International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

Decision Support System for Selection and Ranking Security Alternatives

Khaled Abdulkareem Alenezi[1], Imad Fakhri Al-Shaikhli[2], Sufyan Salim Mahmood AlDabbagh[3], Tami Alzabi[4]

[1]Central Agency for Information Technology, Kuwait

[2]Department of Computer Science, International Islamic University of Malaysia, 53100 Jalan GombakKuala Lumpur, Malaysia,

[3]University of Mosul

[4]Project House, Kuwait

Abstract: ***Nowadays, there is wide range of alternatives for hardware and software available in the market; this would create a complex problem for agencies decision makers to select the best tools, software and hardware. When it comes to the information security, alternatives selection is become one of the most important issues. During the network security design, a number of hardware, software, need to be selected in order to make the required design. This design would increase the security and the acceptance of the decision makers. Selection of software and hardware are classified as a daily multi-attribute problem with conflicting criteria. Performance, reliability, usability and other features would play important roles in the selection process. In this paper, we proposed a framework for security tools selection using hybrid of TOPSIS and AHP; AHP is used to calculate the criteria weight while TOPSIS is used with the calculated weight to rank the available security hardware and/or software alternatives. According to the ranking result, the decision maker can select the best alternative with respect to his/her preference***

Keywords: AHP, TOPSIS, SIEM

1. Introduction

Security Information and Event Management (SIEM) automates the incident management (identification and resolution) based on built-in business rules to improve the compliance. The SIEM is used to fulfill the compliance requirements and also to aware from the real-time internal and external threats [1].

The SIEM integrates Security Information Management (SIM) and Security Event Management (SEM). SIEM technology delivers real time analysis of the security alerts that are generated by network hardware and applications. SIM provides long-term storage, reporting and analysis of log data while the SEM deals with real-time monitoring, notifications, security devices, correlation of events, applications, and systems [2, 3]. SIEM provides real-time analysis and correlation by combining SIM and SEM. According to the [3] SIEM technology is usually used for the following three primary purposes; (1) compliance: for log management and create reports for compliance purposes (2) threat management: for the real-time monitoring of user activity, for the access of data, and application activity and incident management (3) A deployment that provides a combination of compliance and threat management capabilities.

To perform functions efficiently and effectively, a SIEM tool requires integration and pre-deployment with numerous security devices and it also needs reporting data from a firewall, an authentication service (LDAP, AAA, etc.), IDS sensor, and vulnerability scan data require integrating during the incident handling phase. Correlations and operational efficiency gains are used for identification phase [4]. SIEM identify security events in real time by the correlation of input data. The input data received by SIEM system is usually in textual format [5].

There are four main functions of SIEM tools: (1) log consolidation: it provides centralized logging to a server, (2) threat correlation: the artificial intelligence used to search through multiple logs and log entries for the identification of the attackers, (3) incident Management: this function is used from identification to the eradication of the threat after its identification. This function includes notifications, automated responses, and response and remediation logging, (4) Reporting: this includes reporting of operational efficiency and effectiveness, and compliance (SOX, HIPPA, FISMA, etc.) [4].

2. Literature Review

According to the researcher's observations, there is very few works done on developing decision making framework comprising: methodology for selecting software packages, criteria for evaluating software packages, technique for evaluating software packages (Jadhav and Sonar, 2009). In addition to that, there is need of system/tool having inbuilt knowledge of software evaluation criteria and evaluation technique which can assist decision makers not only in software selection but also increase efficiency, and brings consistency and transparency in the process of software selection. Although, functional criteria for software selection are not similar for different software packages, other criteria related to the quality, cost and benefits, vendor, hardware and software requirements, opinion of different stakeholders about the software package, and output characteristics of the software package are common and can be used for evaluation of any software package[6].

Evaluation criteria for software define the following framework or software; hybrid knowledge based system approach[7],Quality evaluation of floss projects[8], a fuzzy based decision making procedure[9], integrated AHP-TOPSIS model for software selection under multi-criteria perspective [10], Criteria for ERP selection using an AHP approach [11], FUZZY AHP-TOPSIS two stages method[12].

3. Methodology

The methodology of the proposed Decision support system consists of three main components, namely, alternatives, criteria, and weight. Alternatives represent the solution that the decision makers are trying to pick one of them. Evaluation criteria are the criteria that been used to evaluated the available alternatives, while the weight represent the criteria important according the decision maker preference. With the availability of these three components, we can construct the decision making matrix. According to the literature, one of the most successful and used algorithms in real life selection problems is TOPSIS while AHP is widely used to calculate the weight importance of criteria.

