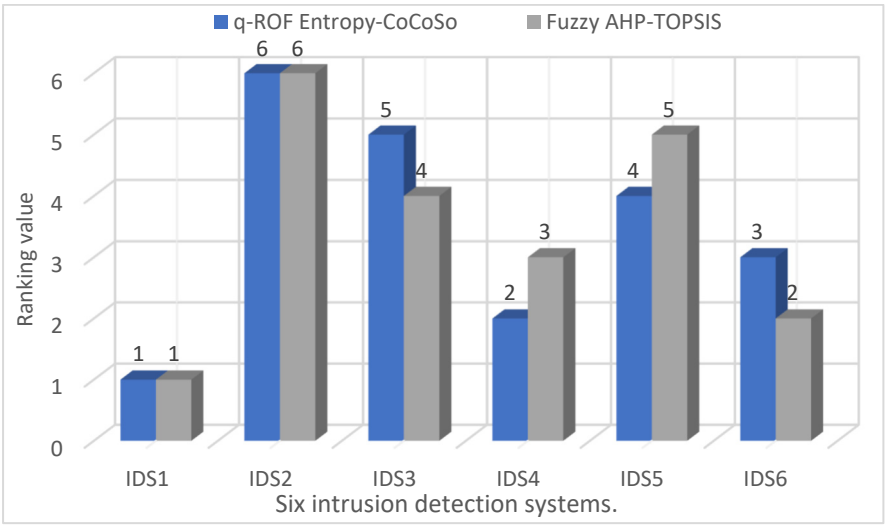

Figure 7. Final ranking of the six IDSs using various approaches.

4.5. Sensitivity Analysis

We have conducted a sensitivity analysis from the three perspectives of changes in parameter q, parameter γ, and parameter Ψ. Sensitivity analysis was conducted on the results obtained to confirm their reliability and stability and to examine the change that occurred

to them as a result of the change in some inputs and parameters. In decision-making approaches, some parameters are defined subjectively based on the perception of the problem by decision-makers and the extent of the risks in the environment. Consequently, these parameters change according to the circumstances in which the decision-making system is being modeled. In our proposed Entropy-CoCoSo q-ROF approach, three parameters—q, γ, and Ψ—are defined, which are determined based on the personal preferences of the experts. Accordingly, several changes were made to these parameters to show their decisive influence on the final IDS's ranking results. These changes were divided into four scenarios. The first scenario refers to the change in the values of parameter q. The second scenario indicates the change in the values of parameter γ. The third scenario refers to the change in the values of parameters q and γ. Lastly, the fourth scenario refers to the change in the values of parameter Ψ.

The first scenario is the effect of a change in parameter q on the evaluation of IDSs. Accordingly, the value of the parameter q was changed several times, from q = 2 to q = 20, to show its impact on the evaluation of IDSs, as presented in Figure 8. Although the value of the q parameter has been changed several times, the order of the IDSs has not changed at all. IDS_1 remains the best alternative throughout the sensitivity analysis and parameter value change q, followed by IDS_4. By contrast, IDS_2 remains the lowest in order despite the change in the value of the parameter q. The changes that can be observed based on the change in the value of the parameter q in the order of the IDSs, show there is a large convergence between the values of the assessment of IDS_4 and IDS_6 at the value of q = 2. Significant convergence occurs between the IDS_4 and IDS_1 assessment values at q = 8; otherwise, the order of the IDSs remains the same despite the presence of some increases in the weights of the IDSs.

