Journal of Computing, Science &Technology
https://focjournal.unidel.edu.ng/
editorjcst@unidel.edu.ng
ISSN:.....Print
ISSN: ..... Online

Prioritizing Response Alternatives to Denial of Service on Mobile Devices Using Fuzzy ELECTRE III Method

S. B. Oyong[1], U. O. Ekong[2], O. U. Obot[3],S. E. Mughele[4]
[1,2]Department of Cybersecurity, Faculty of Computing, University of Uyo, Akwa Ibom State, Nigeria
[3]Department of Software Engineering, Faculty of Computing, University of Uyo, Akwa Ibom State, Nigeria
[4]Department of Cybersecurity, Faculty of Computing, University of Delta, Agbor, Nigeria
samueloyong@gmail.com[1], uyiekong@yahoo.com[2], okureobot@uniuyo.edu.ng[3],s.mughele@unidel.edu.ng[4]

Corresponding Author's Email: samueloyong@gmail.com

Article Info
Date Received: 12-03-2024
Date Accepted: 05-05-2024

Keywords:
Prioritizing, Alternative response, Denial of service, Fuzzy ELECTRE III method, Mobile devices.

ABSTRACT

The business world today depends on the internet, using mobile devices, for communication and business transactions. Given this shift towards cyber communication, the attack vector has also increased, especially denial of service (DOS) assaults. DOS attacks attempt to exhaust the resources of the target object, making it unusable to legitimate users. In an effort to curb the menace, automated intrusion response system (AIRS) used fuzzy ELECTRE III method to rate and prioritize response alternatives. ELECTRE III method outranks the alternative responses to the attack by pairing alternatives and selects the best option in terms of time and acceptable cost. The relationship, $M_i \rightarrow M_k$, implies that Mi is preferred to M_k (a concordance relationship) and vice versa. Other options in the relationship can be indifference (discordance test) and incomparable. This technique can be applied to other areas of multi-attribute decision making (MADM) problems. The optimum response obtained was reset connection (RST), which can be applied to foil DOS attacks in real time and at minimum cost. In addition a case study showing the implementation of an improved technique to invoicing process in a company is demonstrated with strategy #2 (purchase of an off-the-shelf application) chosen as the best option.The traditional method of selecting response action to an attack had been subjective and at the discretion of the administrator. However, in this paper, the process has been automated using Julia/REPL kernel in Jupyter Notebook platform; and reduced internal attacks like espionage and intellectual property theft by setting aside privileged users or staff like system administrators, computer operators or contractors.

1.0 INTRODUCTION

In cyber security, understanding potential threats is the first line of defense. One of such threats is denial of service (DOS) attacks [1]. DOS seeks to make host systems, the network or servers unavailable to its intended users by overwhelming them with volumes of internet control message protocol (ICMP) echo requests such as ping of death (PoD), or exploiting host systems and network vulnerabilities [2]. Distributed denial of service (DDOS) was introduced to DOS family of attacks in 1999. This attack type uses multiple machines (zombies) to simultaneously attack a network site [3] [2].

According to [2], DOS seems to be the most expensive computer crime for victim organizations. In 2000, DOS attacks cost organizations to the tune of $26,064,050:00. For instance, several DDOS attacks were perpetrated that brought down Yahoo, buy.com, Amazon, CNN and ebay, and in 2016, domain name system (DNS) was hit by massive DOS attacks and caused major internet platforms and services to be unavailable to users in Europe and North America [3]. Similarly, in 2018, GitHub was hit by DOS attacks and disrupted its services. From the foregoing, DOS attacks represent the major security threats to internet services, resulting in serious losses in revenue and reputation of affected organizations. Over 5000 targets were victims of over 12,000 DOS attacks within three weeks in 2001 [3].

Internet components such as network servers, switches, routers, hubs and modems are common targets of DOS attacks. The attacks are perpetrated using the following techniques [2] [4]:

i. TCP SYN (Transmission Control Protocol Synchronization) flood
ii. Smurf attack (ICMP flood)
iii. Land attack
iv. UDP (user datagram protocol) flood
v. Trinoo (DDOS attacks)
vi. Tribal flood Network (TFN and TFN2K)
vii. Stacheldraht
viii. Ping of Death (PoD).

These attack types are classified into:

i. Volume based attacks
ii. Protocol attacks
iii. Application layer attacks
iv. Advanced persistent DOS (APDOS) attacks

Resources attacked by such DOS types include processor time, memory, disk space, bandwidth, buffer and descriptors (descriptors are structures that contain information that describes data variables)

To foil DOS/DDOS attacks, the following techniques may be used:

i. Automated Intrusion Response Systems (AIRS)
ii. Access control list (ACL)
iii. Firewalls
iv. Intelligent Routers

ACL is a set of rules applied on host systems to control permissions; and also offer defense to a network by controlling in-coming and out-going traffic from a single point [3], while firewalls and intelligent routers are used to control incoming and outgoing traffic respectively [5].

AIRS applies fuzzy ELECTRE III (translated to Elimination and Choice Expressing REality) method to rate and prioritize a set of alternative responses that best satisfy a given set of criteria with the help of security experts. Unfortunately, there has been little research effort in identifying alternative responses for different attack scenarios that can be used by other researchers [6]. Criteria are sets of requirements or independent attributes that have to be satisfied by several alternatives. Each criterion may be measured in different units, as such, they have to be normalized to obtain a dimensionless classification. This will provide a common numeric range or scale that allows aggregation into a final score [7].

After normalization, Decision makers (DM) use concordance and discordance indices to analyze outranking relations among different alternatives, and to choose the best alternative response to an attack [8]. Concordance index measures acceptance, while discordance index measures indifference or disagreement.

