Proceedings of the Cyber Secure Nigeria Conference – 2023

A Brief Overview on Applications of Multi-Criteria Decision Making Methods in Web Application Security

[1]Abdulraheem, A.O., [2]Adepoju, S.A., [3]Ojerinde, A.O. & [4]Abisoye, O.A
Department of Computer Science
Federal University of Technology
Minna, Niger State, Nigeria,
E-mails: adebayoakano1@gmail.com, solo.adepoju@futminna.edu.ng, o.ojerinde@futminna.edu.ng,
o.abisoye@futminna.edu.ng;
Phones: [1]+2348162879973; [2]+2348035829748; [3]+2348022226995; [4]+2348060546074

ABSTRACT

Various fields of endeavours have seen the increasing application of multi criteria decision making (MCDM) methods, this includes web application security as new challenges arise in the sector. More MCDM methods are being created and existing methods are combined to give better solutions. This paper performs a review of selected works that are related to the use of MCDM in web application security, examining the methods used, applications and results. Twenty one works were reviewed, with ten papers critically analysed, all published between 2014 and 2023. They were analysed based on MCDM techniques used and security evaluation methods. Results from this review shows that combined MCDM methods were more effective in addition to AHP, TOPSIS and fuzzy-techniques being prevalent. The review carried out in this paper provides a clear insight on various potential applications of MCDM in web application security.

Keywords: Multi Criteria Decision Making (MCDM); Web Application Security; Literature Review

1.. INTRODUCTION

The use of the internet ever since it came into existence has continued to increase across the various sectors of human endeavours. Software generally and web applications are basically designed to satisfy the business goals of organizations and there is a constant pressure on website developers to secure websites.

The prevalence of Internet of Things devices (Ahmad et.al., 2019) and huge data flow in the 4G to 5G evolution, has led to a rise in challenges faced by the security of web and mobile applications and has gained considerable research interest in banking, financial services, e-commerce, healthcare, telecommunications, media, education, as well as government and national defence (Miraz & Ali, 2018). In this respect, there is an increasing need for huge investment in the application security sector. Valued at USD 4 billion in 2019, the sharply growing global market in application security is projected to reach USD 9 billion by 2022, and USD 15.25 billion by 2025 at a compound annual growth rate of 25% (Medeiros et.al, 2016).

According to a report by Lars Lofgren, approximately 54% of the companies universally say they have experienced at least one attack within a year. The report also highlights that just 38% of businesses were prepared to handle these cyber-attacks (Lofgren, 2019). Reports of security failures of web applications for data breaches include important data such as phone number, names and addresses of 5001 students stolen. Few reports cited that web applications such as an entrance examination web application had been attacked for more than 50 times during examinations (Hackett et.al, 2011).

Providing assured information security in any web application is complex and a formidable task while providing effective information security for any web application is a decision-based task. In particular, Multi-criteria decision-making procedures play a very significant and critical role in these types of tasks (Healthcare data breach report, 2019).

2. OVERVIEW OF MULTI CRITERIA DECISION MAKING METHODS (MCDM)

Since the 1960s, Multi Criteria Decision Making (MCDM) has been an active research area and has produced many theoretical and applied articles and books (Roy, 2005). MCDM methods have been designed to present alternatives and classify alternatives in a small number of categories, and/or rank alternatives in a subjective preference order. MCDM is a generic term for all methods that exist for helping in decision making according to their preferences, in cases where there is more than one conflicting criterion (Ho, 2008). Using MCDM can be said to be a way of dealing with complex problems by breaking the problems into smaller pieces. After weighing some considerations and making judgements about smaller components, the pieces are reassembled to present an overall picture to the decision makers. Modern MCDM methods enable decision-makers to deal with all above mentioned types of information (Mardani et.al, 2015).

The MCDM methods cover a wide range of distinct approaches. The MCDM methods can be classified into two categories: the discrete MCDM or discrete multi-attribute decision-making (MADM) and continuous multi-objective decision-making (MODM) methods (Chauhan & Vaish, 2012). Multiple criteria decision-making (MCDM) has grown as a part of operations research, concerned with designing computational and mathematical tools for supporting the subjective evaluation of performance criteria by decision-makers (Zavadskas et.al, 2014).