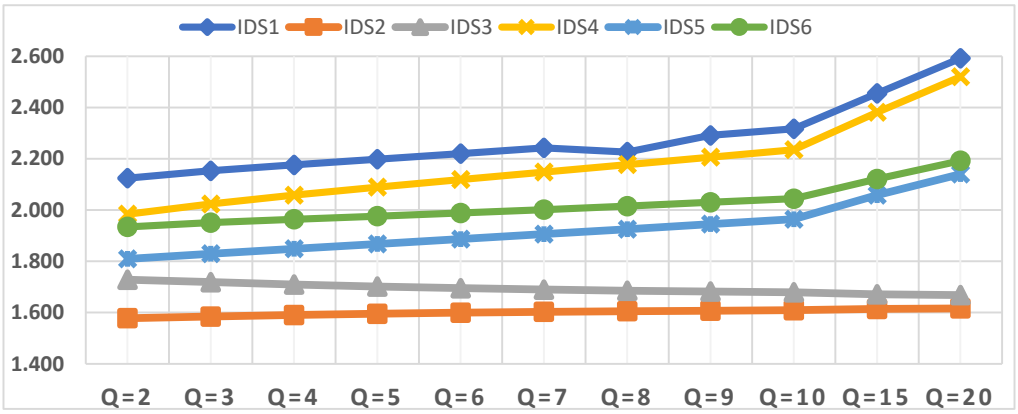

Figure 8. Closeness coefficient values of IDSs in terms of different values of q.

The second scenario is the effect of a change in parameter γ on the evaluation of IDSs. Accordingly, the value of the parameter γ was changed several times, from γ = 0.1 to γ = 1.0, to show its effect on the evaluation of IDSs, as shown in Figure 9. Although the value of the parameter γ was changed several times, the order of the IDSs changed only when the value of parameter γ = 1.0. IDS_1 remains the best alternative throughout the sensitivity analysis and parameter value change γ = 0.1 to γ = 0.9 followed by IDS_4, except when parameter value γ = 1.0, then IDS_6 becomes the second rank in the analysis process. In contrast, IDS_2 remains lowest in order throughout the change of the value of the parameter γ = 0.0 to γ = 0.9, except when the value of γ = 1.0 is changed, then IDS_2 becomes the fifth rank, penultimate. The changes that can be observed based on the change in the value of the parameter q in the order of IDSs, is that when the value of the parameter γ = 1.0, the order of the IDSs changes so that IDS_1 is in the first order, while IDS_6 is in the second order, and IDS_4 is in the third order. On the contrary, the rank of some IDSs was changed, such as the rank of IDS_2 and the IDS_5, which became the fifth and sixth, respectively.

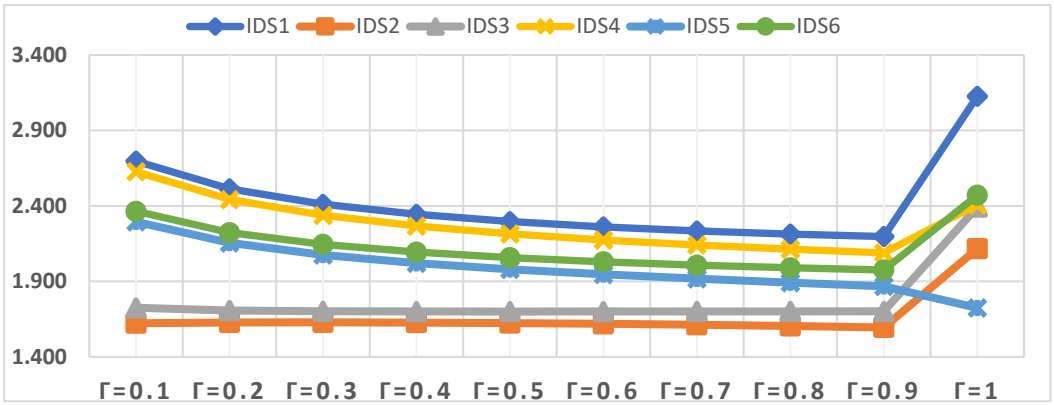

Figure 9. Closeness coefficient values of IDSs in terms of different values of γ.

The third scenario is the effect of a change in parameter q and γ on the evaluation of IDSs. Accordingly, the values of q and γ were changed several times, from q = 2 to q = 15, and γ = 0.1 to γ = 1 to show their combined effect on the assessment of the IDSs, as shown in Figure 10. Although the values of the parameters q and γ changed many times, the order of the IDSs has not changed at all. IDS_1 remains the best alternative during sensitivity analysis and changing the values of q and γ parameters, followed by IDS_4. In contrast, IDS_2 remains the lowest in terms of rank despite the change in the values of the two parameters q and γ. Changes that can be observed based on the change in the value of parameters q and γ for the order of IDSs, is that there is a great convergence between the values of the evaluation process weights for the IDSs used in the study. The convergence between the weights of the IDSs is difficult to see in Figure 10, and this is one of the shortcomings of Figure 10.