AHP Method

The Analytic Hierarchy Process (AHP) is a multi-criteria decision making approach for dealing with complex decision problems. Saaty[13]in his seminal work first introduced this approach. This is a multi-level structured technique providing a comprehensive framework for evaluating different alternative solutions for a certain problem. By defining objective, criteria, sub criteria and alternatives of a decision problem, AHP provides the alternative solutions. It first decomposes decision problem into different criteria, if these criteria are more complex and then AHP further decompose into sub criteria and so on. After this, each criterion is analysed independently. Once the hierarchy has been constructed, then AHP analytically evaluates its different criteria by comparing them to one another. AHP uses a pair wise comparison technique for evaluating different alternatives. Pair wise comparisons define the relative importance of each alternative with reference to each criterion. From this pair wise comparison AHP extract weights of importance of each criterion. On the basis of each criterion, AHP measures the performance of each alternative. The AHP transforms these assessments into numerical values and then uses these numerical values to elaborate the priorities of each alternative. Final decision is taken on the basis of these priorities. [13, 14]has described the following steps to apply AHP:

1) Construct a hierarchy model which describes alternatives, criteria, and sub criteria for evaluation of these alternatives.
2) Establish pair wise comparison for the criteria and alternatives to extract the decision matrices with a nine point scale.
3) In the third step, pair wise comparison procedure is repeated for each criterion and then priority of alternatives is acquired by accumulating the weights.
4) Make a final decision on the basis of these priorities.

TOPSIS

TOPSIS Method

The TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) is a multi-criteria decision making approach, which was originally developed by Yoon and Hwang in 1981. TOPSIS allocate scores to each alternative on the basis of their geometric distance from positive and negative ideal solutions. And then we choose best alternative, according to this technique, best alternative would be the one that shortest geometric distance to the positive ideal solution and longest geometric distance to the negative ideal solution. In general, TOPSIS method follows the below steps:

1. *Step 1: Construct the normalized decision matrix*

This process tries to transform the various attributes dimensions into non-dimensional attributes; this process allows a comparison across the attributes. The matrix $(x_{ij})_{m*n}$ is then normalized form $(x_{ij})_{m*n}$ to the matrix,$R = (r_{ij})_{m*n}$ using the normalization method:

$$r_{ij} = x_{ij} \Big/ \sqrt{\sum_{i=1}^{m} x_{ij}^2} \quad \dots\dots\dots\dots (1)$$

This process will result a new Matrix R where R is as shown below

$$R = \begin{bmatrix} r_{11} & r_{12} & \dots & r_{1n} \\ r_{21} & r_{22} & \dots & r_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ r_{m1} & r_{m2} & \dots & r_{mn} \end{bmatrix}$$

2. *Step 2: Construct the weighted normalized decision matrix*

In this process, a set of weights $w = w_1, w_2, w_3, \cdots, w_j, \cdots, w_n$, from the decision maker is accommodated to the normalized decision matrix; the resulted matrix can be calculated by multiplying each column from normalized decision matrix (R) with its associated weightw_j. It should be noted that the set of the weights is equal to 1,

$$\sum_{j=1}^{m} w_j = 1 \dots\dots\dots\dots (2)$$

This process will result a new Matrix V where V is as shown below:

$$V = \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{m1} & v_{m2} & \dots & v_{mn} \end{bmatrix} = \begin{bmatrix} w_1 r_{11} & w_2 r_{12} & \dots & w_n r_{1n} \\ w_1 r_{21} & w_2 r_{22} & \dots & w_n r_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ w_1 r_{m1} & w_2 r_{m2} & \dots & w_n r_{mn} \end{bmatrix}$$

3. *Step 3: Determining the ideal and negative ideal solutions*

In this process, two artificial alternatives A^* (the ideal alternative) and A^- (the negative ideal alternative) are defined as:

$$A^* = \left\{ \left(\left(\max_i v_{ij} \,\middle|\, j \in J \right), \left(\min_i v_{ij} \,\middle|\, j \in J^- \right) \middle| i = 1,2, \dots, m \right) \right\} = \{ v_1^*, v_2^*, \dots, v_j^*, \cdots v_n^* \} \dots\dots\dots\dots (3)$$

$$A^- = \left\{ \left(\left(\min_i v_{ij} \,\middle|\, j \in J \right), \left(\max_i v_{ij} \,\middle|\, j \in J^- \right) \middle| i = 1,2, \dots, m \right) \right\}$$

$$= \{v_1^-, v_2^-, \dots, v_j^-, \cdots v_n^-\} \cdots\cdots\cdots (4)$$

It should be noted that J is a subset of$\{i = 1,2, \dots, m\}$, that present the benefit attribute while J^- is the complement set of J, it can be noted asJ^c, which the set of cost attribute

