

Integrated Fuzzy Based Computational Mechanism for the Selection of Effective Malicious Traffic Detection Approach

SULTAN H. ALMOTIRI 

Computer Science Department, College of Computer and Information Science, Umm AlQura University, Makkah 21955, Saudi Arabia

e-mail: shmotiri@uqu.edu.sa


This work was supported by the King Abdul Aziz City for Science and Technology (KACST), under Grant 14-INF727-10.

ABSTRACT A mechanism to effectively detect malicious traffic in the present context where new cyber criminals and threatening actors are emerging every day, has become a compelling need. These invaders use overwhelming tactics that mask the nature of attacks and make bad acts seem innocuous. A growing number of trustworthy electronic systems and facilities have been introduced with the fast development of pervasive digital technologies. However threats to cyber-security continue to grow, posing hindrance in the efficient use of digital services. The detection and classification of malicious traffic due to security threats can be done by an efficacious traffic detection approach. The development of a smart, precise malicious traffic detection system has therefore become a subject of extensive research. Current traffic detection systems are typically employed in conventional network traffic detection. These systems sometimes face failure and cannot recognize many known or modern security threats. This is because they rely on conventional algorithms which focus less on precise selection and classification of functions. As a result, several well-known traffic signatures remain unidentified and latent. Hence, there is a need to evaluate each significant malicious traffic detection system based on the performance of the system. In this research work, the author has used the Fuzzy AHP methodology which is designed to address the issues related to the vagueness, uncertainties and total awareness of languages. In addition, the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) was implemented in order to assess the order of preference. Furthermore, the Multi-Criteria Decision-Making (MCDM) method was used for classifying the impact of the alternatives according to their overall performance. The study's conclusive evaluations will be a corroborative reference for the practitioners working in the domain of assessing and selecting the most effective traffic detection approach for more reliable, efficient and systematic design.

INDEX TERMS Anomaly IDS, malicious traffic detection, DDoS, network Security, fuzzy logic.

I. INTRODUCTION

Nowadays, the world is witnessing a proliferation of the web with various inventions and technical advances. Innovations in industry have compelled the companies and authorities worldwide to develop and use advanced networks. These networks are an integration of a number of security factors including encryption, data completeness, authentication, and innovations such as distributed database systems, Internet voice, wireless connectivity, and web services [1]. Computers are not only being used for research or commercial purposes, but have become a lifestyle product in the present

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran Tariq .

day world. People of different ages, lifestyles, training and psychology prefer to live in a virtual reality now. Such virtual reality influences the everyday work of the user. In the past, computers were mainly used for accessing the information. Today, computers are not only accessed for expertise, but are also a means to gain money, give or spread opinions, and contribute to social interactions. In their digital social life, electronics devices are interfaces for users. With its resources, capacities and services, but also challenges, the internet is the dwelling place of this digital social interaction. There has been a massive breakthrough in the networking field.

Malicious practices in the online platform are also regarded as intrusion. An intrusion is classified as any operation that compromises security policies of the network infrastructure

[7], [21]. Intrusion detection system (IDS) is a computational machine or Communications Channel software and hardware used to detect or target malicious users – which are intended to fix vulnerabilities in firewall and spam protection application in this area. The IDS enables the monitoring and control of the system. The network architecture and security flaws can be audited and the credibility of critical system and databases can be assessed by the IDS. Besides this, interaction pattern statistics based on a combination of the targeted attack, abnormal behavior analysis, and the operating system audit can also be done [13]. Yet another additional benefit of the IDS is its capacity to document an organization's intrusion or potential risk to raise public awareness via log files of the latest trends of attacks. The categories of IDS-detected device attacks are classified into three distinct categories: (i) scanning attacks, (ii) denial of service (DOS) attacks, and (iii) penetration attacks [14]. Each of these 3 types of computer attacks is distinguished by different signatures. Actions-IDS is intended for the study, identification and triggering of an alarm. Upon setting an alert, network managers may need to review logs to determine whether such an activity reported is potentially abnormal or not.

The growing detection capability of malicious traffic operations has contributed to an assaulting technique that is complex and comprehensive. More than one linked and co-influenced machine node assaults are orchestrated attacks. They allow the attackers to access the Internet for an undetectable operation. Coordinated attacks are the undistorted functionality caused by the hackers/ intruders' request to expose their illicit practices by a device or by a network. If a collection of computing devices that is connected with various locations is managed by a bad actor, or an operator initiates a connection, it can be very difficult to track back to the start because of the complexities of the internet. This poses a huge risk to the legitimate Internet activity and is the cause for data leakage, clicking abuse, denial of service (DoS), assault, e-mail fraud, etc.; incidents which are becoming increasingly common nowadays [2].

Numerous malicious attempts on Networks, like DDoS, and ORM, are among the most critical issues in today's society. DDoS is a significant source of data. DDoS cyber-attacks are becoming a common worldwide internet disruption. Since these assaults/threats require network services and transport levels where verification of whether the access is legitimate or destructive is a challenging task, it becomes difficult to protect the systems against such attacks. An association of the DDoS can conveniently misrepresent its default gateway, which hides the actual cause of the incident. DDoS attacks have two targets. The first target is to use the host's resources and the second is to use the network's throughput. The present schemes for safeguarding the host's resources include drop input packets by fields. These schemes could be the *protocol type* or the *port number*. However, the downside of doing so is that it cannot be properly separated from malicious traffic by regular transport [3].

Technologies and methods used to identify suspicious traffic are updated by using the IDS framework. This framework monitors the malicious traffic by using signature-based, anomaly-based, network-based, host-based, mining-based and hybrid-based detection techniques. Although they have proven to be efficient network protection elements, they do not recognize malfunctions when: (1) traffic is encrypted, or (2) traffic is collected in the case of large traffic to retain the scalable detection [4], [22]–[24]. Many researchers have investigated the path of detecting malicious activity based on abnormal networks [4]–[6], [25], [26], primarily by extracting normal traffic patterns and creating a database of specifications. However, there is a lack of research on the comparative analysis of malicious traffic detection approach. The present study intends to achieve this objective.

Furthermore, selection of malicious traffic detection approach is a decision making problem [4]–[6]. Therefore, I have opted for an integrated fuzzy AHP-TOPSIS method for the *selection* of effective malicious traffic detection approach. The Fuzzy AHP is designed to model the vagueness, uncertainty and total awareness of languages. In addition, the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) was used to assess the order of preference. The multi-criteria decision-making (MCDM) method was employed for classifying the impact of the alternatives according to their overall performance. The findings of this paper's empirical framework will help in the assessment process; facilitating in the choice of an effective traffic detection approach for more reliable, efficient and systematic design.

The rest of this article is structured as follows: Background on malicious traffic detection approach has been discussed in Section 2. The integrated methodology with architectural and experimental results is covered in Section 3. Section 4 presents the comparison between fuzzy and classical based methods. Section 5 summarizes the research and provides some possible outlooks before concluding the article.

II. MALICIOUS TRAFFIC DETECTION APPROACH

Malware grows and changes continuously. An overview of the contact that the malware conducts in the network is one way to classify a malware. These malicious traffic patterns can be used to classify malicious programs by means of Machine Learning. Machine learning encounters two hurdles: the development of malicious as well as regular traffic, and retraining systems with malware. Traffic analysis is focused on the extraction of HTTP proxy log data of communication trends that are malware-specific. Compatible techniques compute functionality from the proxy log areas and create a detector that makes assumptions about the target activity of the specific malware group. A software or hardware and application suite is used to automatically investigate suspicious or potentially unsuitable behaviors on or around the computer system.