The goal of the MCDM is to choose the best set of alternatives (solutions) according to the defined criteria. Some of the common examples of MCDM tools include; Analytical Hierarchy Process (AHP), Analytical Network Process (ANP), Technique for Order of Preference with Similarity to an Ideal Solution (TOPSIS), Elimination Et Choix Traduisant la Realite (ELECTRE) and Preference Ranking Organization Methods for Enrichment Evaluation (PROMETHEE).

3. METHODOLOGY

The research methodology used in this study is a literature study of the various decisions making models that have been used in web application security as well as identifying multi criteria decision making techniques which limits the scope of applying decision models in web application security by analysis and comparisons.

Existing related works were studied along with their applications, using resources from various databases particularly; Research Gate, Science Direct (Elsevier), The American journal of information systems, Institute of electrical and electronics engineer IEEE Access, Google scholar and so on. Based on these, decision models applied in web application security were identified across areas such as; network, computing, data and information security. Works that fall within the context of web application security, application security and MCDM were selected in this review.

4. RESULTS AND DISCUSSIONS

4.1 Analysis Based on MCDM Techniques Used In Web Application Security Studies
From the review carried out, AHP, TOPSIS, fuzzy logic, fuzzy-AHP, ANP and SMART are the most prevalent techniques used, combined in variants that are aimed at achieving the goals of the various papers.

Attaallah, et.al. (2023) designed a fuzzy based decision making technique to evaluate security risks in healthcare web applications, using a combination of AHP and TOPSIS. Ansari, et.al. (2022) presents a fuzzy TOPSIS based method to examine the behavioural impact for durable security in the context understudy. Kumar, et.al. (2021) used the Fuzzy Analytic Hierarchy Process (Fuzzy AHP) for evaluating the efficacy of overall sustainable-security in web applications, and its characteristics. In (Agrawal, et.al., 2020), the authors used a combined hybrid approach of fuzzy set theory and analytical hierarchy process (AHP) called fuzzy –AHP, associating with TOPSIS method to evaluate factors of healthcare information security. AHP and TOPSIS were found to be the predominantly used MCDM methods in a survey by D. Macek, et.al.

In an article by (Kumar, et.al., 2020), an incorporated fuzzy technique of AHP and TOPSIS was found to be exceptional for an efficient assessment of alternatives, the authors have taken a fuzzy based hybrid technique of AHP-TOPSIS which helps to gain optimum results, to select attributes with positive impact on the overall usable security of applications, in a bid to recommend a framework for usable security assessment. Efforts by (Agrawal, et.al., 2020), had the authors use the Fuzzy AHP mechanism to determine the sustainability goals and long term impact of symmetrical sustainability.

Alenezi, et.al., used the hybrid method of Fuzzy AHP TOPSIS for the evaluation of security design tactics and its attributes, carrying out an investigation of factors or attributes that contribute to security design tactics. It also analyses the prioritization of these attributes to find out the most relevant attribute among a number of attributes. In a fuzzy based integrated approach of AHP and TOPSIS, by (Agrawal, et.al., 2019), the authors used a technique that involves integrating Fuzzy AHP and Fuzzy TOPSIS for the assessment of sustainable security of web applications. The efficacy of the technique was then tested on a web application. P. K. Gade and M. Osuri evaluated the Analytical Network Process (ANP) and the Simple Multi-Attribute Rating Technique (SMART) in a bid to suggest an appropriate security decision model for mobile application developers.