2.0 REVIEW OF RELATED WORKS

In recent years, malware developers and hackers are attacking and breaching information security, specifically using denial of service attack types. Currently, the following cyber security breaches are worrisome and require urgent attention: DOS assaults, anomaly detection, software vulnerability diagnosis (weak points in both hardware and software that are exploited by malware developers), phishing (a social engineering attack, which deceives users to revealing their important and secret information) and malware identification [9]. Unfortunately, most of the tools used for these breaches are freely available on the internet [3].

[10] classified DOS attacks in terms of protocols (these are rules or regulations guiding the use of and transmission of data between devices and the internet) with respect to application layer on one hand and Network and Transport layers on the other hand. DOS attacks in Application layer of TCP/IP stack can affect Telnet, hypertext transfer protocol (HTTP), internet message access protocol (IMAP), file transfer protocol (FTP), secure shell (SSH), Internet relay chat (IRC), Simple mail transfer protocol / post office protocol (SMTP/POP), Transport layer security / secure socket layer (TLS/SSL), and more; while DOS attacks on Network layer and Transport layer can affect protocols like TCP, UDP and ICMP with examples like TCP-SYN flood, UDP flood and ICMP echo requests. Although software patching (identifying and correcting vulnerable and weak points in software programs) can protect target objects against known attacks, it does not deter or stop DOS flooding attacks [3].

However, [11] proposed the use of intrusion detection system (IDS) to detect DDOS attacks in software defined networks (SDN) using machine learning (ML) tools like K-Nearest Neighbor (KNN), Naïve Bayes (NB), K-Medoids, and K-means to categorize incoming traffic into normal or malware traffic. The drawback of this technique is that it can deal only with malware of known signature families attacking host systems. [12] Conducted intrusion detection of DDOS using REPTree classifier on KDD Cup 99 dataset. The drawback of this technique is that KDD cup 99 dataset is not only old, but full of redundant features. KDD stands for knowledge discovery in databases.

[5] used access control list (ACL) to mitigate DOS attacks. Similarly, [13] proposed a defense mechanism for DDOS in SDN by analyzing specific features of SDN to determine their suitability in foiling DDOS attack. The experiment was performed against spoofed UDP flooding (a misrepresentation of reality by a fake). [14] Attempted to balance the cost of response to that of damage done by an attack. Also, [15] proposed the use of automated intrusion response system (AIRS) to counter malware attacks, however, the proposal was not concretized with example works.

[16] used ELECTRE III method to classify requirements in software development project. [17] Attempted to improve on ELECTRE III method using linear programming models, because ELECTRE III method does not give complete outranking of alternatives since some relations are not comparable. [18] Utilized interval-valued triangular fuzzy numbers (IVTFN) in expressing experts' opinions into group consensus opinion. [19] Evaluated the effect of different normalization techniques on simple adaptive weight (SAW) method of MCDM process. Similarly, [20] provided an overview of different weighting methods in MCDM and classified them into objective, subjective and integrated methods; while [21] extended the use of ELECTRE method using intuitionistic fuzzy sets (IFS) to handle imprecise and vague decisions of decision makers.

[22] presents open command and control, OpenC2, which is a suite of building blocks that enable coordinated defense in cyber related actions. [6] Surveyed intrusion response systems (IRS) by considering taxonomy, countermeasures pool, general architecture, and decision making approaches to minimize the effects of cyber-attacks on cyber physical systems (CPS). Unfortunately, IRS has received minimal attention from the research community [6] with respect to identifying response actions for different attack scenarios

that can be used by other researchers. [23] summarized responses on automated and semi-automated incident responses as described in scholarly literature. The solutions are, however, classified based on what input data they used, what response they choose from, and how they relate to actions (beneficial or otherwise).

[24] presents autonomous cloud intrusion response system (ACIRS), which detects masquerades, host based and network based attacks and selects appropriate response to mitigate these attacks. Similarly, [25] opines that cyber threat intelligence is inclusive, covering threat information, data format, sharing and collaboration as well as incident response. Incident response domain covers response processes and courses of action. However, incident response with its many advantages has not received much research attention [25] [26]. [26 opined that incident handling is an activity in cyber security incident response. The paper surveyed approaches towards semi or automated incident handling and response backed by recommender systems. Recommender systems are information filtering systems that are currently attracting the attention of researchers.

3.0 METHODOLOGY

The data used in this research work is denial of service (DOS) attack type, contained in NSL-KDD dataset, among others. The aim of this work is to prioritize intrusion response alternatives with the help of security experts that will be used to foil such attacks in real time and at minimum cost. DOS attacks are categorized into vulnerability based attacks and flood based attacks, as depicted in Figure 1.

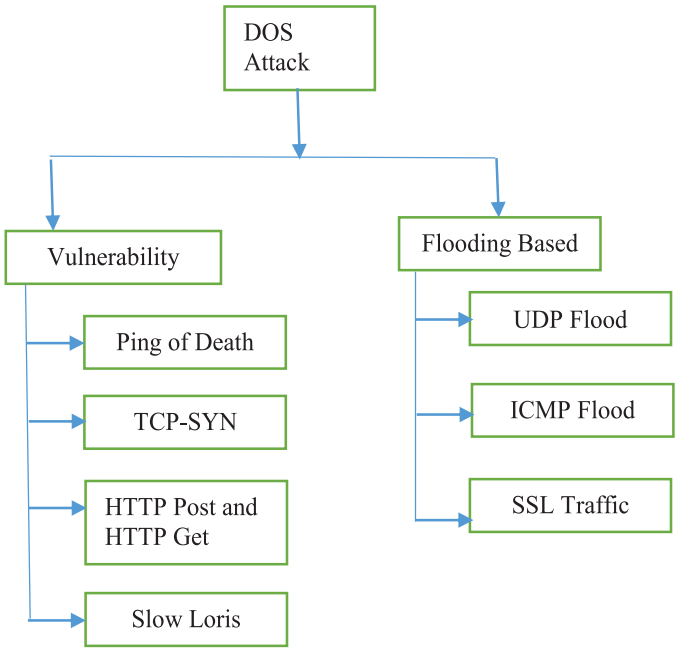

Figure 1: DOS Attack

Categories Source: [3]

Criteria	aj	Bj	Cj
C	2.0	2.2	3.0
I	2.0	3.0	4.0
A	1.0	1.0	1.0
RC	3.0	3.8	4.0

However, decision makers (DM) determined response alternatives to the various DOS attack types, as depicted in Table 1.