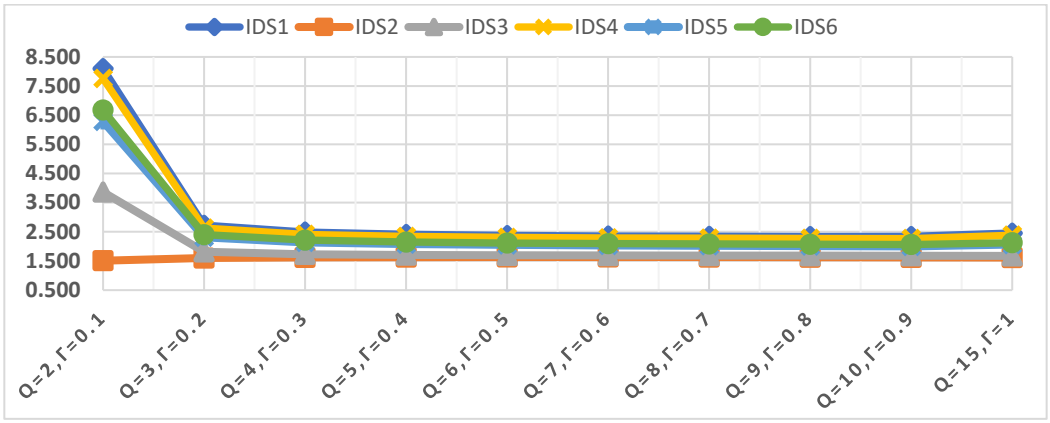

Figure 10. Closeness coefficient values of IDSs in terms of the different values of q and γ.

The fourth scenario is the effect of a change in parameter Ψ on the evaluation of IDSs. Accordingly, the value of parameter Ψ was changed several times from Ψ = 0.1 to Ψ = 1.0, to show its effect on the evaluation of the IDSs, as shown in Figure 11. Although the value of parameter Ψ was changed several times, the order of the IDSs did not change at all. IDS_1 remains the best alternative throughout the sensitivity analysis and parameter value change Ψ = 0.1 to Ψ = 0.9, followed by IDS_4. On the contrary, IDS_2 remains in the lowest order by changing the parameter value Ψ = 0.1 to Ψ = 1.0.

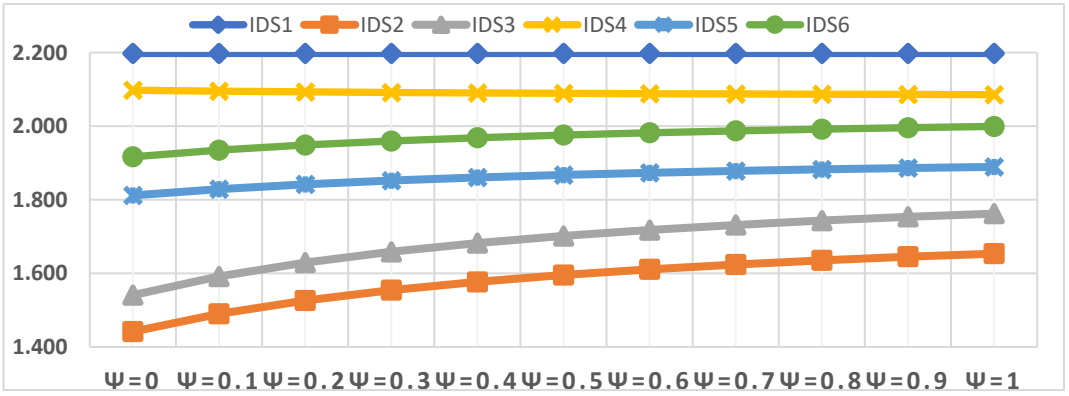

Figure 11. Closeness coefficient values of the IDSs in terms of the different values of Ψ.

5. Conclusions

Given the spread of computer networks and the dependence of public and private institutions on their efficiency and quality of work, any disruption or sabotage of them may lead to great losses. Information systems and networks are constantly subject to cyber-attacks. Thus, firewalls and antivirus are not enough to fend off all these attacks, as they are only able to protect the "front entrance" of computer systems and networks. IDSs can help protect your corporation from malicious activities. There are different types of IDSs to protect networks, as intrusion attacks are becoming more and more common on a global scale. In addition, hackers using new technologies are trying to penetrate systems. An IDS is a tool that identifies these attacks and will take an immediate step to get the system back to normal, as the IDS can also detect network traffic and send an alarm if a breach is found.