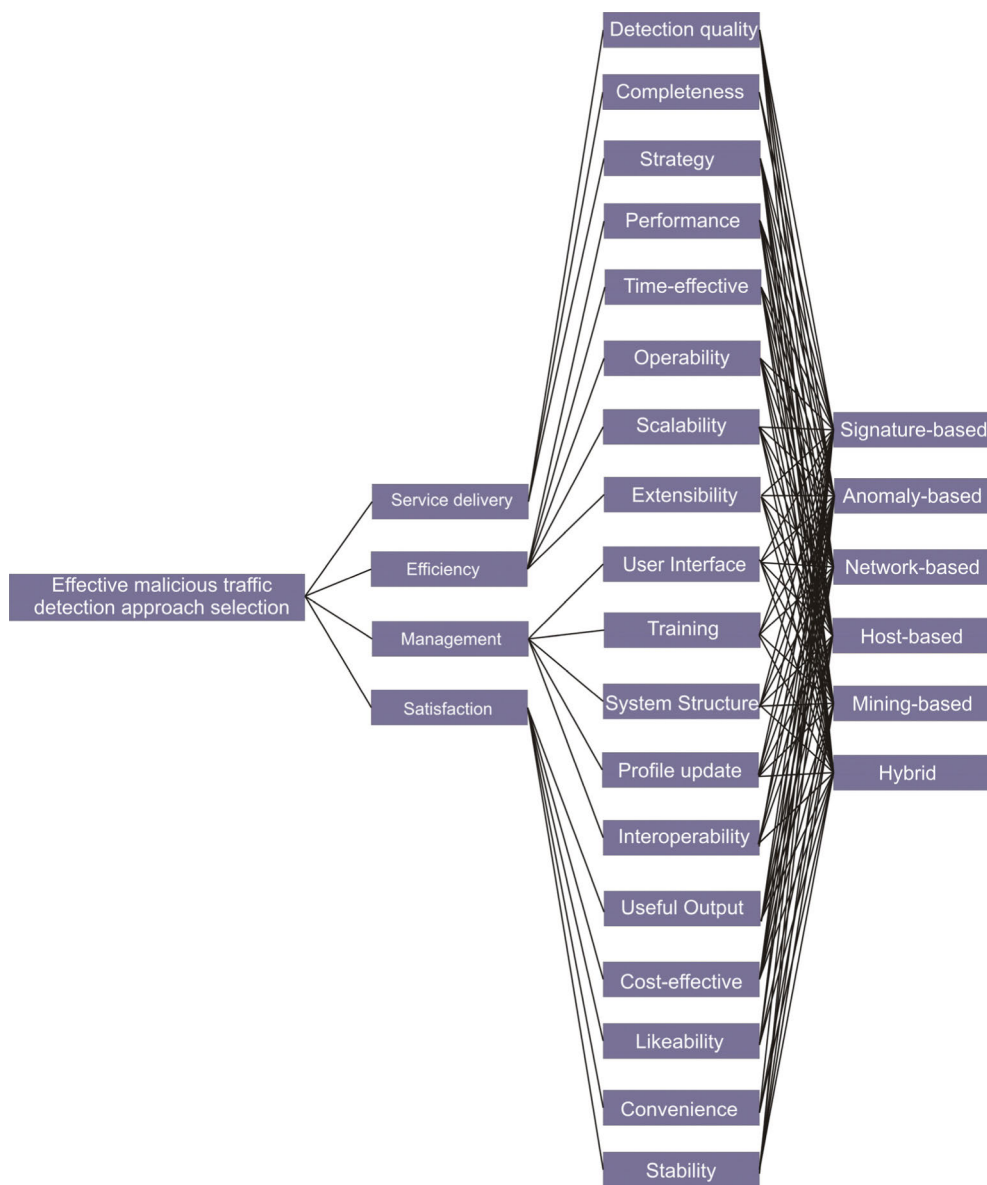


FIGURE 1. Hierarchical Representation of the MCDM Problem.

Preventive checks aim to prevent undesirable incidents, while detective checks aim to recognize unwanted incidents after they arise. Usually, the IDS is utilized as a detective search to alert people about abuse and to provide details about the frequency of the incident. Such detective controls incorporate signature-based approaches as well as uncommon traffic analysis and antivirus scanners. This enables broader identification, but suffers from issues of false alarms. The IDS can also be employed as a preventive mechanism; the current IDS can disrupt a host’s device call or disrupt the operation of the network. In this situation, the IDS needs to be changed so as to allow for this kind of operation only when the inappropriate behavior is clearly defined. In the present study, I have used different criteria for evaluating the performance of these malicious traffic detection systems at the implemen-

tation phase [4]–[8]. The criteria includes: *Service delivery*, *Efficiency*, *Management*, and *Satisfaction* which are represented as *DF1*, *DF2*, *DF3* and *DF4*, respectively. Fig. 1, given below, represents the structure of malicious traffic detection and elucidates the selected criteria.

- Service delivery (DF1): Network service delivery is established to maintain quick, safe and reliable delivery of information and communications streaming over a digital network. Service delivery is further affected by its sub-factors-*Detection quality*, *completeness* and *strategy* [25], which are further added in the hierarchy at level 2.
- Efficiency (DF2): The volume of units that have been assigned from an objective is efficiency. It is a calculation in more statistical or scientific terms of how well

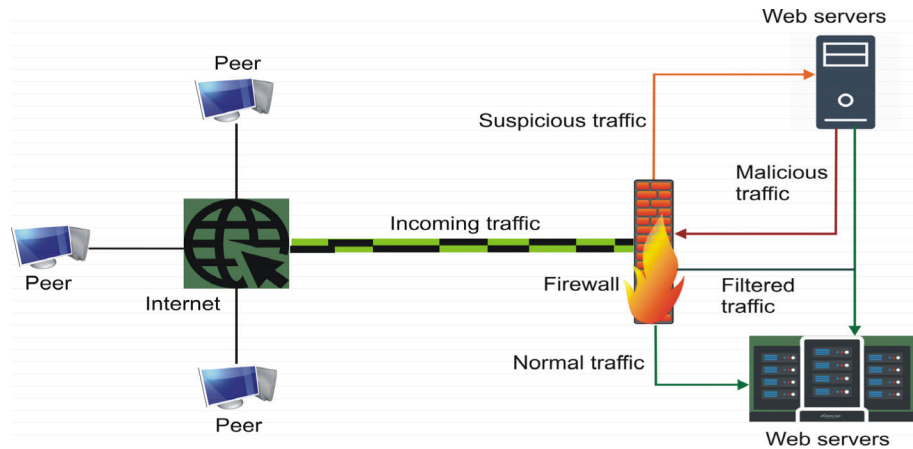


FIGURE 2. Overview of Malicious Traffic.

a technique is used for malicious traffic detection. Efficiency is further affected by *Performance, time-effective, operability, scalability and extensibility* as explained by their definitions [12]. These sub-attributes are further added in the hierarchy at level 2.

- Management (DF3): Centrally controlled management and monitoring solution ensure handling and managing multi-site infrastructure with interactive monitoring systems. This factor is affected by *User interface, training, system structure, profile update and interoperability* as per their introduction [18]. These sub-factors have also been added in the hierarchy at level 2.
- Satisfaction (DF4): The requirements whereby malicious traffic detection is implemented would be fulfilled. Criteria of acceptance that explain the intended result are the requirements of satisfaction. This factor is influenced by its sub-factors such as *Useful output, cost-effective, likeability, convenience and stability* [21]. These sub-factors are added in the hierarchy at level 2.

Besides the attributes mentioned above, this study also discusses about six types of malicious traffic detection systems as alternatives. These types are: *Signature-based; anomaly-based; network-based; host-based; mining-based; and hybrid-based detection techniques*. Malicious traffic detection systems typically consist of one or more sensing devices and a monitoring station. As traffic must be interpreted by the control to evaluate it, it is symmetrically distributed to key locations in the entire network. The Fig. 2 represents the structure of malicious traffic detection in a generalized form.

A. SIGNATURE-BASED

The signature-based identification methods for monitoring the malicious traffic have been in use for a long while now. The oldest known IDS rely heavily on signature definitions by viral scanners to classify infected data. The information of valuable signatures and the actions of current malware is particularly useful for the identification of the malicious code. For instance, *Snort* [5] is a device that tracks network

traffic in an open-sourced malicious traffic detection system to track intrusion signals. Snort is designed, much like other IDS systems, with a collection of standards or signatures which are considered to be the suspects of log traffic. The aim is to equate the actual observed malicious network traffic with such a collection of known accounts of attacks. Signature numbers could be thousands in a standard IDS database [8]. A standard signature can be interpreted as a series of network header checks and payload information – values for some standard header fields, traditional textual substrates, and function names. The “clean” evaluation of all the signatures towards one network packet hence results in hundreds of thousands of operational processes on machines. This is one of the main factors preventing large-scale deployment of such services on and outside high-speed networks. The identification of suspected malware can however be achieved with the help of signature-based detection approaches. Thus, the method is not effective for unknown malicious traffic. The following Fig. 3 shows the graphical structure of Signature-based traffic detection method.

B. ANOMALY-BASED

Anomaly-based malicious traffic detection focuses on abnormalities. It is an intrusion detection system for the identification and exploitation by tracking the actions of the device and categorizing them as normal or abnormal. The categorization in this case is not based on trends and signatures, but on algorithms or rules and intends to identify any misuse which comes from normal machine operations. Anomaly-based malicious software detection techniques aims to identify suspicious activity that could signify the existence of malicious network bottlenecks [6], such as higher bandwidth frequency, large amounts of traffic, traffic on abnormal channels and unexpected system conduct. Anomaly-based traffic detectors aim to approximate the system’s “natural” behavior, and establish an anomaly when the difference between an instant and a standard behavior exceeds a predetermined limit. The “abnormal” behavior of the system can also be

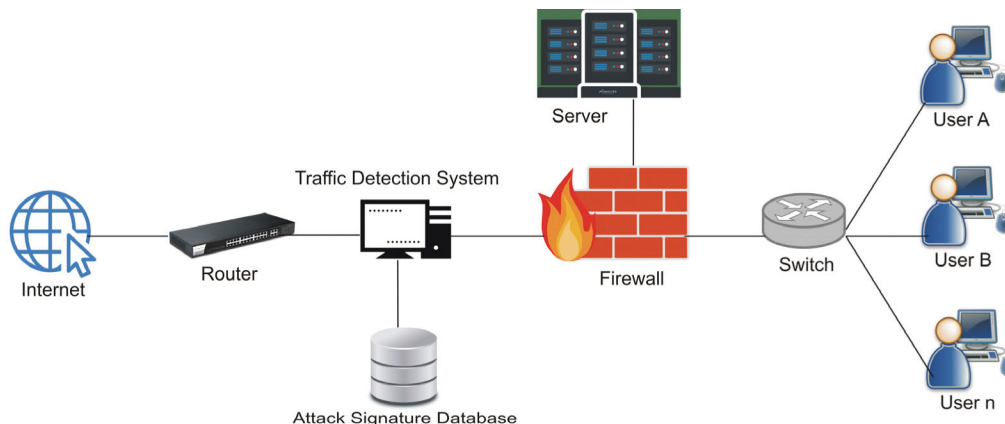


FIGURE 3. Graphical Illustration of Signature-based Traffic Detection.