4. Step 4: Separation measurement calculation based on the Euclidean distance

In the process, the separation measurement is done by calculating the distance between each alternative in V and the ideal vector A^* using the Euclidean distant which is given by:

$$S_{i^*} = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^*\right)^2}, \qquad i = (1,2, \cdots m) \ \cdots\cdots\cdots (5)$$

Similarly, the separation measurement for each alternative in V from the negative ideal $A^-$is given by:

$$S_{i^-} = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - v_j^-\right)^2}, \qquad i = (1,2, \cdots m) \ \cdots\cdots\cdots (6)$$

In the end of step 4, two values namely S_{i^*} and S_{i^-} for each alternative has been counted, these two values represent the distance between each alternative and both (the ideal and the negative ideal).

5. Step 5: Closeness to the ideal solution calculation

In the process, the closeness of A_i to the ideal solution $A^*$is defined as:

$$C_{i^*} = S_{i^-}/(S_{i^-} + S_{i^*}), \ 0 < C_{i^*} < 1, \quad i = (1,2, \cdots m) \ \cdots\cdots\cdots (7)$$

It is obvious that, $C_{i^*} = 1$ if and only if $(A_i = A^*)$, similarly, $C_{i^*} = 0$ if and only if $(A_i = A^-)$

6. Step 6: Ranking the alternative according to the closeness to the ideal solution

The set of the alternative $A_i$can now be ranked according to the descending order of C_{i^*}, the highest value the better performance.

4. Result and Discussion

Security information and event management (SIEM) continues to gain market weight. InformationWeek realised a reportfocused on the adoption of SIEM toolsbased on the vendors and the trends.Due to the cost and complexity of SIEM deployments, these purchases aren't to be made easily; in additional to that it requiressignificant pre-instillation inputs.

In terms of overall performance, IBM/Q1 Labs, Novell and HP/Arc Sight earned the top three slots for satisfaction. The rankings were established using 10 criteria, weighted by importance, with Usability, Performance, Feature performance, Reliability, Product performance, Flexibility, Real-time analysis, Automated log collection.

The mentioned report published online in July, 2012 offering wide information on vendor results and performance indicators across the SIEM landscape, which can offer great inputs to the decision makers to select the best solutions among the available alternatives.

Although most of the information about the products is available, it is hard to decision maker to select the best tool according to their weight of criteria. Therefore, SIEM tools selection and benchmarking considered as complex multi attribute problem.

Multi attribute selection (TOPSIS-AHP) is proposed to rank the available SIEM alternatives according to their score. Table 1 represent the score of each tool with respect to each criterion

Table 1: score of the tools with respect to criteria

Solution Name	*Criteria*	*Score*
IBM/Q1 Labs:	Percentage of respondents using the product	14%
	Overall vendor performance (out of 100% possible score)	76%
	Feature performance (out of 100% possible score)	84%
	Top Three Vendor Performance Ratings	
	• Product reliability (1-5 scale)	4
	• Product performance (1-5 scale)	3.9
	• Flexibility in meeting needs (1-5 scale)	3.9
	Top Three Rated Features	
	• Real-time analysis for alerts (1-5 scale)	4.3
	• Automated log collection (1-5 scale)	4.3
	• Support for up to 1,000s of events/sec.(1-5 scale):	4.3
Novell:	Percentage of respondents using the product	11%
	Overall vendor performance (out of 100% possible score)	75%
	Feature performance (out of 100% possible score):	81%
	Top Three Vendor Performance Ratings	
	• Product reliability (1-5 scale)	4
	• Product performance (1-5 scale)	3.9
	• Flexibility in meeting needs (1-5 scale)	3.8
	Top Three Rated Features	
	• Compliance reports (1-5 scale)	4.2
	• Automated log collection (1-5 scale)	4.2
	• Real-time analysis for alerts (1-5 scale)	4.1
HP/ ArcSight:	Percentage of respondents using the product	15%
	Overall vendor performance (out of 100% possible score)	74%
	Feature performance (out of 100% possible score)	77%
	Top Three Vendor Performance Ratings	
	• Product reliability (1-5 scale)	4
	• Product performance (1-5 scale)	3.8
	• Flexibility in meeting needs (1-5 scale)	3.8
	Top Three Rated Features	
	• Real-time analysis for alerts (1-5 scale)	4
	• Automated log collection (1-5 scale)	4
	• Event normalization (1-5 scale)	4

Using different scale might lead to confuse in taking the right decision. As we can see in figure 1, the alternatives are matched at some points while other points the differences are clear. Though, the decision maker cannot use the graph to make the decision