In this regard, this study discusses the most effective and used IDSs. This study was conducted with the participation of many experts under the q-ROF environment to deal with the uncertainty that may occur as a result of different circumstances and differences in evaluation frameworks. Six intrusion-detection systems, namely, Suricata (IDS_1), Zeek (IDS_2), Security onion (IDS_3), Snort (IDS_4), Wazuh (IDS_5), and OSSEC (IDS_6), were evaluated according to four key criteria and thirteen sub-aspects. The main criteria were protected system, audit source location, targets, and types. The sub-aspects, on the basis of which the effectiveness of the intrusion-detection systems was evaluated, were HIDS, NIDS, hybrids, host log files, network packets, application log files, IDS sensors alerts, applications, network, host, open-source, closed source, and freeware. A hybrid MCDM approach, including q-ROF entropy-CoCoSo techniques, was proposed, where entropy was applied to evaluate the main criteria and their sub-aspects. The CoCoSo method is applied to rate six IDSs according to their effectiveness. Afterward, comparative and sensitivity analyses were performed to confirm the stability, reliability, and performance of the proposed approach. The findings indicate that most of the IDSs appear to be systems with high potential. According to the results, Suricata is the best IDS that relies on multi-threading performance. Although the results here confirm that the proposed method is applicable and effective, it has some limitations. The key limitation of the approach is the difficult mathematical algorithm for the computation of Hamacher functions.

Author Contributions: Conceptualization, M.A.-B., A.G., K.M.S., I.E., K.M. and A.J.; methodology, M.A.-B., A.G., K.M.S., I.E., K.M. and A.J.; software, M.A.-B., A.G.; validation, M.A.-B., A.G., K.M.S., I.E., K.M. and A.J.; formal analysis, M.A.-B., A.G.; investigation, M.A.-B., A.G., K.M.S., I.E., K.M. and A.J.; resources, M.A.-B., A.G.; writing—original draft preparation, M.A.-B., A.G., K.M.S.; writing—review and editing, M.A.-B., A.G., K.M.S., I.E., K.M. and A.J.; visualization, M.A.-B., A.G., K.M.S., I.E., K.M.; supervision, M.A.-B., K.M. and A.J.; project administration, M.A.-B. funding acquisition K.M. and A.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study did not involve humans or animals.

Informed Consent Statement: The study did not involve humans.