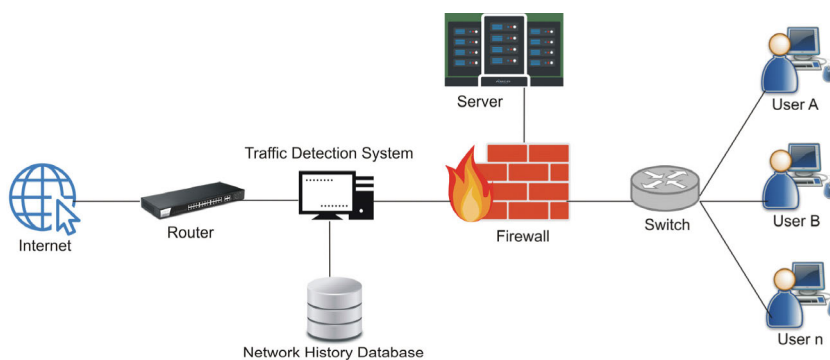


FIGURE 4. Graphical Illustration of Anomaly-based Traffic Detection.

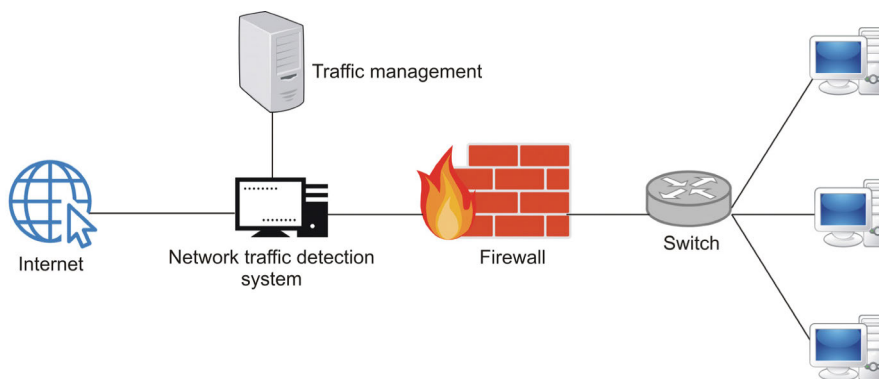


FIGURE 5. Graphical Illustration of Network-based Traffic Detection.

modeled and an alarm is raised when the discrepancy between the behavior observed and that predicted falls below a certain threshold. Fig. 4 shows the graphical structure of Anomaly-based traffic detection approach.

C. NETWORK-BASED

Network-based intrusion detection systems (NIDS) are smart, network-distributing devices that systematically inspect malicious traffic through networks. NIDS may be hardware or device based devices, and can be connected to

different network media like wireless connections, FDDI, and many others, based on the model of the device. NIDS also has two interfaces in the network. One of the most general complaints is that of the unfaithful network communications, and the other to monitor and track [11]. A network-based malicious traffic detects destructive traffic. In order to examine all traffic, along with unicast traffic, NIDS typically requires unfaithful internet connectivity. NIDS are passive instruments that do not intervene with controlling traffic. Fig. 5 depicts a structure typical of the NIDS.

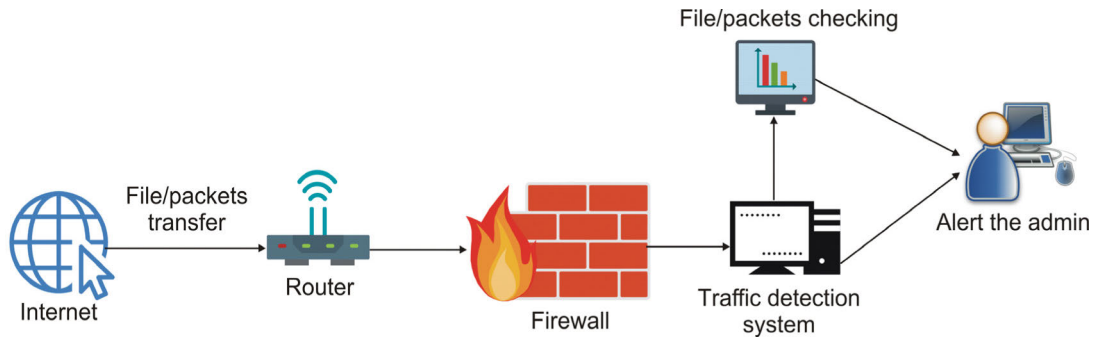


FIGURE 6. Graphical Illustration of Host-based Traffic Detection.

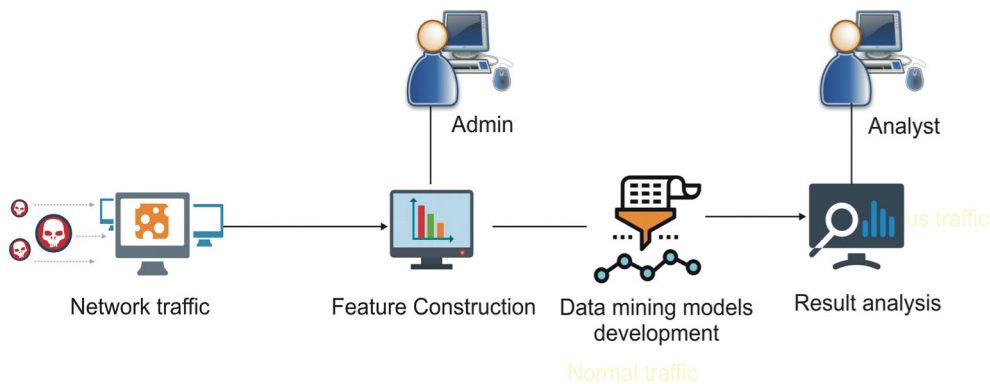


FIGURE 7. Graphical Illustration of Mining-based Traffic Detection.

Network-based approach snips the firewall's internal gateway in read-only configuration and delivers warnings via another network connection to the NIDS centralized management server.

D. HOST-BASED

The Host-based malicious traffic detection approach analyzes device status, system calls, memory management change, program logs, and other behaviors of the system. The evolution of the traditional host-based intrusion prevention system (HIPS) is a new device white-listing method. Host-based IDS operates on host systems and detects the symptoms of alleged activity. Examples may involve device registry updates, failed login efforts, or backdoor deployment. In most cases, host-based IDSs control device objects, operations and memory sections. The IDS will typically monitor the characteristics of each object in order to identify modifications, such as privileges, size, date and time of modification and hazardous contents [9]. The operations on or guided to the web server of a specific host are analyzed by using HIDS. They have several benefits, but with a significantly decreased area of activity than network-based intrusion detection systems (NIDS). Just like firewalls, these tools can vary from minor consumer models to far more sophisticated business models that enable centralized surveillance and administration.

One possible weakness with the centrally controlled HIDS is that the data needs to be distributed over the network system

to ensure the program to detect an assault on the control system in real time. If we deliberately target the host in query via the same channel, we will not be allowed to do so. It is possible that if we see many devices accidentally, we may try to minimize these problems by sending a daily signal from the system to the management system so that we can take on a query [10]. Fig. 6 shows the graphical structure of Host-based malicious traffic detection approach.

E. MINING-BASED

Effective mining methods are not sufficient to build deployable IDSs directly. Although the mining-based malicious traffic detection promises to be adequately detected and generalized, there are a few problems with their design and adoption. The benefit of using data mining techniques is that they can detect the new threats that are handmade. However, data mining traffic detection approach is only effective if the rate of detection is greater than a passably low false positive rate of detection by the manufactured method [12]. One efficient method of detecting malicious traffic is to recognize possible intrusion. However malicious traffic is hard to identify. In general, the traffic is similar to normal traffic because malware use standard protocols for establishing communications. In addition, malicious traffic is not volume-intensive and does not cause increased network latency. Thus, approaches focused on anomalies are not

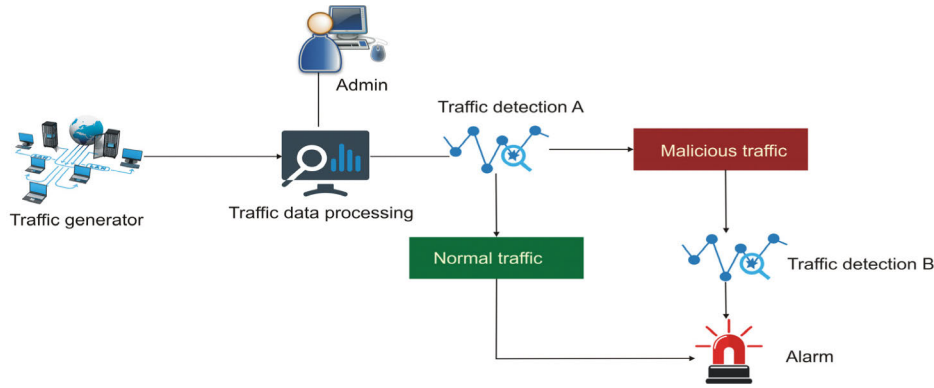


FIGURE 8. Graphical Illustration of Hybrid Traffic Detection.

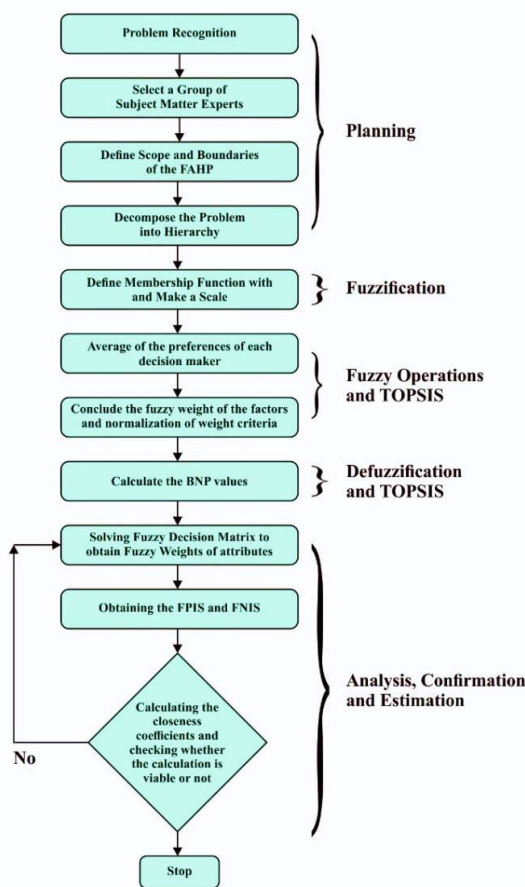


FIGURE 9. Flow Chart of Fuzzy AHP-TOPSIS Method.

helpful in detecting malicious traffic. Various data mining methods can be used effectively to detect the malicious traffic involving machine learning, classification as well as clustering. Fig. 7 shows the graphical representation of mining based traffic detection approach.