Table 1: Response Alternatives to DOS attacks
Source: [14]

Attack Type	Response Alternatives
DOS	I Shutdown Host (SH) II Reboot Host (RH) III Restart process (RP) IV Reset Connection (RST)

MCDM has many methods such as AHP, TOPSIS, ELECTRE, and more. Fuzzy ELECTRE III method is used in this paper to outrank, prioritize and select optimum response in Julia/REPL kernel. The environment provided for the kernel is Jupyter Notebook platform.

3.1 Fuzzy ELECTRE Method

Multiple criteria decision making problems are solved using alternative response actions based on the security criteria (Attributes) formulated by security experts. In this paper, security experts were contacted using mobile phone interview, and response actions presented in Table 1 are gotten from literature. Other options that could be used to get data or information of the DM could be by questionnaire, observation, surveys and more. The Julia package that is used to solve the MCDM problem is JMcDM [27]. It is used in solving complex problems encountered by security experts. The JMcDM technique used in this paper is Fuzzy ELECTRE III method.

In a decision process, there are m alternative responses, n criteria, weighting function, w_j and vector function (which determines if the criterion is beneficial or costly). The criteria for this research work constitute the following security attributes: Confidentiality (C), integrity (I), availability (A) and response cost (RC). Five decision makers (DM) are selected for this work, k:

K = [DM1, DM2, DM3, DM4, DM5]

And their opinions sought to rate the criteria subject to the security situation encountered.

Decision makers' opinions are processed using the following steps:

Step 1: Rank the criteria

Table 2 depicts the rank order of criteria determined by the decision makers (DM).

Table 2: Random rank order of the criteria by DM

Criteria	DM1	DM2	DM3	DM4	DM5
C	2	3	2	2	2
I	3	2	3	4	3
A	1	1	1	1	1
RC	4	4	4	3	4

Source: [28]

Step 2: Determine Aggregated Fuzzy Importance Weight from the values in Table 2

This is achieved using Eq. (1), Eq. (2), Eq. (3), and Eq. (4) respectively:

$$Wj = (aj, bj, cj). \quad (1)$$

Where

$$j = 1, 2, 3, \ldots n$$

$$a_j = \min\{y_{jk}\} \quad (2)$$

$$b_j = \frac{1}{k}\sum_{k=1}^{K} yjk \quad (3)$$

$$c_j = \max\{y_{jk}\} \quad (4)$$

y_{jk} is the rank of jth criterion by kth decision maker; and aj, bj, and cj are triplets representing the fuzzy importance weight of the jth criterion.

For instance, from Table 2, criterion C provides the values for

$$aj = 2.0$$

$$bj = \frac{1}{5}\sum_{k=1}^{5}(2+3+2+2+2)$$

$$= \frac{11}{5} = 2.2$$

$$Cj = 3.0$$

Similarly for criterion I, the weighted values include:

$$a_j = 2.0$$

$$b_j = \frac{1}{5}\sum_{k=1}^{5}(3+2+3+4+3)$$

$$= \frac{15}{5} = 3.0$$

$$c_j = 4.0$$

The computed values are depicted in Table 3.

Table 3: Aggregated Fuzzy Importance Weights for DOS attack type

Criteria	aj	Bj	Cj
C	2.0	2.2	3.0
I	2.0	3.0	4.0
A	1.0	1.0	1.0
RC	3.0	3.8	4.0

Step 3: Normalize the fuzzy importance weights in Table 3

This is achieved by using Eq. (5), Eq. (6), Eq. (7) and Eq. (8).

$$Wj = (w_{j1}, w_{j2}, w_{j3}) \quad (5)$$

Where

$$W_{j1} = \frac{1}{aj}/\sum_{j=1}^{n}\frac{1}{aj} \quad (6)$$

$$W_{j2} = \frac{1}{bj}/\sum_{j=1}^{n}\frac{1}{bj} \quad (7)$$

$$W_{j3} = \frac{1}{cj}/\sum_{j=1}^{n}\frac{1}{cj} \quad (8)$$

Applying these formulae for criterion C gives

$$W_{c1} = \frac{1}{2}/\left(\frac{1}{2}+\frac{1}{2}+\frac{1}{1}+\frac{1}{3}\right) = \frac{0.5}{0.5+0.5+1.0+0.33} = \frac{0.5}{2.33} = 0.21$$

$$W_{c2} = \frac{1}{2.2}/\left(\frac{1}{2.2}+\frac{1}{3}+\frac{1}{1}+\frac{1}{3.8}\right) = \frac{0.45}{0.45+0.33+1.0+0.26} = \frac{0.45}{2.04} = 0.22$$

$$W_{c3} = \frac{1}{3}/\left(\frac{1}{3}+\frac{1}{4}+\frac{1}{1}+\frac{1}{4}\right) = \frac{0.33}{0.33+0.25+1.0+0.25} = = \frac{0.33}{1.83} = 0.18$$

Observe that the addition is done column wise for each criterion.in Table 3.