Table 1: Classification based on MCDM techniques used

Authors	AHP	TOPSIS	ANP	SMART	Fuzzy logic	Fuzzy-AHP	Fuzzy - TOPSIS
(Attaallah, et.al., 2023)	True	True			True		
(Ansari, et.al., 2022)							True
(Kumar, et.al., 2021)						True	
(Agrawal, et.al., 2020)		True				True	
(Macek, et.al., 2020)	True	True					
(Kumar, et.al., 2020)	True	True			True		
(Agrawal, et.al., 2020)	True					True	
(Alenezi, et.al., 2020)		True				True	
Agrawal, et.al., 2019)						True	True
(P. K. Gade and M. Osuri, 2014)			True	True			

4.2 Analysis Based On Evaluation Methods Used In Web Application Security Studies

Attaallah, et.al. used MCDM-based fuzzy methodology to evaluate security attributes and their risk factors. The integrated approach of fuzzy AHP and fuzzy TOPSIS is extremely proficient to scrutinize healthcare web application security from the design tactics viewpoint for gauging HWAs' rankings and fix their security risks. Kumar et.al., applied fuzzy AHP method on ten successive versions of an institutional web application to corroborate the efficiency of this approach.

In Agrawal, et.al., the study analyses the sensitivity of the evaluated results in a section on threat to validity through sensitivity analysis and confusion matrix approach. The study then compares a classical AHP-TOPSIS method with the result of the Fuzzy AHP-TOPSIS method, which showed that the latter can provide a slightly accurate and better result than the former. Macek, et.al., carried out a Systematic Literature Review on the Application of MCDM for Information Security Risk Assessment. The authors in (Kumar, et.al), proposed a methodology that was tested on an institutional website application, to ensure efficacy of the framework. The researchers used classical AHP process to evaluate the accuracy of outcomes gotten from the fuzzy AHP and TOPSIS.

The result obtained through the classical AHP process highly correlates with the results obtained through the Fuzzy process. The most prioritized factor found is the user error protection and the second is security durability. Agrawal, et.al., elaborated on a sustainable security elements hierarchy. The results show that fuzzy AHP proves more efficient than other classical approaches. The paper by Alenezi, et.al., takes a Fuzzy AHP-TOPSIS evaluation model for prioritization of contributing factors of security design tactics and overall security assessment with regards to alternatives. The most prioritized factor was found to be the specialized access in testability, followed by cancel/undo in support of usability. The results validate that for more secure web applications, the developer should use tactics of specialized access tactics in testability.

The sustainable security of web applications is estimated with the assistance of a tree structure and fuzzy AHP – TOPSIS method in (Agrawal, et.al., 2019). The identified sustainability attributes are then verified against identified security attributes. The results showed that assessment of sustainable security helps developers to develop guidelines which further makes web applications design more sustainable and secure. P. K. Gade and M. Osuri carried out studies on decision models that have been used for information Technology (IT) security purpose, as well as application security, followed by analysis and comparison of decision models based on desirable security criteria and alternatives. These analysis and comparisons were made with the aid of mathematical procedures; chiefly matrix equations and matrices. Finally, the most suitable decision model was selected based on the analysis and comparison made.

Table 2: Classification Based On Evaluation Methods Used In Web Application Security Studies

Authors	Evaluation Method
(Attaallah, et.al., 2023)	Evaluation of security attributes and their risk factors
(Ansari, et.al., 2022)	Evaluation of healthcare security threats based on given factors.
(Kumar, et.al., 2021)	Evaluation of sustainable-security
(Agrawal, et.al., 2020)	Sensitivity analysis and confusion matrix approach
(Macek, et.al., 2020)	Systematic Literature Review
(Kumar, et.al., 2020)	proposed framework and hierarchy of usable-security factors
(Agrawal, et.al., 2020)	Sensitivity Analysis
(Alenezi, et.al., 2020)	Evaluation model
Agrawal, et.al., 2019)	Tree structure for estimation
(P. K. Gade and M. Osuri, 2014)	Literature review, analysis and comparisons with the aid of mathematical procedures; chiefly matrix equations and matrices

5. CONCLUSION

A good number of multi criteria decision making methods have been formulated and used over time, based on the selected works that have been reviewed. The prevalence of AHP and TOPSIS methods with fuzzy integration points to their preference and advantage over other methods. Combining multiple methods have also become commonplace, aimed at balancing deficiencies that exist in individual methods. With proper assessment of the strengths and weaknesses of these methods, applying the right combinations could prove to be extremely successful. This paper is capable of pointing users and IT practitioners in the right direction when choosing methods or combinations of methods for securing web applications.