F. HYBRID

Many researchers have reported in the previous years about the issues in using anomaly-based including hybrid traffic detection approach. Anomaly-based method in novel targets

on computer network is more successful than a signature-based method. In certain instances, however, the signature-based method is easy to detect anomaly-system threats. The accuracy varies according to the sample used to evaluate certain techniques. This sample also does not reflect the actual network traffic. It can consist of various malicious strategies for detecting the traffic such as module for anomaly and misuse identification. By using the Hybrid traffic detection method, the aim is to increase the detection rate and reduce the false positive frequency by gaining the benefits of detecting misuse and detecting anomalies. The hybrid model may enhance precision and detect novel infringements. Fig. 8 represents the graphical illustration of hybrid malicious traffic detection approach.

III. METHODOLOGY AND RESULTS

From the analysis of specific literature review, I concluded that Fuzzy-AHP and Fuzzy-TOPSIS have been employed in different studies to determine the best optimized solution in MCDM related challenges. There are also several pertinent reviews that describe malicious trafficking, assessment of the difference between malicious security threats and its concrete execution to satisfy maximum security requirements. However, author of the paper did not find any study that propositioned the use of Fuzzy-AHP and Fuzzy-TOPSIS to evaluate the malicious traffic on internet perspective. Therefore, my investigation effort will create an evaluation to calculate 6different alternatives of an educational institution, Babasaheb Bhimrao Ambedkar University in Lucknow, India, in malicious trafficking perspective through the integrated Fuzzy-AHP-TOPSIS. This evaluation hybrid technique will not only be more successful in providing secure services, but will also allow the higher education institutes to examine their current security’s level.

A. FUZZY AHP-TOPSIS

The methodology of the study offers a context within which the research is carried out by a researcher [21]. The analysis methodology used in this study to achieve the objective of evaluating malicious trafficking in network is based on fuzzy AHP-TOPSIS, an important MCMD tool. To weights

TABLE 1. Fuzzy-Aggregated Pair-Wise Comparison Matrix at Level 1.

	DF1	DF2	DF3	DF4
DF1	1.00000, 1.00000, 1.00000	0.34124, 0.40457, 0.48125	0.56164, 0.94587, 1.37856	0.38754, 0.43458, 0.47569
DF2	2.08457, 2.50452, 2.94125	1.00000, 1.00000, 1.00000	0.84580, 0.97854, 1.24587	0.79457, 0.88857, 1.02565
DF3	0.73126, 1.11111, 1.79857	0.83547, 1.03568, 1.25659	1.00000, 1.00000, 1.00000	0.50459, 0.70567, 0.93586
DF4	2.13451, 2.33126, 2.57526	0.98856, 1.14968, 1.27567	1.08854, 1.43458, 2.12354	1.00000, 1.00000, 1.00000

TABLE 2. Fuzzy Aggregated Pair-Wise Comparison Matrix at Level 2 for Service Delivery.

	DF11	DF12	DF13
DF11	1.00000, 1.00000, 1.00000	0.41000, 0.55000, 0.79000	0.80000, 1.24000, 1.78000
DF12	1.26000, 1.81000, 2.43000	1.00000, 1.00000, 1.00000	0.38000, 0.55000, 0.84000
DF13	0.56000, 0.80000, 1.25000	1.19000, 1.81000, 2.63000	1.00000, 1.00000, 1.00000

TABLE 3. Fuzzy Aggregated Pair-Wise Comparison Matrix at Level 2 for Efficiency.

	DF21	DF22	DF23	DF24	DF25
DF21	1.00000, 1.00000, 1.00000	0.97125, 1.25547, 1.61125	1.06564, 1.59857, 2.22564	0.77265, 1.01852, 1.29159	0.76753, 0.91459, 1.10952
DF22	0.62145, 0.84587, 1.03058	1.00000, 1.00000, 1.00000	0.64, 0.91, 1.34	0.43741, 0.63114, 0.97447	0.35441, 0.49114, 0.87142
DF23	0.45854, 0.62885, 0.94365	0.74645, 1.09448, 1.56447	1.00000, 1.00000, 1.00000	0.52114, 0.66114, 0.79114	0.52441, 0.66114, 0.92114
DF24	0.77585, 0.99045, 0.29874	1.03044, 1.58414, 2.32444	1.26484, 1.51745, 1.92423	1.00000, 1.00000, 1.00000	0.56114, 0.65114, 0.81114
DF25	0.90456, 1.09841, 1.31412	1.14747, 2.04774, 2.85456	1.08412, 1.51441, 1.92147	1.23444, 1.53412, 1.78456	1.00000, 1.00000, 1.00000

TABLE 4. Fuzzy Aggregated Pair-Wise Comparison Matrix at Level 2 for Management.

	DF31	DF32	DF33	DF34	DF35
DF31	1.00000, 1.00000, 1.00000	1.87000, 2.60000, 3.21000	1.46000, 1.68000, 1.97000	1.45000, 2.44000, 3.39000	0.48000, 0.57000, 0.79000
DF32	0.31100, 0.38000, 0.53400	1.00000, 1.00000, 1.00000	0.61000, 0.78000, 1.03000	0.77000, 0.95000, 1.24000	0.16000, 0.20000, 0.25000
DF31	1.00000, 1.00000, 1.00000	1.87000, 2.60000, 3.21000	1.46000, 1.68000, 1.97000	1.45000, 2.44000, 3.39000	0.48000, 0.57000, 0.79000
DF32	0.31100, 0.38000, 0.53400	1.00000, 1.00000, 1.00000	0.61000, 0.78000, 1.03000	0.77000, 0.95000, 1.24000	0.16000, 0.20000, 0.25000

TABLE 5. Fuzzy Aggregated Pair-Wise Comparison Matrix at Level 2 for Satisfaction.

	DF41	DF42	DF43	DF44	DF45
DF41	1.00000, 1.00000, 1.00000	1.00000, 1.52000, 1.93000	0.49000, 0.64000, 1.00000	0.42000, 0.57000, 1.00000	0.22000, 0.29000, 0.42000
DF42	0.51844, 0.65700, 1.00000	1.00000, 1.00000, 1.00000	0.57124, 0.67445, 0.80125	0.31441, 0.39112, 0.56147	0.27414, 0.34415, 0.52125
DF43	1.00000, 1.56000, 2.04000	1.25542, 1.49441, 1.75147	1.00000, 1.00000, 1.00000	1.00000, 1.32000, 1.55000	0.30000, 0.44000, 0.80000
DF44	1.00000, 1.75000, 2.38000	1.78412, 2.56112, 3.22112	0.64500, 0.75000, 1.00000	1.00000, 1.00000, 1.00000	0.54000, 0.91000, 1.58000
DF45	2.38000, 3.44000, 4.54000	1.92114, 2.85114, 3.70125	1.25000, 2.27000, 3.33000	0.63200, 1.09800, 1.85000	1.00000, 1.00000, 1.00000

assessment of the variables and their interdependence on each other in the AHP, Fuzzy-AHP is used. And finally, the TOPSIS system is employed for the alternative’s ranks. A detailed description of these approaches has been discussed below.

B. Fuzzy-AHP

Fuzzy logic, which is based on mathematical fuzzy-set theory, is an advanced type of conventional logic which was coined by [11]. The uncertainties of a problem are considered by Fuzzy-logic when it is difficult to evaluate whether the solution of the problem is either *fully true* or *completely false*. It deliberates 0 and 1 to be two extreme cases of reality

and introduces some other cases between 0 and 1 for the purpose of addressing and handling ambiguous and imprecise decision-making information [22]. The AHP is a multi-criteria approach for decision making and is used in problems of decision analysis. It is the AHP generalization [23].

C. Fuzzy-TOPSIS

Ching-Lai Hwang and Yoon originally devised TOPSIS as a MCDM method for solving problems [28]. It is an upgraded version of Zelany’s displaced ideal solution definition. TOPSIS was found to be the best MCDM method to solve the problem of rank reversal, specifying that the alternative

TABLE 6. Summary of the Results.