For criterion I,

$$w_{I1} = \frac{1}{2}/\left(\frac{1}{2}+\frac{1}{2}+\frac{1}{1}+\frac{1}{3}\right) = \frac{0..5}{0.5+0.5+1.0+0.33} = \frac{0.5}{2.33} = 0.21$$

$$w_{I2} = \frac{1}{3}/\left(\frac{1}{2.2}+\frac{1}{3}+\frac{1}{1}+\frac{1}{3.8}\right) = \frac{0.33}{0.45+0.33+1.0+0.26} = \frac{0.33}{2.04} = 0.16$$

$$w_{I3} = \frac{1}{4}/\left(\frac{1}{3}+\frac{1}{4}+\frac{1}{1}+\frac{1}{4}\right) = \frac{0.25}{0.33+0.25+1.0+0.25} = \frac{0.25}{21.83} = 0.14$$

The complete computations are depicted in Table 4

Table 4: Normalized Aggregated Fuzzy Importance Weights for DOS Attack Type Source: [28]

Criteria	Wj_1	Wj_2	Wj_3
C	0.21	0.22	0.18
I	0.21	0.16	0.14
A	0.43	0.49	0.54
RC	0.14	0.13	0.14

Step 5: Create an array of directional vector, which is objectives, for each criterion.

Objectives = [maximum, maximum, maximum, minimum]

Step 6: Generate Decision Matrix for DOS Attack Type

Decision matrix is generated from opinions of decision makers using linguistic variables, which are converted to crisp values using equivalent triangular fuzzy numbers (TFN). The subjective words or phrases are depicted in Table 5.

Table 5: Linguistic Variables and Equivalent Fuzzy Numbers Source: [28]

Positive linguistic variables	Negative linguistic variables	Triangular fuzzy numbers (TFN)
Ineffective (I)	Ineffective (I)	(0, 0, 1)
Very Poor (VP)	Very Poor (VP)	(0, 1, 3)
Poor (P)	Poor (P)	(1, 3, 5)
Average (A)	Average (A)	(3, 5, 7)
Good (G)	Bad (B)	(5, 7, 9)
Very Good (VG)	Very Bad (VB)	(7, 9, 10)
Excellent (E)	Noxious (N)	(9, 10, 10)

Table 6 depicts the opinions of DM on the criteria with respect to each response alternative

Table 6: Linguistic variables of decision makers (DMs) for DOS attack type Source: [28]

Alternative Responses	CRITERIA			
	C	I	A	RC
SH	Excellent	Excellent	Ineffective	Noxious
RH	Good	Good	Poor	Very bad
RP	Average	Average	Good	Average
RST	Poor	Poor	Very Good	Poor

Replace the linguistic variables with equivalent TFN values from Table 5

This is depicted in Table 7.

Table 7: Decision Matrix in Terms of TFN for DOS attack type Source: [28]

	C	I	A	RC
SH	(9,10,10)	(9,10,10)	(0,0,1)	(9,10,10)
RH	(5,7,9)	(5,7,9)	(1,3,5)	(7,9,10)
RP	(3,5,7)	(3,5,7)	(5,7,9)	(3,5,7)
RST	(1,3,5)	(1,3,5)	(7,9,10)	(1,3,5)

From Table 7, find the average of each TFN and create a decision matrix, X,as depicted in Table 8 for DOS attacks.

Table 8: Defuzzified Decision Matrix (averaging the TFN) Source: [28]

Response Alternatives	CRITERIA			
	C	I	A	RC
SH	9.67	9.67	0.33	9.67
RH	7.00	7.00	3.00	8.67
RP	5.00	5.00	7.00	5.00
RST	3.00	3.00	8.67	3.00

For instance, Table 8 is generated as follows, for response alternative SH in Table 7:

$$SH_{11} = (9 + 10 + 10)/3 = \frac{29}{3} = 9.67$$

$$SH_{12} = (9 + 10 + 10)/3 = \frac{29}{3} = 9.67$$

$$SH_{13} = (0 + 0 + 1)/3 = \frac{1}{3} = 0.33$$

$$SH_{14} = (9 + 10 + 10)/3 = \frac{29}{3} = 9.67$$

$$RH_{21} = (5 + 7 + 9)/3 = \frac{21}{3} = 7.00, \text{ etc.}$$

Do the same for other alternative responses

Step 8: Key in the matrix in a DataFrame (df) consisting of criteria and response alternatives,depicted in Table 8, averaged weights w, and objectives in Julia/REPL snippet, then run the program.

4.0 RESULTS

For DOS attack type, reset connection (RST) is selected and used to counter attack in real time and at minimum cost. A screenshot of Julia/REPL result and hyper parameters of the snippet is depicted in Figure 2.

```
In [23]: using JMcDM
         df1 = DataFrame(
         C = [9.67, 7.00, 5.00, 3.00],
         I = [9.67, 7.00, 5.00, 3.00],
         A = [0.33, 3.00, 7.00, 8.67],
         RC = [9.67, 8.67, 5.00, 3.00]);
         weights = [0.20, 0.17, 0.49, 0.14];
         objectives = [max, max, max, min];
         result = electre(df1, weights, objectives);
         result.bestIndex

Out[23]: (4, 1)

In [24]: objectives

Out[24]: 4-element Vector{Function}:
          max (generic function with 27 methods)
          max (generic function with 27 methods)
          max (generic function with 27 methods)
          min (generic function with 27 methods)

In [25]: weights

Out[25]: 4-element Vector{Float64}:
          0.2
          0.17
          0.49
          0.14

In [26]: df1

Out[26]: 4 rows × 4 columns

          |   | C       | I       | A       | RC      |
          |   | Float64 | Float64 | Float64 | Float64 |
          | 1 | 9.67    | 9.67    | 0.33    | 9.67    |
          | 2 | 7.0     | 7.0     | 3.0     | 8.67    |
          | 3 | 5.0     | 5.0     | 7.0     | 5.0     |
          | 4 | 3.0     | 3.0     | 8.67    | 3.0     |
```

Figure 2: Julia /REPL Prioritization of Optimum Response for DOS. Source: [28]

From Figure 2, the code cell snippet is displayed as In[23] and Out[23], where In[ ] is input vector (cell) through which data is sent to Julia/REPL kernel, and Out[ ] is output vector, where the result of computation from Julia/REPL kernel is displayed respectively. The number inside the square braces is auto filled, and represents the kernel's order of execution. The input and output cells of the same operation/result carry the same number. The DataFrame (df1) represents the decision matrix. Other parameters in the In[23] cell include weights, objectives, and electre(df1, weights, objectives), which is assigned to a variable called result. The last command in the code snippet is result.bestIndex. The result is displayed in Out[23] cell, with 4 representing Reset Connection (RST) as the optimum response to select at minimum cost. The second number 1 (shutdown host), represents the least preferred response, as it will incur high response cost if selected.