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

References

1. Ahmad, T.; Zhang, D. Using the internet of things in smart energy systems and networks. *Sustain. Cities Soc.* **2021**, *68*, 102783. [CrossRef]
2. Jaafar, G.A.; Abdullah, S.M.; Ismail, S. Review of Recent Detection Methods for HTTP DDoS Attack. *J. Comput. Netw. Commun.* **2019**, *2019*, 1283472. [CrossRef]
3. Harter, G.T.; Rowe, N.C. *Testing Detection of K-Ary Code Obfuscated by Metamorphic and Polymorphic Techniques BT—National Cyber Summit (NCS) Research Track 2021*; Choo, K.-K.R., Morris, T., Peterson, G., Imsand, E., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 110–123.
4. Malhotra, P.; Singh, Y.; Anand, P.; Bangotra, D.K.; Singh, P.K.; Hong, W.-C. Internet of Things: Evolution, Concerns and Security Challenges. *Sensors* **2021**, *21*, 1809. [CrossRef] [PubMed]
5. Mullet, V.; Sondi, P.; Ramat, E. A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. *IEEE Access* **2021**, *9*, 23235–23263. [CrossRef]
6. Wu, Z.; Shen, S.; Zhou, H.; Li, H.; Lu, C.; Zou, D. An effective approach for the protection of user commodity viewing privacy in e-commerce website. *Knowl.-Based Syst.* **2021**, *220*, 106952. [CrossRef]
7. Quincozes, S.E.; Albuquerque, C.; Passos, D.; Mossé, D. A survey on intrusion detection and prevention systems in digital substations. *Comput. Netw.* **2021**, *184*, 107679. [CrossRef]
8. Alharbi, A.; Seh, A.H.; Alosaimi, W.; Alyami, H.; Agrawal, A.; Kumar, R.; Khan, R.A. Analyzing the Impact of Cyber Security Related Attributes for Intrusion Detection Systems. *Sustainability* **2021**, *13*, 12337. [CrossRef]
9. Carta, S.; Podda, A.S.; Recupero, D.R.; Saia, R. A Local Feature Engineering Strategy to Improve Network Anomaly Detection. *Futur. Internet* **2020**, *12*, 177. [CrossRef]
10. Lu, Y.; Teng, S. Application of Sequence Embedding in Host-based Intrusion Detection System. In Proceedings of the 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Dalian, China, 5–7 May 2021; pp. 434–439.
11. Oliveira, N.; Praça, I.; Maia, E.; Sousa, O. Intelligent Cyber Attack Detection and Classification for Network-Based Intrusion Detection Systems. *Appl. Sci.* **2021**, *11*, 1674. [CrossRef]
12. Bhati, N.S.; Khari, M. *A Survey on Hybrid Intrusion Detection Techniques BT—Research in Intelligent and Computing in Engineering*; Kumar, R., Quang, N.H., Kumar Solanki, V., Cardona, M., Pattnaik, P.K., Eds.; Springer: Singapore, 2021; pp. 815–825.
13. Zachos, G.; Essop, I.; Mantas, G.; Porfyrakis, K.; Ribeiro, J.C.; Rodriguez, J. An Anomaly-Based Intrusion Detection System for Internet of Medical Things Networks. *Electronics* **2021**, *10*, 2562. [CrossRef]
14. Díaz-Verdejo, J.; Muñoz-Calle, J.; Estepa Alonso, A.; Estepa Alonso, R.; Madinabeitia, G. On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks. *Appl. Sci.* **2022**, *12*, 852. [CrossRef]
15. Sikora, M.; Fujdiak, R.; Kuchar, K.; Holasova, E.; Misurec, J. Generator of Slow Denial-of-Service Cyber Attacks. *Sensors* **2021**, *21*, 5473. [CrossRef] [PubMed]
16. Alyami, H.; Ansari, M.T.; 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. [CrossRef]
17. Abdel-Basset, M.; Gamal, A.; ELkomy, O.M. Hybrid Multi-Criteria Decision Making approach for the evaluation of sustainable photovoltaic farms locations. *J. Clean. Prod.* **2021**, *328*, 129526. [CrossRef]
18. Yager, R.R. Generalized Orthopair Fuzzy Sets. *IEEE Trans. Fuzzy Syst.* **2017**, *25*, 1222–1230. [CrossRef]
19. Atanassov, K. Intuitionistic Fuzzy Sets. *Fuzzy Sets Syst.* **1999**, *20*, 110–116.
20. Yager, R.R. Pythagorean fuzzy subsets. In Proceedings of the 2013 Joint IFSA World Congress and NAFIPS Annual Meeting (IFSA/NAFIPS), Edmonton, AB, Canada, 24–28 June 2013; pp. 57–61.
21. Mishra, A.R.; Rani, P. A q-rung orthopair fuzzy ARAS method based on entropy and discrimination measures: An application of sustainable recycling partner selection. *J. Ambient Intell. Humaniz. Comput.* **2021**, 1–22. [CrossRef]
22. Shang, C.; Saeidi, P.; Goh, C.F. Evaluation of circular supply chains barriers in the era of Industry 4.0 transition using an extended decision-making approach. *J. Enterp. Inf. Manag.* 2022, *in press*. [CrossRef]
23. Meng, W.; Tischhauser, E.W.; Wang, Q.; Wang, Y.; Han, J. When Intrusion Detection Meets Blockchain Technology: A Review. *IEEE Access* **2018**, *6*, 10179–10188. [CrossRef]
24. Abushark, Y.B.; Irshad Khan, A.; Alsolami, F.; Almalawi, A.; Mottahir Alam, M.; Agrawal, A.; Kumar, R.; Ahmad Khan, R. Cyber Security Analysis and Evaluation for Intrusion Detection Systems. *Comput. Mater. Contin.* **2022**, *72*, 1765–1783. [CrossRef]
25. Almotiri, S.H. Integrated Fuzzy Based Computational Mechanism for the Selection of Effective Malicious Traffic Detection Approach. *IEEE Access* **2021**, *9*, 10751–10764. [CrossRef]
26. Sharma, S.; Kaul, A. Hybrid fuzzy multi-criteria decision making based multi cluster head dolphin swarm optimized IDS for VANET. *Veh. Commun.* **2018**, *12*, 23–38. [CrossRef]