The first level	The weight of first level	The second level	Local weight of second level	The final weight of the second level	Defuzzified Weights
DF1	0.14611, 0.15123, 0.19147	DF11	0.20841, 0.21511, 0.22911	0.03000, 0.03200, 0.04300	0.03500
		DF12	0.30200, 0.31000, 0.45200, 0.46300, 0.48700	0.00500, 0.04600, 0.06200, 0.07000, 0.09300	0.03800
		DF21	0.20200, 0.22500, 0.22000, 0.25100, 0.31100, 0.35300, 0.51400	0.05800, 0.06700, 0.08400, 0.19000, 0.09900, 0.18000	0.07100
		DF22	0.22000, 0.25100, 0.31100, 0.35300, 0.51400	0.06300, 0.07500, 0.19000, 0.09900, 0.18000	0.00900
DF2	0.28900, 0.31241, 0.35141	DF23	0.11200, 0.16900, 0.21100, 0.27400, 0.51000, 0.57100, 0.60400	0.03200, 0.05000, 0.07400, 0.07000, 0.09600	0.05200
		DF24	0.16900, 0.21100, 0.27400, 0.51000, 0.57100, 0.60400	0.07400, 0.07000, 0.09600	0.07400
		DF31	0.23300, 0.23800, 0.26400, 0.28000, 0.31000, 0.14100, 0.14100, 0.04000	0.04800, 0.05003, 0.08000, 0.03100, 0.04000	0.06300
		DF32	0.13500, 0.14100, 0.14100, 0.04000, 0.12500, 0.13600, 0.17700, 0.05400	0.02800, 0.03100, 0.04000, 0.03000, 0.05400	0.03300
DF3	0.20800, 0.22600, 0.30612	DF33	0.59200, 0.60200, 0.72700, 0.22200, 0.43100, 0.08900, 0.10000, 0.46300, 0.45900, 0.14000	0.12300, 0.13600, 0.22200, 0.10000, 0.14000	0.15200
		DF34	0.43100, 0.46300, 0.45900, 0.14000, 0.23500, 0.07600, 0.08700, 0.25500, 0.26600, 0.10800	0.08900, 0.10000, 0.14000, 0.08700, 0.10800	0.01100
		DF41	0.52800, 0.17000, 0.18000, 0.53500, 0.54800, 0.22300	0.17000, 0.18000, 0.22300	0.06500
		DF42	0.40200, 0.13000, 0.14000, 0.41400, 0.42800, 0.17400	0.13000, 0.14000, 0.17400	0.04800
DF4	0.32411, 0.34400, 0.40722	DF43	0.23200, 0.24000, 0.26900, 0.10900	0.07500, 0.08000, 0.10900	0.04900
		DF44	0.27700, 0.28400, 0.28900, 0.06400	0.05100, 0.05700, 0.06400	0.01100
		DF45	0.27700, 0.28400, 0.28900, 0.06400	0.05100, 0.05700, 0.06400	0.01100

ranking can be modified when a non-optimal alternative is found [26]. The key concept of TOPSIS is that a minimum distance from PIS, and a maximum NIS distance should be the best choice amongst all the competing alternatives [29]. In this concept, NIS minimises the benefit criteria and maximizes the cost criteria, whereas the PIS maximises the benefit criteria and minimises the cost criteria [30]. TOPSIS is the best-known alternative rating approach for MCDM issues.

A three step approach was used in this analysis to define, prioritize and classify both obstacles and solutions. In the very first point, the scenario in malicious traffic detection approach performance was studied and obstacles and solutions in relation to practices were established. The second step used fuzzy analytic hierarchy process (Fuzzy-AHP) to determine the weights of the criteria and sub-criteria for evaluating the alternatives. In the third step, the fuzzy Technique for Order Preference by Similarities to Ideal Solution (Fuzzy-TOPSIS) was employed to prioritize and classify the alternatives. While decision-making can be accomplished with the use of fuzzy AHP, it can be enhanced by combining multifunctional decision-making processes with other policy support tools [17], [27], [41], [42]. This research there-

fore proposes hybrid techniques of fuzzy AHP and TOPSIS to select the effective malicious traffic detection approach, as illustrated in Fig. 9.

During this MCDM process, experts, academicians and researchers have established and assessed the evaluation practices, barriers and solutions for efficient malicious traffic detection system through the literature evaluations in which the established barriers and solutions are shown.

Saaty [42] introduced the Analytic Hierarchy Process (AHP) which is considered to be one of the most important and efficient methods for addressing difficult multiple criteria decision-making [28]–[32]. However, there are some constraints in the use of the AHP, like an inconsistent judgmental reach and the lack of ambiguity. Fuzzy’s approach was also used to address these issues [33]–[36], [43], [44]. Chang [45] proposed Fuzzy AHP technique, the Triangular Fuzzy Number (TFN), which is preferred for making the Fuzzy AHP’s pair-wise scale. This scale is used as the scope analysis tool to calculate the computational scope pair-wise.

TOPSIS was introduced by Hwang and Yoon [46] as one of the multiple criteria decision making methods (MCDM). It is generally used for major issues of rankings. Selective

TABLE 7. Subjective Cognition Results of Evaluators in Linguistic Terms.

Properties/ Alternatives	MTD1	MTD2	MTD3	MTD4	MTD5	MTD6
DF11	2.450, 4.450, 6.450	2.910, 4.640, 6.550	1.450, 3.000, 4.910	1.180, 2.820, 4.820	2.090, 3.730, 5.730	2.450, 4.270, 6.270
DF12	2.820, 4.820, 6.820	3.180, 5.180, 7.100	1.450, 3.070, 4.910	0.820, 2.270, 4.270	3.000, 4.820, 6.820	2.090, 3.730, 5.730
DF13	4.270, 6.270, 8.140	2.820, 4.820, 6.820	3.180, 5.180, 7.100	1.450, 3.070, 4.910	0.820, 2.270, 4.270	3.000, 4.820, 6.820
DF21	5.360, 7.360, 9.120	3.730, 5.730, 7.550	2.450, 4.450, 6.450	0.910, 2.450, 4.450	2.450, 4.270, 6.270	3.910, 5.910, 7.820
DF22	4.640, 6.640, 8.550	3.000, 5.000, 7.140	2.180, 4.090, 6.140	2.820, 4.640, 6.640	1.910, 3.730, 5.730	2.550, 4.450, 6.450
DF23	3.120, 5.000, 7.140	2.450, 4.450, 6.450	0.910, 2.450, 4.450	2.450, 4.270, 6.270	3.910, 5.910, 7.820	3.910, 5.910, 7.910
DF24	5.360, 7.360, 9.090	4.280, 6.370, 8.370	2.450, 4.450, 6.450	2.910, 4.640, 6.550	1.450, 3.000, 4.910	3.180, 5.180, 7.090
DF25	4.280, 6.370, 8.370	4.270, 6.270, 8.140	2.820, 4.820, 6.820	3.180, 5.180, 7.100	1.450, 3.070, 4.910	2.090, 3.730, 5.730
DF31	3.180, 5.180, 7.100	1.450, 3.070, 4.910	0.820, 2.270, 4.270	3.000, 4.820, 6.820	0.820, 2.270, 4.270	3.000, 4.820, 6.820
DF32	2.450, 4.450, 6.450	0.910, 2.450, 4.450	2.450, 4.270, 6.270	3.910, 5.910, 7.820	2.450, 4.270, 6.270	3.910, 5.910, 7.820
DF33	2.180, 4.090, 6.140	2.820, 4.640, 6.640	1.910, 3.730, 5.730	2.550, 4.450, 6.450	1.910, 3.730, 5.730	2.550, 4.450, 6.450
DF34	0.910, 2.450, 4.450	2.450, 4.270, 6.270	3.180, 5.180, 7.100	1.450, 3.070, 4.910	0.820, 2.270, 4.270	3.000, 4.820, 6.820
DF35	2.450, 4.450, 6.450	2.910, 4.640, 6.550	2.450, 4.450, 6.450	0.910, 2.450, 4.450	2.450, 4.270, 6.270	3.910, 5.910, 7.820
DF41	2.820, 4.820, 6.820	3.180, 5.180, 7.100	2.180, 4.090, 6.140	2.820, 4.640, 6.640	1.910, 3.730, 5.730	2.550, 4.450, 6.450
DF42	4.280, 6.370, 8.370	2.450, 4.450, 6.450	0.910, 2.450, 4.450	2.450, 4.270, 6.270	3.910, 5.910, 7.820	3.910, 5.910, 7.910
DF43	4.270, 6.270, 8.140	2.820, 4.820, 6.820	2.450, 4.450, 6.450	2.910, 4.640, 6.550	1.450, 3.000, 4.910	3.180, 5.180, 7.090
DF44	5.360, 7.360, 9.120	3.730, 5.730, 7.550	2.820, 4.820, 6.820	3.180, 5.180, 7.100	1.450, 3.070, 4.910	2.090, 3.730, 5.730
DF45	4.640, 6.640, 8.550	3.000, 5.000, 7.140	2.180, 4.090, 6.140	2.820, 4.640, 6.640	1.910, 3.730, 5.730	2.550, 4.450, 6.450

characteristics should be at the shortest possible distance from the ideal positive solution, and farthest from the ideal negative solution [37]–[39]. The TOPSIS approach has some restrictions in the ambiguity of the flow of data [47] that Yu [49] has reported is defined by the flaw and ambiguity of many policy issues. Therefore, a complexity of the decision-making process may result in a fuzzy environment. Thus the fuzzy TOPSIS approach was introduced. The solution of multi-criteria decision making concerns in the fuzzy based setting, and the handling of decisions and assessments of decision-makers can be done in a more suitable and efficient manner by using fuzzy TOPSIS than the standard TOPSIS process [20], [24]. According to [40], [41], [48] the phases of the integrated fuzzy AHP TOPSIS methodology used in this study can be given as follows:

D. RESULTS

This sub-section addresses numerous statistical results from the implementation of the integrated fuzzy AHP-TOPSIS model. Safety specialists typically perform behavioral assessments to examine the performance of different malicious traffic detection approaches. To that end, the problematic actions of broad collections of indicators of implementation must be defined and characterized. Experts and researchers in security and intrusion detection have a challenging task

of quantifying numerically the impact of malicious traffic detection approaches on existing cyber-attack environments. I have used a well-developed and validated decision maker technique, fuzzy based unified technique of AHP-TOPSIS, in order to achieve the goal in my research paper. This procedure is highly effective in prioritizing the different malicious traffic detection approaches as per their detection capability evaluation in modern cyber security situation.

For producing a more substantial result, I took recommendations from 70 security experts from different software firms and academic institutions. These experts had more than 11 years of research and development experience in the field of network security with relevant expertise in using the proposed simulations in a sustainable environment. They discussed about the criteria and gave the linguistic values with the help of the scale [25]–[30]. This contribution's analysis was done by collating the experts' inputs. The information subcontracted from these experts was composed with the observed investigations.