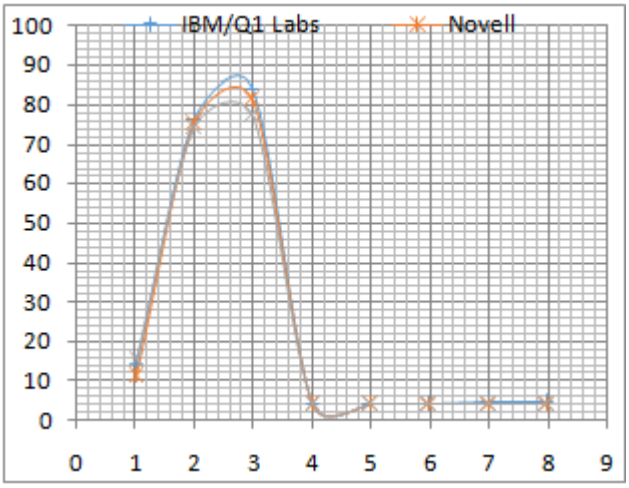

Figure 1: data representation of each alternative

a) ***Non-weighted decision***

Suppose all criteria are treated equally (all the criteria have the same important), the first step of TOPSIS is normalize the data so that, all the criteria will be unit less. This action would make the graph clearer to the decision maker to take his decision even before completing the other operation.

The result of TOPSIS depicted that IBM/Q1 is the best tool followed by HP/ArcSight. Finally Novell is last tool in the list. Table 2 shows the positive ideal, negative ideal and final ranking of each alternative.

Table 2: positive ideal, negative ideal and final ranking of each alternative

Alternative	S*	S⁻	Rank
IBM/Q1 Labs	0.0612	0.1525	0.7136
Novell	0.1761	0.0738	0.2953
HP/ArcSight	0.0992	0.1718	0.6339

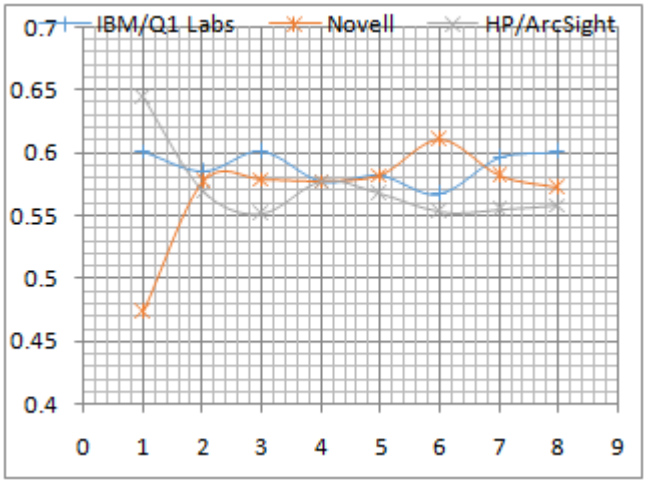

Figure 2: Normalized data of each alternative

b) ***Weighted decision***

Usually, each decision maker/user has some preferences and weights for each criterion. It is very rear when the decision maker treats the entire criterion equally. An expert in information security is asked to make the pairwise comparison between the creations to generate the weight of each criterion. Table 3 is the result of weight counted using AHP multi attribute technique.

Table 3: Criteria weights calculated using AHP

Criteria	Weight counted by AHP
Usability	0.040625
Performance	0.077267
Feature performance	0.174736
Reliability	0.316639
Product performance	0.097633
Flexibility	0.052849
Real-time analysis	0.145645
Automated log collection	0.094605

The result is then recalculated using weighted criteria. The new result of TOPSIS depicted that IBM/Q1 is the best tool followed by Novell. Finally HP/Arc Sight is last tool in the list. Table 2 shows the positive ideal, negative ideal and final ranking of each alternative. See figure 3

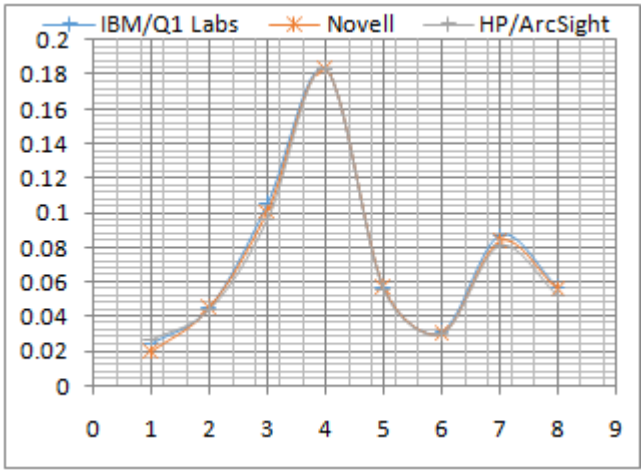

Figure 3: normalized weighted data

The change in the ranking is due to the gain of weight for some features where Novell is performing better than HP/ArcSight, for instance, Feature performanceFeature performance. This rank might be change when the weight is changed. Table 4 shows the positive ideal, negative ideal and final ranking of each alternative.