4.1 Accessing the Hyper parameters of the Code Snippet

The essence of accessing the hyper parameters of the code snippet is to offer explanation on their roles. In[24], In[25] and In[26] respectively carry the commands to assess each hyper parameter; the results from the system are displayed in the equivalent outputs, Out[24], Out[25], and Out[26] respectively. From Out[24] in Figure 2, Objectives depict effects of criteria on response alternatives, whether a particular response alternative will be beneficial (maximize effect) or detrimental (minimize effect). For instance, the first three criteria are beneficial to the response action, while response cost (RC) reduces the effect of the response action.

Also, from Out [25] in Figure 2, the weights depict the views of each DM on the criteria with respect to each response alternative. More so, the criteria are not of equal importance [29] [27], as such, they are rated differently by different DMs. The sum of all the weights should be equal to 1. They are of type float with 64 bit word length.

Similarly, from Out[26] in Figure 2, the decision matrix, represented in pandas dataframe (df1), consists of the four rows of response alternatives, and four columns of criteria used to assess the response alternatives. When keyed into the input cell, criteria and response alternatives are transposed. The values are all Float64 data type. Although the rows are numbered, they represent Shutdown host (SH), Reboot Host (RH), Restart Process (RP), and Reset Connection (RST) respectively in DOS attack type.

4.2 Discussion

In this section, a certain company, like Power holding Nigeria, is not comfortable with customer complaints about the billing system (giving estimated bills) and has decided to do something about it. To improve on the billing system of the company, MCDM (MADM) methods are used to solve the problem. Decision makers (DM) proposed seven alternative strategies to choose from. They are depicted in Table 9.

Table 9: Strategies used to improve the billing process of PHCN Company

	ALTERNATIVE STRATEGIES
Strategy #1	Nil solution
Strategy #2	Purchase an off-the-shelf Application
Strategy #3	The company develop an application in-house
Strategy #4	The company developed an application in-house using high technology
Strategy #5	The company buys a commercial software and modified to suit them.
Strategy #6	The company outsources the development of a software to another company
Strategy #7	The outsourced company uses very high technology to develop the software

The company reorganized its subsystems to five and chose five criteria to rate and outrank the strategies. The criteria include:

i. Technology
ii. Time
iii. Durability
iv. Quality
v. Cost.

Table 10 depicts a decision matrix and criteria weights used to rate the strategies.

Table 10: Decision matrix, Criteria Weights and Vectors used to rate and outrank the strategies

Strategic Alternatives	CRITERIA				
	Cost	Time	Quality	Durability	Technology
Strategy #1	Very low (1)	Very low (1)	Very low (1)	Very low (1)	Very low (1)
Strategy #2	Low (3)	Very low (1)	Average (5)	High (7)	Average (4)
Strategy #3	High (7)	High (7)	Average (5)	Average (5)	Low (3)
Strategy #4	Very High (9)	Average (5)	High (7)	High (7)	Average (6)
Strategy #5	Average (5)	Average (5)	Very High (9)	High (7)	Average (5)
Strategy #6	High (7)	Low (3)	High (7)	High (7)	High 97)
Strategy #7	Very High (10)	Very High (9)	Very High (10)	Very High (9)	Very High (9)
Weights	0.108	0.187	0.181	0.165	0.128
Vector	Minimize	Minimize	Maximize	Maximize	Maximize

The values in the Table 10 are quantified using a 10-point scale of linguistic variables. ELECTRE methods are used to solve the same problem and results compared.

4.2.1 ELECTRE 1 Results

ELECTRE 1 results are presented in a matrix format as depicted in Figure 3.

	M_1	M_2	M_3	M_4	M_5	M_6	M_7
M_1	-	0	1	1	0	1	1
M_2	1	-	1	1	1	1	1
$M3$	0	0	-	0	0	0	0
M_4	0	0	1	-	0	0	1
M_5	1	0	1	1	-	0	1
M_6	0	0	1	1	1	-	1
M_7	0	0	1	0	0	0	-

Figure 3: Results of ELECTRE 1 presented in a matric format Source:[30]

Where $M_i$represents the strategy I; and M_k represents strategy k

Figure 3 gives a partial preference of alternatives. That is, each row shows whether or not M_i dominates other alternatives; and each column shows whether or not M_i dominated by other alternatives. The rows and columns represent, respectively, net concordance (acceptance) and indifference (discordance) indices in the relationship. The relationship $M_i \rightarrow M_k$ or $M_iSM_k$implies that M_i is accepted in preference to M_k – a concordance relationship. If the relationship is true, then a binary value of 1 is represented and 0 otherwise as shown in Figure 3.
Accordingly, from Figure 3 strategy #2 is selected as the best since it is not dominated by any other alternative. Strategies #1, 5, and 6 are equally selected as the better (next best) options; while strategies #4, 7, and 3 have the lowest subsequent ranks with strategy #3 being the worst hit. The same problem is solved using ELECTRE III, IV and IS methods. The results obtained using these methods is depicted in Figure 4, Figure 5 and Figure 6 respectively.