The different factors for the performance evaluation at implementation phase were: *Service delivery*, *Efficiency*, *Management and Satisfaction*; they have been represented as *DF1*, *DF2*, *DF3* and *DF4*, respectively. Systematic approach of fuzzy-AHP TOPSIS was used according to the hierarchical structure shown in Fig. 2 to determine the impact of

TABLE 8. The Normalized Fuzzy-Decision Matrix.

Properties/ Alternatives	MTD1	MTD2	MTD3	MTD4	MTD5	MTD6
DF11	0.320, 0.580, 0.850	0.470, 0.740, 1.000	0.270, 0.560, 0.860	0.250, 0.550, 0.860	0.490, 0.740, 1.000	0.300, 0.530, 0.790
DF12	0.340, 0.610, 0.870	0.380, 0.640, 0.890	0.420, 0.690, 1.000	0.390, 0.700, 1.000	0.400, 0.650, 0.890	0.260, 0.470, 0.720
DF13	0.370, 0.630, 0.900	0.420, 0.690, 0.950	0.210, 0.460, 0.730	0.120, 0.350, 0.660	0.370, 0.600, 0.860	0.370, 0.600, 0.860
DF21	0.490, 0.750, 1.000	0.320, 0.590, 0.860	0.130, 0.360, 0.670	0.370, 0.660, 0.970	0.490, 0.740, 0.980	0.490, 0.740, 0.980
DF22	0.500, 0.720, 0.930	0.390, 0.660, 0.940	0.290, 0.540, 0.820	0.420, 0.690, 1.000	0.290, 0.570, 0.880	0.320, 0.560, 0.810
DF23	0.340, 0.540, 0.780	0.320, 0.580, 0.850	0.470, 0.740, 1.000	0.270, 0.560, 0.860	0.250, 0.550, 0.860	0.490, 0.740, 1.000
DF24	0.580, 0.800, 0.990	0.340, 0.610, 0.870	0.380, 0.640, 0.890	0.420, 0.690, 1.000	0.390, 0.700, 1.000	0.400, 0.650, 0.890
DF25	0.460, 0.680, 0.890	0.370, 0.630, 0.900	0.420, 0.690, 0.950	0.210, 0.460, 0.730	0.120, 0.350, 0.660	0.370, 0.600, 0.860
DF31	0.580, 0.800, 1.000	0.490, 0.750, 1.000	0.320, 0.590, 0.860	0.130, 0.360, 0.670	0.370, 0.660, 0.970	0.490, 0.740, 0.980
DF32	0.500, 0.720, 0.930	0.320, 0.580, 0.850	0.470, 0.740, 1.000	0.270, 0.560, 0.860	0.250, 0.550, 0.860	0.490, 0.740, 1.000
DF33	0.460, 0.680, 0.890	0.340, 0.610, 0.870	0.380, 0.640, 0.890	0.420, 0.690, 1.000	0.390, 0.700, 1.000	0.400, 0.650, 0.890
DF34	0.580, 0.800, 1.000	0.370, 0.630, 0.900	0.420, 0.690, 0.950	0.320, 0.580, 0.850	0.470, 0.740, 1.000	0.270, 0.560, 0.860
DF35	0.500, 0.720, 0.930	0.490, 0.750, 1.000	0.320, 0.590, 0.860	0.340, 0.610, 0.870	0.380, 0.640, 0.890	0.420, 0.690, 1.000
DF41	0.320, 0.580, 0.850	0.470, 0.740, 1.000	0.270, 0.560, 0.860	0.370, 0.630, 0.900	0.420, 0.690, 0.950	0.210, 0.460, 0.730
DF42	0.340, 0.610, 0.870	0.380, 0.640, 0.890	0.420, 0.690, 1.000	0.490, 0.750, 1.000	0.320, 0.590, 0.860	0.130, 0.360, 0.670
DF43	0.370, 0.630, 0.900	0.420, 0.690, 0.950	0.210, 0.460, 0.730	0.120, 0.350, 0.660	0.370, 0.600, 0.860	0.370, 0.600, 0.860
DF44	0.490, 0.750, 1.000	0.320, 0.590, 0.860	0.130, 0.360, 0.670	0.370, 0.660, 0.970	0.490, 0.740, 0.980	0.490, 0.740, 0.980
DF45	0.500, 0.720, 0.930	0.390, 0.660, 0.940	0.290, 0.540, 0.820	0.420, 0.690, 1.000	0.290, 0.570, 0.880	0.320, 0.560, 0.810

different malicious traffic detection approaches. I chose 6 types-*signature-based, anomaly-based, network-based, host-based, mining-based and hybrid-based detection techniques*, which were represented as *MTD1, MTD2, MTD3, MTD4, MTD5 and MTD6*, respectively.

The hierarchical levels were prepared to control the variables and determine the outcomes. With the help of [28]–[33], the fuzzy-aggregated pair-wise comparison matrix at level 1 was developed, as shown in Tab. 1. Likewise, the fuzzy aggregated pair-wise comparison matrix at level 2 of the hierarchy was collated for service delivery, efficiency, management and satisfaction in Tab. 2 to Tab. 5, respectively. Tab. 6 shows the summary of the results.

In Tab. 7 to Tab. 9, subjective cognition results of evaluators in linguistic terms, the normalized fuzzy-decision matrix and weighted normalized fuzzy-decision matrix were obtained with the help of [34]–[38]. To be more comprehensive, an integration to measure the weights of the factor of each point was performed. Furthermore, Tab. 10 and Fig. 10 demonstrate the Closeness coefficients to the aspired level among the different alternatives with the help of [39], [40] and the tree structure of the criteria in this work.

Finally the global weights of factors obtained by fuzzy-AHP were given to fuzzy-TOPSIS method as inputs to gen-

erate rank for each alternative. The performance of different malicious traffic detection approaches has been tested by using integrated fuzzy-AHP-TOPSIS. The effective performance of six malicious traffic detection approaches was in the order of: *MTD4, MTD5, MTD6, MTD1, MTD2 and MTD3*. As per the assessment of this study, *MTD4*, the *Host-based malicious traffic detection approach*, is the most accurate and effective detection technique for malicious traffic among all the six competing alternatives.

IV. COMPARISON BETWEEN FUZZY AND CLASSICAL BASED METHODS

Problem domains where we are not able to decide whether the solution of the specified problem is completely true or completely false come under the ambit of MCDM problems. Efforts to derive solutions for these problems without considering their imprecision will produce inefficient results. In this context, fuzzy-logic proves to be highly accurate in giving efficient and effective results for such problems. It has the ability to address uncertainty that is present in the information related to the problem [47] and can generate solutions to the problem in more than two possibilities. That can be in the form of $0, 0.1, 0.2, \dots, 0.9, 1$, or *can be completely true, completely false, partially true, or partially*

TABLE 9. The Weighted Normalized Fuzzy-Decision Matrix.

Properties/ Alternatives	MTD1	MTD2	MTD3	MTD4	MTD5	MTD6
DF11	0.054, 0.116, 0.278	0.041, 0.095, 0.242	0.059, 0.121, 0.296	0.041, 0.100, 0.260	0.045, 0.098, 0.239	0.041, 0.089, 0.149
DF12	0.041, 0.095, 0.198	0.061, 0.121, 0.233	0.054, 0.116, 0.278	0.041, 0.095, 0.242	0.059, 0.121, 0.296	0.041, 0.100, 0.260
DF13	0.102, 0.137, 0.299	0.114, 0.144, 0.306	0.041, 0.095, 0.198	0.061, 0.121, 0.233	0.034, 0.091, 0.200	0.032, 0.089, 0.200
DF21	0.029, 0.067, 0.158	0.036, 0.072, 0.162	0.102, 0.137, 0.299	0.114, 0.144, 0.306	0.125, 0.155, 0.344	0.116, 0.157, 0.344
DF22	0.070, 0.126, 0.275	0.054, 0.116, 0.278	0.029, 0.067, 0.158	0.036, 0.072, 0.162	0.019, 0.052, 0.135	0.016, 0.050, 0.137
DF23	0.054, 0.116, 0.278	0.041, 0.095, 0.242	0.059, 0.121, 0.296	0.041, 0.100, 0.260	0.045, 0.098, 0.239	0.063, 0.120, 0.233
DF24	0.041, 0.095, 0.198	0.061, 0.121, 0.233	0.034, 0.091, 0.200	0.032, 0.089, 0.200	0.063, 0.120, 0.233	0.112, 0.146, 0.306
DF25	0.102, 0.137, 0.299	0.114, 0.144, 0.306	0.125, 0.155, 0.344	0.116, 0.157, 0.344	0.112, 0.146, 0.306	0.024, 0.055, 0.133
DF31	0.029, 0.067, 0.158	0.036, 0.072, 0.162	0.054, 0.116, 0.278	0.041, 0.095, 0.242	0.059, 0.121, 0.296	0.041, 0.100, 0.260
DF32	0.077, 0.131, 0.230	0.065, 0.123, 0.228	0.041, 0.095, 0.198	0.061, 0.121, 0.233	0.034, 0.091, 0.200	0.032, 0.089, 0.200
DF33	0.042, 0.080, 0.169	0.029, 0.067, 0.158	0.102, 0.137, 0.299	0.114, 0.144, 0.306	0.125, 0.155, 0.344	0.116, 0.157, 0.344
DF34	0.059, 0.118, 0.240	0.047, 0.109, 0.243	0.029, 0.067, 0.158	0.036, 0.072, 0.162	0.019, 0.052, 0.135	0.016, 0.050, 0.137
DF35	0.054, 0.116, 0.278	0.041, 0.095, 0.242	0.059, 0.121, 0.296	0.054, 0.116, 0.278	0.041, 0.095, 0.242	0.059, 0.121, 0.296
DF41	0.041, 0.095, 0.198	0.061, 0.121, 0.233	0.034, 0.091, 0.200	0.041, 0.095, 0.198	0.061, 0.121, 0.233	0.034, 0.091, 0.200
DF42	0.102, 0.137, 0.299	0.114, 0.144, 0.306	0.125, 0.155, 0.344	0.102, 0.137, 0.299	0.114, 0.144, 0.306	0.125, 0.155, 0.344
DF43	0.029, 0.067, 0.158	0.036, 0.072, 0.162	0.019, 0.052, 0.135	0.029, 0.067, 0.158	0.036, 0.072, 0.162	0.019, 0.052, 0.135
DF44	0.077, 0.131, 0.230	0.065, 0.123, 0.228	0.043, 0.096, 0.196	0.017, 0.059, 0.152	0.049, 0.108, 0.221	0.065, 0.121, 0.223
DF45	0.054, 0.116, 0.278	0.041, 0.095, 0.242	0.059, 0.121, 0.296	0.041, 0.100, 0.260	0.045, 0.098, 0.239	0.045, 0.098, 0.239
	0.029, 0.067, 0.158	0.036, 0.072, 0.162	0.019, 0.052, 0.135	0.016, 0.050, 0.137	0.024, 0.055, 0.133	0.041, 0.095, 0.198