Table 4: positive ideal, negative ideal and final ranking of each alternative

Alternative	S*	S⁻	Rank
IBM/Q1 Labs	0.0018	0.0127	0.8759
Novell	0.0091	0.0062	0.4052
HP/ArcSight	0.0116	0.007	0.3763

5. Conclusion

Information security is everyday issue, therefore, tools; software to protect the information should be selected carefully. Security tools and software is a complex multi attribute problem. In this research, Multi attribute selection (TOPSIS-AHP) is proposed to rank the available security alternatives. A study case on SIEM software selection is developed.

Two experiments was performed to rank SIEM software, the first experiment aimed to rank the alternative where all the criteria are weighted equally and second experiment has involved the weight of the criteria before the final ranking is calculated. In both cases IBM/Q1 labs software shows high

performance and ranked number 1. The other two software are changing their place between two and three in each experiment. This rank might be change if the weight of criteria is changed. This framework is usable for any security tools and software selection such as selecting IDS, Antiviruses, Firewalls and etc.

6. Acknowledgment

This research is a part of PhD project by Khaled Alenezi at International Islamic University Malaysia. Authors would like to acknowledge The Central Agency for Information Technology at State of Kuwait government, for their time, resource and help in many ways.

References

[1] U. Essays. (2013). *Security Information And Event Management*. Available: http://www.ukessays.com/essays/security/security-information-and-event-management.php?cref=1
[2] S. Dorigo, "Security information and event management," ed: Radboud University Nijmegen. Retrieved from http://www.ru.nl/publish/pages/578936/thesis_sander_dorigo.pdf, 2012.
[3] M. Nicolett and K. M. Kavanagh, "Magic quadrant for security information and event management," *Gartner RAS Core Reasearch Note (May 2009)*, 2011.
[4] D. Swift, "A practical application of SIM/SEM/SIEM automating threat identification," *Paper, SANS Infosec Reading Room, The SANS*, 2006.
[5] E. Novikova and I. Kotenko, "Analytical Visualization Techniques for Security Information and Event Management," in *Parallel, Distributed and Network-Based Processing (PDP), 2013 21st Euromicro International Conference on*, 2013, pp. 519-525.
[6] M. L. M. Kiah, A. Haiqi, B. B. Zaidan, and A. A. Zaidan, "Open source EMR software: Profiling, insights and hands-on analysis," *Computer Methods and Programs in Biomedicine*.
[7] A. S. Jadhav and R. M. Sonar, "Framework for evaluation and selection of the software packages: A hybrid knowledge based system approach," *Journal of Systems and Software*, vol. 84, pp. 1394-1407, 2011.
[8] L. Aversano and M. Tortorella, "Quality evaluation of floss projects: Application to ERP systems," *Information and Software Technology*, vol. 55, pp. 1260-1276, 2013.
[9] H.-Y. Lin, P.-Y. Hsu, and G.-J. Sheen, "A fuzzy-based decision-making procedure for data warehouse system selection," *Expert Systems with Applications*, vol. 32, pp. 939-953, 2007.
[10] S. K. Misra and A. Ray, "Integrated AHP-TOPSIS Model for Software Selection Under Multi-criteria Perspective," in *Driving the Economy through Innovation and Entrepreneurship*, ed: Springer, 2013, pp. 879-890.
[11] J. P. Silva, J. J. Goncalves, J. A. Fernandes, and M. M. Cunha, "Criteria for ERP selection using an AHP approach," in *Information Systems and Technologies (CISTI), 2013 8th Iberian Conference on*, 2013, pp. 1-6.
[12] N. Demirtaş, Ö. N. Alp, U. R. Tuzkaya, and H. Baraçli, "Fuzzy AHP-TOPSIS two stages methodology for ERP software selection: An application in passenger transport sector," in *15th international research/expert conference" trends in the development of machinery and associated technology*, 2011, pp. 12-18.
[13] T. L. Saaty, "Analytic hierarchy process," in *Encyclopedia of Operations Research and Management Science*, ed: Springer, 2013, pp. 52-64.
[14] T. L. Saaty, *What is the analytic hierarchy process?*: Springer, 1988.