4.2.2 ELECTRE III Results

Figure 4 depicts the results in box format, as boxes are used to represent the classified results. As stated earlier, from Figure 4, an arrow from alternative Mi to alternative Mk ($M \rightarrow M_k$ or M_iSM_k) indicates that strategy #i dominates strategy #k. Any two alternatives appearing in the same box are indifferent; and any two alternatives that are in disconnected boxes are incomparable. Therefore, from Figure 4, strategy #2 is incomparable to strategies #6 and #6. However, strategy #5 and #6 are indifferent; and strategy #3 is ranked as the least preferred option. It can be seen that the result concerning strategy #3 is comparable to that of ELECTRE 1 result.

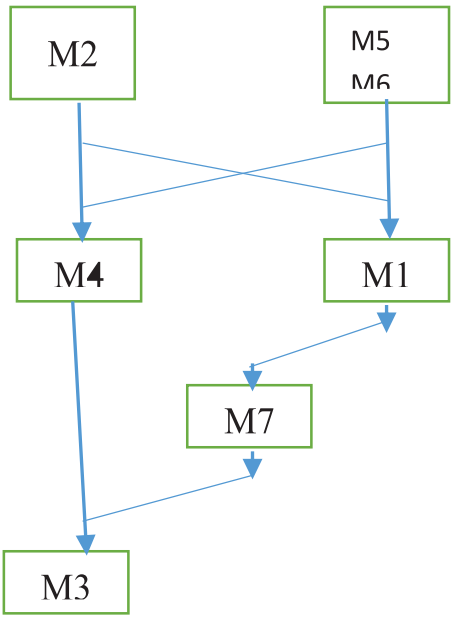

Figure 4: Classification Results using ELECTRE III
Source: [30]

4.2.3 ELECTRE IV Results

Similar to ELECTRE III results, this result is presented in box format as depicted in Figure 5.

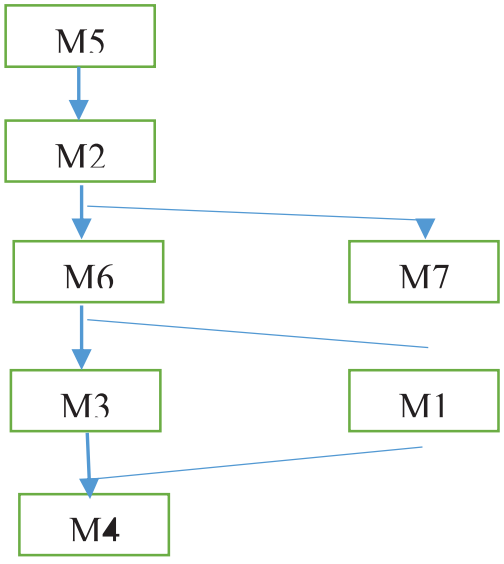

Figure 5: Classification results using ELECTRE IV
Source: [30]

From Figure 5, strategy #5 was ranked the best, followed by strategy #2 and strategy #4 was the least preferred.

4.2.4 ELECTRE IS Results

Figure 6 depicts the results of ELECTRE IS, in which strategy #2 is the most preferred one, followed by strategy #5, while strategy #4 is the least preferred.

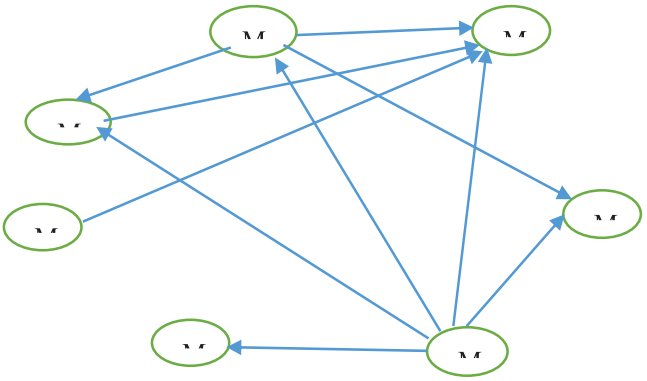

Figure 6: Outranking Results using ELECTRE IS
Source: [30]

From the foregoing, out of the four ELECTRE methods used, strategy #2 was the best choice, followed by strategy #5. Observe that in ELECTRE IV, strategy #5 outranked strategy #2. This is due to the fact that it does not consider weighting functions in its computation. It should also be noted that ELECTRE III, IV and IS yield more incomparable and indifferent alternatives than the other method (ELECTRE 1). This is partly because the three methods use fuzzy pseudo criteria in ranking alternatives, rather than the fixed rate.

4.3 COMPARING WITH OTHER METHODS

The results discussed in this subsection are also based on the case study. Since MCDM operates based on two categorical methods: compensatory and non-compensatory methods. In compensatory method, models are based on multiple attribute utility theory (MAUT), where a single overall (consensus) attribute (criterion) is estimated by aggregating all the criteria and the single criterion is used to rate and outrank the alternative strategies. Simple adaptive weighting (SAW) method and Analytic hierarchy process (AHP) are common examples. Non-compensating MADM models are based on comparison of alternatives using individual criteria. ELECTRE and Maxmin techniques are common examples. The difference between these two categories is that the weights in ELECTRE methods are"coefficient of importance". That is , they do not depend on criteria substitution. Which means that a very bad value on a criterion cannot be substituted by a very good value on another criterion.

SAW gets its overall score for each alternative by summing the criteria values and multiplying the result with their corresponding weights. This method, for the case at hand, gives a ranking order of (2,5, 6,1,7,4,3) with the corresponding score set at (1.404, 0.88, 0.81, -0.078, -0.16, -0.20, -1.22) respectively [30]. Please note that in the SAW aggregation process, cost-like (minimized) criteria are assigned negative values, whereas benefit-like (maximized) values are given positive values. Observe that the top rank strategies in the SAW method are comparable to that of ELECTRE methods results.