false. Therefore, to make Classical AHP or TOPSIS more efficient and powerful while addressing MCDM problems, I integrated fuzzy logic with it.

In this context, I have also provided a comparative study of both the classical and fuzzy based approach. From the analysis of different research studies, it has been found that applying different methods on the same data shows variations in the final results. This implies that a comparative study will be beneficial for achieving more reliable results [40]. Thus, the accuracy of results has been checked by the researcher through the implementation of different techniques [41]. The author of this work has also checked the result's accuracy by applying AHP-TOPSIS integrated with fuzzy logic. Fuzzification and defuzzification of fuzzy logic changes the accuracy of results in F-AHP TOPSIS while comparing them with classical AHP-TOPSIS. Thus, fuzzy based approach needs conversion from numeric to TFN values. The comparative results of this work are presented in the Tab.11 and Fig. 11 with comparative values corresponding to each alternative (MTD-1 to MTD-6) under classical and fuzzy based approach of AHP-TOPSIS.

According to Tab.11 and Fig. 11, the results obtained by using the AHP-TOPSIS methodology have got sig-

TABLE 10. Closeness Coefficients to the Aspired Level Among the Different Alternatives.

Alternatives	d+i	d-i	Gap Degree of CC+i	Satisfaction Degree of CC-i
MTD1 A1	1.249451	1.333754	0.5167545	0.4848825
MTD2 A2	0.699454	0.840778	0.5474574	0.4545528
MTD3 A3	0.787126	1.484754	0.6544575	0.3468867
MTD4 A4	2.165457	1.484784	0.4077747	0.5937746
MTD5 A5	2.005745	1.536445	0.4347794	0.5667548
MTD6 A6	0.448774	0.397784	0.4657798	0.5354467

nificant correlation (*Pearson correlation coefficient is 0.96316*) with the results obtained through the classical approach. AHP-TOPSIS integrated with fuzzy logic had more efficiency than the classical AHP TOPSIS. Fig. 9 depicts the graphical representation of the comparative results.

V. CONCLUSION

This research presented an integrated fuzzy AHP-TOPSIS method for the performance evaluation of different malicious traffic detection approaches. The Fuzzy AHP is employed to simulate language uncertainty, ambiguity and absolute

TABLE 11. Comparison the Results of Classical and Fuzzy AHP-TOPSIS Methods.

Methods/Alternatives	MTD1	MTD2	MTD3	MTD4	MTD5	MTD6
Fuzzy-AHP-TOPSIS	0.4848825	0.4545528	0.3468867	0.5937746	0.5667548	0.5354467
Classical-AHP-TOPSIS	0.4798834	0.4554874	0.3321547	0.5945847	0.5785497	0.5458441

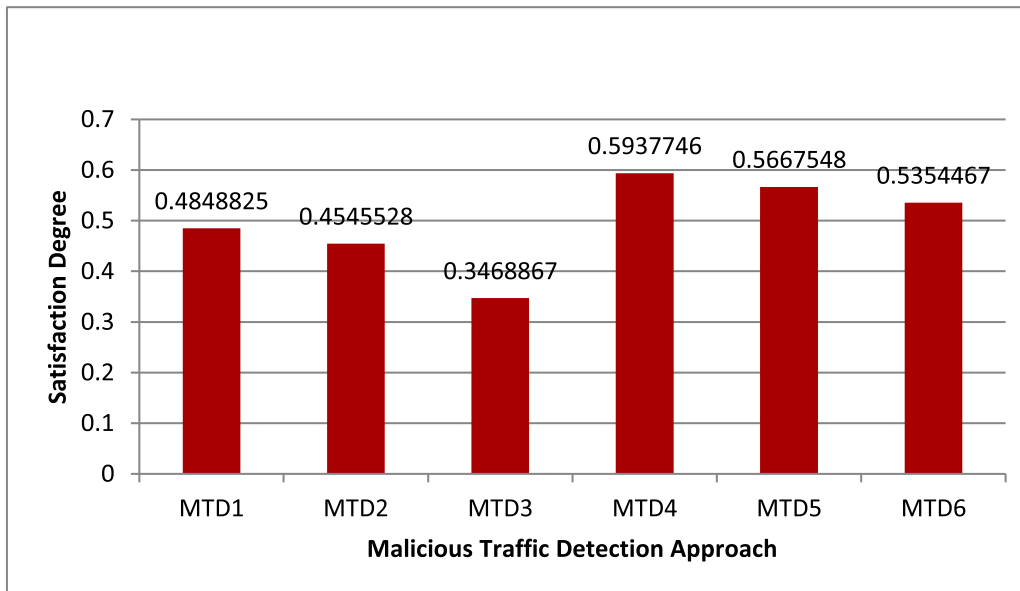


FIGURE 10. Graphical Representation of Closeness Coefficients to the Aspired Level among the Different Alternatives.

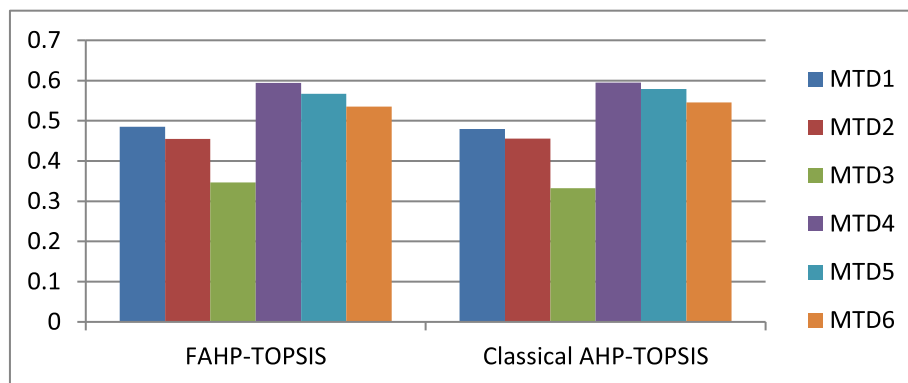


FIGURE 11. Comparative Results of Classical and Fuzzy Based AHP Techniques.

awareness. Additionally, the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), and the Multi-Criteria Decision-making (MCDM) methods are used for categorizing the alternatives’ effect according to their final performance, and to determine their order of preference. I showed different resolution of observations based on the identified set of criteria and alternatives. The findings of this study ranked the alternative (MTD4), the Host-based malicious traffic detection approach, to be the most successful and enduring malicious traffic detection mechanism among all the six alternatives. The evaluation of different traffic detection approaches incorporated in this study as well as the results drawn from the empirical analysis will support the professionals in developing high-quality traffic detection approach for malicious activities. The tabulations of my research endeavour are both conclusive and reliable; hence the findings will aid the practitioners in designing

more secure and trustworthy mechanisms for defense against internal and external threats and attacks.

REFERENCES

- [1] M. T. J. Ansari, D. Pandey, and M. Alenezi, “STORE: Security threat oriented requirements engineering methodology,” *J. King Saud Univ.-Comput. Inf. Sci.*, to be published, doi: 10.1016/j.jksuci.2018.12.005.
- [2] J. Liu, Y. Xiao, K. Ghaboosi, H. Deng, and J. Zhang, “Botnet: Classification, attacks, detection, tracing, and preventive measures,” *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, Dec. 2009, Art. no. 692654.
- [3] T. Peng, C. Leckie, and K. Ramamohanarao, “Protection from distributed denial of service attacks using history-based IP filtering,” in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 1, May 2003, pp. 482–486.
- [4] A. Boukhtouta, N. E. Lakhdari, S. A. Mokhov, and M. Debbabi, “Towards fingerprinting malicious traffic,” in *Proc. ANT/SEIT*, Jun. 2013, pp. 548–555.
- [5] B. Saha and A. Gairola, “Botnet: An overview,” CERT-In, New Delhi, India, White Paper CIWP-2005-05, Jun. 2005.
- [6] D. H. Shin, K. K. An, S. C. Choi, and H.-K. Choi, “Malicious traffic detection using K-means,” *J. Korean Inst. Commun. Inf. Sci.*, vol. 41, no. 2, pp. 277–284, Feb. 2016.