27. Ogundoyin, S.O.; Kamil, I.A. A Fuzzy-AHP based prioritization of trust criteria in fog computing services. *Appl. Soft Comput.* **2020**, *97*, 106789. [CrossRef]
28. Kumar, R.; Alenezi, M.; Ansari, M.; Gupta, B.; Agrawal, A.; Khan, R. Evaluating the Impact of Malware Analysis Techniques for Securing Web Applications through a Decision-Making Framework under Fuzzy Environment. *Int. J. Intell. Eng. Syst.* **2020**, *13*, 94–109. [CrossRef]
29. Duan, W.-Q.; Gulistan, M.; Abbasi, F.H.; Khurshid, A.; Al-Shamiri, M.M. q-Rung double hierarchy linguistic term set fuzzy AHP; applications in the security system threats features of social media platforms. *Int. J. Intell. Syst.* **2021**, 1–34. [CrossRef]
30. Panityakul, T.; Mahmood, T.; Ali, Z.; Aslam, M. Analyzing and controlling computer security threats based on complex q-rung orthopair fuzzy heronian mean operators. *J. Intell. Fuzzy Syst.* **2021**, *41*, 6949–6981. [CrossRef]
31. Cheng, S.; Jianfu, S.; Alrasheedi, M.; Saeidi, P.; Mishra, A.R.; Rani, P. A New Extended VIKOR Approach Using q-Rung Orthopair Fuzzy Sets for Sustainable Enterprise Risk Management Assessment in Manufacturing Small and Medium-Sized Enterprises. *Int. J. Fuzzy Syst.* **2021**, *23*, 1347–1369. [CrossRef]
32. Peng, X.; Dai, J.; Garg, H. Exponential operation and aggregation operator for q-rung orthopair fuzzy set and their decision-making method with a new score function. *Int. J. Intell. Syst.* **2018**, *33*, 2255–2282. [CrossRef]
33. Wei, G.; Gao, H.; Wei, Y. Some q-rung orthopair fuzzy Heronian mean operators in multiple attribute decision making. *Int. J. Intell. Syst.* **2018**, *33*, 1426–1458. [CrossRef]
34. Liu, P.; Wang, P. Some q-Rung Orthopair Fuzzy Aggregation Operators and their Applications to Multiple-Attribute Decision Making. *Int. J. Intell. Syst.* **2018**, *33*, 259–280. [CrossRef]
35. Darko, A.P.; Liang, D. Some q-rung orthopair fuzzy Hamacher aggregation operators and their application to multiple attribute group decision making with modified EDAS method. *Eng. Appl. Artif. Intell.* **2020**, *87*, 103259. [CrossRef]
36. Liu, Z.; Liu, P.; Liang, X. Multiple attribute decision-making method for dealing with heterogeneous relationship among attributes and unknown attribute weight information under q-rung orthopair fuzzy environment. *Int. J. Intell. Syst.* **2018**, *33*, 1900–1928. [CrossRef]
37. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detection and Prevention Systems. *IEEE Access* **2019**, *7*, 46595–46620. [CrossRef]
38. Martinez, C.V.; Sollfrank, M.; Vogel-Heuser, B. A Multi-Agent Approach for Hybrid Intrusion Detection in Industrial Networks: Design and Implementation. In Proceedings of the 2019 IEEE 17th International Conference on Industrial Informatics (INDIN), Helsinki-Espoo, Finland, 22–25 July 2019; Volume 1, pp. 351–357.
39. Badotra, S.; Panda, S.N. SNORT based early DDoS detection system using Opendaylight and open networking operating system in software defined networking. *Clust. Comput.* **2021**, *24*, 501–513. [CrossRef]