TOPSIS method is another MAUT method, and for the current case, it has a ranking order of (2, 6, 5, 1, 4, 7, and 3) with the relative closeness to the ideal solution as (0.70, 0.60, 0.59, 0.55, 0.47, 0.42, 0.36) respectively [30]. The TOPSIS index for strategies 6, 5, and 1 (ie, 0.60, 0.59 and 0.55) are comparable to ELECTRE 1 method, whereas with SAW, only strategies #5 and #6 are comparable.

Similarly, a noncomparable method, Maxmin, was also used in the analysis. For the given case, Maxmin method results had a ranking order of (2, 5, 6, -3, 4, 7, -1). Contrary to TOPSIS, SAW, and ELECTRE methods, Maxmin method took strategy #1 (ie, No change) as the least preferred because it had the lowest value in quality, durability and technology, its lowest cost and time values not-withstanding. Also, strategy #3, which is seen as the worst strategy by TOPSIS, SAW and some ELECTRE methods, is considered as a moderate strategy by Maxmin method.

5.0 CONCLUSION

The results presented in this paper, including those adapted from [30], have important implications in efforts made by the research community to combat the menace of malware on mobile devices, host systems, networks and their users. This paper has successfully used Fuzzy ELECTRE III method to prioritize and select optimum response to the attack in real-time, at minimum cost and devoid of human intervention; and saved the target object from damage.

Secondly, the discussion in section 3 has shown that ELECTRE methods are many and each has its strength and weakness. For instance, ELECTRE 1 and ELECTRE IS are designed for selection problems. While ELECTRE 1 uses true criteria, ELECTRE IS uses pseudo criteria, and allows DMs to choose decision parameters individually instead of fixed values.

ELECTRE II, III, and IV are used for ranking problems. Unlike ELECTRE 1, ELECTRE II defines two outranking relations instead of one: the strong and weak relations. More so, in ELECTRE II, all criteria are true but it requires too many threshold parameters. ELECTRE III is like ELECTRE II, but it uses pseudo criteria and it defines indifference and strict preference threshold [31]. Also, in ELECTRE III method, concordance and discordance thresholds are fuzzy, but in ELECTRE IS, discordance index is binary.

ELECTRE IV does not support the use of weighting functions and assume that all criteria are equal, an opinion not accepted by some researchers [32]. In another development, ELECTRE TRI is used when the criteria are more than the minimum 5 [20].

Above all, ELECTRE III method is the most suitable to use for practical applications because it accounts for:

i. The DMs preference weights
ii. Uncertainty in data for both concordance and discordance indices.
iii. Indifference and incomparable alternative pairs.

5.1 Scientific Implications of Findings

i. Data generated these days are huge and unstructured. They are generated in the cloud,

stored in the cloud (use of servers with huge disk spaces), processed in the cloud, and results transmitted to the device through its IP address. Thus usurping the overhead of mobile devices (low processing power, minimal memory and short battery life). The secured internet, policed by this product, will enable researches with good results, as malware may not even find space to avert controlled environment (sand boxes).

ii The application of this paper will assist the clients in their day to day online transactions, who could be users, companies or government agents.

5.2 Suggestions for Further Studies

i. To implement these developed and tested techniques, it is recommended that they be integrated to Application Programming Interface (API), and uploaded to the cloud. Then the front end (user interface - UI) should be developed using javascript, HTML and software code control (SCC) system. The UI will interact with the classifier (application) at the back end via the API when an application is input through it, and result transmitted through the output cell to the client.

ii. In this paper, four security criteria (attributes) are used to determine response action against DOS/DDOS attack; however, many untapped security criteria abound such as confidence index, date/time of attack, the target object's importance to the company, transmission channels vulnerability, and more. These attributes should be applied in intrusion detection and control measures and compare results.

REFERENCES

[1] R. Karmanje, N. S. Alhassan and M. Alam. (2018). Denial of Service Attacks and their Countermeasures. *5th International Conference on "Computing for Sustainable Global Development", 14th – 16th March 2018*, New Delhi (INDIA).

[2] M. M. Ali and L. TawalbehL (2006). *Intrusion Detection ofDenial of Service (DOS).* New York Institute of Technology (NYIT), Aman's Campus.

[3] H. S. Obaid. (2020). Denial of Service Attacks: Tools and Categories. *International Journal of Engineering Research and Technology (IJERT), 9(03): 631 – 636*

[4] K. M. Elleithy, D. Blagovic, W. Cheng and P. Sideleau (2014). Denial of Service Attack Techniques: Analysis, Implementation and Comparison. *Systematic, Cybernetics and Informatics,* 3(1):66-71

[5] S. Rao and S. Rao (2011). Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis. *This paper is from the SANS Institute Reading Room site.*

[6] M. Bashendy, A.Tantawy and A. Erradi (2023). Intrusion Response Systems for Cyber-Physical Systems: A Comprehensive Survey, 124:102984. https://doi.org/10.1016/j.cose.2022.102984

[7] N. Vafaei, R. A. Ribeiro, and L.M. Camarinha-Matos, (2016). *Normalization Techniques for Multi-Criteria Decision Making: AHP Case Study.* 7th Doctorial Conference on Computing, Electrical and Industrial Systems (DOCEIS), 261 – 269. DOI: 10.1007/978-3-319-31165-4_26

[8] F. Dammak, L. Baccour, A. M. Alimi (2016). Crisp Mult-Criteria Decision Making Methods: State of the Art. *International Journal of Computer Science and Information Security (IJCSIS), 14(8):252-264*