- [7] H. Bischof, A. Leonardis, and A. Selb, "MDL principle for robust vector quantisation," *Pattern Anal. Appl.*, vol. 2, no. 1, pp. 59–72, Apr. 1999.
- [8] D. S. Kazachkin and D. Y. Gamayunov, "Network traffic analysis optimization for signature-based intrusion detection systems," in *Proc. Spring/Summer Young Researchers Colloq. Softw. Eng.*, no. 2, pp. 14–26, 2008.
- [9] T. M. Chen, "Guarding against network intrusions," in *Computer and Information Security Handbook*. Burlington, MA, USA: Morgan Kaufmann, 2013, pp. 149–163.
- [10] J. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Rockland, MA, USA: Syngress, 2014.
- [11] J. D. Burton, *Cisco Security Professional's Guide to Secure Intrusion Detection Systems*. Rockland, MA, USA: Syngress, 2003.
- [12] W. Lee, S. J. Stolfo, P. K. Chan, E. Eskin, W. Fan, M. Miller, and J. Zhang, "Real time data mining-based intrusion detection," in *Proc. DARPA Inf. Survivability Conf. Expo. II. DISCEX*, vol. 1, Jun. 2001, pp. 89–100.
- [13] S. Duque and M. N. B. Omar, "Using data mining algorithms for developing a model for intrusion detection system (IDS)," *Procedia Comput. Sci.*, vol. 61, pp. 46–51, Jan. 2015.
- [14] R. G. Bace and P. Mell, "Intrusion detection systems," Special Publication (NIST SP)-800-31, 2001. [Online]. Available: <https://www.nist.gov/publications/intrusion-detection-systems>
- [15] E. Alparslan, A. Karahoca, and D. Karahoca, "BotNet detection: Enhancing analysis by using data mining techniques," in *Advances in Data Mining Knowledge Discovery and Applications*, vol. 349. London, U.K.: IntechOpen, 2012, doi: [10.5772/48804](https://doi.org/10.5772/48804).
- [16] M. T. J. Ansari and D. Pandey, "Risks, security, and privacy for HIV/AIDS data: Big data perspective," in *Big Data Analytics in HIV/AIDS Research*. Hershey, PA, USA: IGI Global, 2018, pp. 117–139.
- [17] K. Sahu and R. Shree, "Stability: Abstract roadmap of software security," *Amer. Int. J. Res. Sci., Eng. Math.*, vol. 15, no. 12, pp. 183–186, 2015.
- [18] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal, and R. A. Khan, "Measuring security durability of software through fuzzy-based decision-making process," *Int. J. Comput. Intell. Syst.*, pp. 627–642, 2019.
- [19] R. Kumar, A. Agrawal, and R. A. Khan, "A wake-up call for data integrity invulnerability," *Comput. Fraud Secur.*, vol. 2020, no. 4, pp. 14–19, Apr. 2020.
- [20] A. Agrawal, M. Alenezi, R. Kumar, and R. A. Khan, "Measuring the sustainable-security of Web applications through a fuzzy-based integrated approach of AHP and TOPSIS," *IEEE Access*, vol. 7, pp. 153936–153951, 2019.
- [21] R. Kumar, S. A. Khan, and R. A. Khan, "Analytical network process for software security: A design perspective," *CSI Trans. ICT*, vol. 4, nos. 2–4, pp. 255–258, Dec. 2016.
- [22] K. Sahu, R. Shree, and R. Kumar, "Risk management perspective in SDLC," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 3, pp. 1247–1251, 2014.
- [23] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, and R. A. Khan, "An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of Web applications," *IEEE Access*, vol. 8, pp. 50944–50957, 2020.
- [24] K. Sahu and R. K. Srivastava, "Revisiting software reliability," in *Data Management, Analytics and Innovation*. Singapore: Springer, 2019, pp. 221–235.
- [25] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, and R. A. Khan, "A knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of Web applications," *IEEE Access*, vol. 8, pp. 48870–48885, 2020.
- [26] A. Agrawal, M. Zarour, M. Alenezi, R. Kumar, and R. A. Khan, "Security durability assessment through fuzzy analytic hierarchy process," *PeerJ Comput. Sci.*, vol. 5, p. e215, Sep. 2019.
- [27] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *ICIC Exp. Lett.*, vol. 12, no. 12, pp. 1213–1222, 2018.
- [28] K. Sahu and R. K. Srivastava, "Needs and importance of reliability prediction: An industrial perspective," *Inf. Sci. Lett.*, vol. 9, no. 1, pp. 33–37, 2020.
- [29] R. Kumar, S. A. Khan, and R. A. Khan, "Software security testing a pertinent framework," *J. Global Res. Comput. Sci.*, vol. 5, no. 3, pp. 23–27, 2014.
- [30] R. Kumar, S. A. Khan, and R. A. Khan, "Software security durability," *Int. J. Comput. Sci. Technol.*, vol. 5, no. 2, pp. 23–26, 2014.
- [31] R. Kumar, S. A. Khan, and R. A. Khan, "Durable security in software development: Needs and importance," *CSI Commun.*, vol. 10, pp. 34–36, Oct. 2015.
- [32] R. Kumar, M. Alenezi, M. T. J. Ansari, B. K. Gupta, A. Agrawal, and R. A. Khan, "Evaluating the impact of malware analysis techniques for securing Web applications through a decision-making framework under fuzzy environment," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 6, pp. 94–109, Dec. 2020.
- [33] R. Kumar, S. A. Khan, and R. A. Khan, "Revisiting software security: Durability perspective," *Int. J. Hybrid Inf. Technol.*, vol. 8, no. 2, pp. 311–322, Feb. 2015.
- [34] R. Kumar, S. Khan, and R. Khan, "Revisiting software security risks," *Brit. J. Math. Comput. Sci.*, vol. 11, no. 6, pp. 1–10, Jan. 2015.
- [35] K. Sahu and R. Shree, "Software security: A risk taxonomy," *Int. J. Comput. Sci. Eng. Technol.*, vol. 3, pp. 36–41, Feb. 2015.
- [36] R. Kumar, S. A. Khan, A. Agrawal, and R. A. Khan, "Security assessment through fuzzy-Delphi analytic hierarchy process," *ICIC Exp. Lett., Int. J. Res. Surv.*, vol. 12, no. 10, pp. 1063–1069, 2018.
- [37] R. Kumar, S. A. Khan, A. Agrawal, and R. A. Khan, "Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective," *ICIC Exp. Lett.*, vol. 12, no. 6, pp. 615–620, 2018.
- [38] M. T. J. Ansari, F. A. Al-Zahrani, D. Pandey, and A. Agrawal, "A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development," *BMC Med. Informat. Decis. Making*, vol. 20, no. 1, pp. 1–13, Dec. 2020.
- [39] R. Kumar, S. A. Khan, and R. A. Khan, "Durability challenges in software engineering," *Crosstalk-J. Defense Softw. Eng.*, vol. 52, no. 10, pp. 29–31, 2016.
- [40] S. A. Khan, M. Alenezi, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating performance of software durability through an integrated fuzzy-based symmetrical method of ANP and TOPSIS," *Symmetry*, vol. 12, no. 4, p. 493, Mar. 2020.
- [41] C. Prakash and M. K. Barua, "Integration of AHP-TOPSIS method for prioritizing the solutions of reverse logistics adoption to overcome its barriers under fuzzy environment," *J. Manuf. Syst.*, vol. 37, pp. 599–615, Oct. 2015.
- [42] T. L. Saaty, "What is the analytic hierarchy process?" in *Mathematical Models for Decision Support*. Berlin, Germany: Springer, 1988, pp. 109–121.
- [43] C.-C. Sun, "A performance evaluation model by integrating fuzzy AHP and fuzzy TOPSIS methods," *Expert Syst. Appl.*, vol. 37, no. 12, pp. 7745–7754, Dec. 2010.
- [44] M. T. J. Ansari and D. Pandey, "An integration of threat modeling with attack pattern and misuse case for effective security requirement elicitation," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 3, pp. 1–5, 2017.
- [45] D. Y. Chang, "Applications of the extent analysis method on fuzzy AHP," *Eur. J. Oper. Res.*, vol. 95, no. 3, pp. 649–655, 1996.
- [46] C. L. Hwang and K. Yoon, "Methods for multiple attribute decision making," in *Multiple Attribute Decision Making*. Berlin, Germany: Springer, 1981, pp. 58–191.
- [47] M. Zarour, M. T. J. Ansari, M. Alenezi, A. K. Sarkar, M. Faizan, A. Agrawal, R. Kumar, and R. A. Khan, "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records," *IEEE Access*, vol. 8, pp. 157959–157973, 2020.
- [48] D. Kannan, A. B. L. D. S. Jabbour, and C. J. C. Jabbour, "Selecting green suppliers based on GSCM practices: Using fuzzy TOPSIS applied to a Brazilian electronics company," *Eur. J. Oper. Res.*, vol. 233, no. 2, pp. 432–447, Mar. 2014.
- [49] C.-S. Yu, "A GP-AHP method for solving group decision-making fuzzy AHP problems," *Comput. Oper. Res.*, vol. 29, no. 14, pp. 1969–2001, Dec. 2002.



SULTAN H. ALMOTIRI received the B.Sc. degree (Hons.) in computer science from King Abdulaziz University, Saudi Arabia, in 2003, and the M.Sc. degree in Internet, computer, and system security and the Ph.D. degree in wireless security from Bradford University, U.K., in 2006. He was the Chairman of the Computer Science Department with Umm AlQura University, Saudi Arabia, and also the Vice Dean of eLearning and distance education with Umm AlQura University, where he is currently an Assistant Professor with the Computer Science Department, Faculty of Computer and Information Systems. His research interests include cyber security, cryptography, AI, machine learning, eHealth, eLearning, the IoT, RFID and wireless sensors, and image processing.

...