[9] Y. B. Abushark, A. I. Khan, F. Alsolami, A. Agrawal, R. Kumar and R.D. Khan (2022). Cyber Security and Evaluation for Intrusion Detection Systems. *Computers, Materials and Continua, 72(1):1765 – 1783.* DOI: 10.32604/cmc.2022.025604

[10] M. Abliz (2011). *Internet Denial of Service Attacks and Defense Mechanism*, Universi of Pittsburgh, Department of Computer Science, Technical Report, 1-50

[11] L. Barki, A. Shidling, N. Meti, D. Narayan and M. M. Multa (2016)."Detection of Distributed Denial of Service Attacks in Software Defined Networks", 2576 – 2581

[12] V. D. Katkar, and D. S.Bhatia (2013). Experiments on Detection of Denial of Service Attacks Using REPTree..*International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), 713 – 718.*

[13] S. Luo, J. Wu, J. Li, andB. Pei (2015). "A Defined Mechanism for Distributed Denial of Service Attack in Software Defined Networks", 325-329

[14] D. K. Singh and P. Kaushik (2016). Analysis of decision making factors for automated intrusion response system (AIRS): A review. *International Journal of Computer Science and Information Security*, *14*(6), 471.

[15] Z. Inayat, A. Gani, N. B. Anuar, M.K. Khan and S. Anwar (2016). Intrusion Response System: Foundations, design, and Challenges. ELSEVIER *Journal of Network and Computer Applications*, 62, 53 – 74.

[16] S. A. S. A. Mary and G. Suganya (2016). Multi-Criteria Decision Making Using ELECTRE, *Circuits and Systems, 7:1008 - 1020*

[17] Z. Sun and M. Han (2013). Multi-Criteria Decision Making Method Based on Improved ELECTRE III Method. *International Conference on Educational Technology and Management Science* (ICETMS)

[18] J. Qu, X. Meng, X., Jiang, H. You, P. Wang, and C. A. Shoemaker, (2018). Effective Aggregation of Expert Opinions to Inform Environmental

Management: An Integrated Fuzzy Group Decision Making Framework with Application to Cadmium-Contaminated Water Treatment Alternatives Evaluation. *Journal of Cleaner Production, 209(2019)*:834-845. https://doi.org/10.1016/j.jclepro.2018.10.277

[19] N. Vafaei, R.A. Ribeiro, and L. M. Camarinha-Matos (2018). Selection of normalization technique for weighted average multi-criteria decision making. In *Technological Innovation for Resilient Systems: 9th IFIP WG 5.5/SOCOLNET Advanced Doctoral Conference on Computing, Electrical and Industrial Systems, DoCEIS 2018, Costa de Caparica, Portugal, May 2-4, 2018, Proceedings 9*, 43-52.

[20] G. O. Odu (2019). Weighting Methods for Multi-Criteria Decision Making Techniques. *Journal of Applied Science Environmental Management,* 23(8), 1449 -1457. https://dx.doi.org/10.4314/jasen.v23i87

[21] M. C. Wu (2019). Comparative study of ELECTRE methods with intuitionistic fuzzy sets applied on consumer decision making case. *European Journal of Engineering and Technology Research*, *4*(10), 103-110.

[22] V. Mavroeidis and J. Brule (2020). A Non-proprietary Language for the Command and Control of Cyber Defenses-OpenC2. *Computer and Security.* https://doi.org/10.1016/j.cose.2020.101999

[23] H. Karlzen and T. Sommestad. (2023). Automatic Incident Response Solutions: A Review of Proposed Solutions' Input and Output. *In the 18th International Conference onAvailability, Reliability and Security (ARES 2023), August 29 –Sept. 1, 2023,* Benevento, Italy. https://doi.org/10.1145/3600160.3605066

[24] H. A. Kholidy, A. Erradi, S. Abdelwahed,and F. Baiardi (2016). A Risk Mitigation Approach for Autonomous Cloud Intrusion Response System (ACIRS) *Computing.* Doi: 10.1007/s00607-016-0495-8

[25] D. Schlette, M. Caselli, and D. Pernul (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *In IEEE Communications Surveys and Tutorials.*Doi: 10.1109/COMST.2021.3117338

[26] M. Husak and M. Cermak (2022). SoK: Applications and Challenges of Using Recommender Systems in CyberSecurity Incident Handling and Response *In the* 17th *International Conference on Availability, Reliability and Security (*ARES 2022), *August 23 – 26,* Vienna, Austria. https://doi.org/10.1145/3538969.3538981

[27] M. H. Satman, B. F. Yıldırım,and E. Kuruca, (2021). JMcDM: A Julia package for multiple-criteria decision-making tools. *Journal of Open Source Software*, *6*(65), 3430.

[28] S. B. Oyong (2023). *Intelligent Techniques for Intrusion Detection and Control of Malware in Mobile Devices*. PhD Thesis. University of Uyo, Nigeria, 378p

[29] D. K. Singh, and P. Kaushik (2019). Intrusion response prioritization based on fuzzy ELECTRE multiple criteria decision making technique. *Journal of Information Security and Applications*, *48*, 102359.

[30] A.S. Milani, A. Shanian, and C. El-Lahhan (2006). Using Different ELECTRE Methodsin Strategic Planning in the Presence of Human Behavioral Resistance. *Journal of Applied Mathematics and Decision Science,* vol. 2006, pp. 1-9. DOI: 10.1155/JAMDS/2006/10936

[31] Rodrigues, E.S, Martins, F. C., Pereira, V., and Costa Roboredo, M. (2021). An Algorithm to Elicitate ELECTRE II, III and IV Parameters. *Data Technologies and Applications*, *55*(1): 82-96.

[32] M. Akram, K. Zahid and J. C. R. Alcantud (2022). A new outranking method for multicriteria decision making with complex Pythagorean fuzzy information. *Neural Computing and Applications*, *34*(10), 8069-8102.