REFERENCES

1. Agrawal, M. Alenezi, R. Kumar and R. A. Khan (2019). 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, Digital Object Identifier 10.1109/ACCESS.2019.2946776.
2. Agrawal, A. K. Pandey, A. Baz, H. Alhakami, W. Alhakami, R. Kumar and R. A. Khan (2020). Evaluating the Security Impact of healthCare web Applications through Fuzzy Based Hybrid Approach of Multi Criteria Decision Making Analysis. IEEE Access, vol. 8, pp. 135770 – 135783, 2020, doi: 10.1109/ACCESS.2020.3010729.
3. Agrawal, M. Alenezi, R. Kumar, R.A. Khan (2020). A Unified Fuzzy-Based Symmetrical Multi-Criteria Decision Making method for Evaluating Sustainable-Security of Web Applications. Symmetry 2020, 12, 448; doi:10.3390/sym12030448. http://www.mdpi.com/journal/symmetry.
4. Ahmad U., Chaudhary J., Ahmad M. and Naz A.A. (3 July, 2019) "Survey on Internet of Things (IoT) for Different Industry Environments", Annals of Emerging Technologies in Computing (AETiC), vol. 3, pp. 28–43. Available: http://aetic.theiaer.org/archive/v3/v3n3/p4.html
5. M.J. Ansari, A. Agrawal, R.A. Khan (2022). Durable Security Blueprints for Web Applications Empowering Digital India Initiative. EAI Endorsed Transactions on Scalable Information Systems 04 2022 – 08 2022, Volume 9, Issue 4
6. Attaallah, K. Al-Sulbi, A. Alasiry, M. Marzougui, S.A. Ansar, A. Agrawal, M.J. Ansari, R.A. Khan (2023). Fuzzy-Based Unified Decision-Making Technique to Evaluate Security Risks: A Healthcare Perspective. Mathematics 2023, 11, 2554. https://doi.org/10.3390/math11112554. https://www.mdpi.com/journal/mathematics.
7. Chauhan, A., & Vaish, R. (2012). Magnetic material selection using multiple attribute decision making approach. Materials & Design, 36, 1–5.
8. D. Macek, I. Magdalenic, N. B. Redep (2020). A Systematic Literature Review on the Application of Multi Criteria Decision Making Methods for Information Security Risk Assessment. International Journal of Safety and Security Engineering, Vol. 10, No. 2, April, 2020, pp. 161-174 Journal homepage: http://iieta.org/journals/ijsse.

9. Healthcare Data Breach Report. Accessed: (Mar. 10, 2020) [Online]. Available: https://www.hipaajournal.com/july-2019-healthcaredata-breach-report/

10. Ho, W. (2008). Integrated analytic hierarchy process and its applications–a literature review. European Journal of Operational Research, 186, 211–228.

11. Internet Uses in the World by Region, (20 April, 2020) [online]. Available at: https://www.internetworldstats.com/stats.htm.

12. L. Lofgren. Website Security Guide. (Dec. 20, 2019). [Online]. Available: https://www.quicksprout.com/website-security/

13. M. Alenezi, A. Agrawal, R. Kumar and R. A. Khan (2020). Evaluating Performance of Web Application Security Through a Fuzzy Based Hybrid Multi-Criteria Decision-Making Approach: Design Tactics Perspective. IEEE Access, Vol 8, pp. 25543 – 25556, 2020, Digital Object Identifier 10.1109/ACCESS.2020.2970784.

14. M. Hackett, B. Johnson, and H. Q. Nguyen. (2011). Testing applications on the web Test planning for internet-based systems. Hoboken, NJ, USA: Wiley. [Online]. Available: https://www.oreilly.com/library/view/testingapplications on/9780471201007/

15. Medeiros I., Neves N. and Correia M. (March 2016) "Detecting and Removing Web Application Vulnerabilities with Static Analysis and Data Mining", IEEE Transactions on Reliability, vol. 65, no. 1, pp. 54–69. Available: https://ieeexplore.ieee.org/document/7206620

16. Microsoft (September 28, 2019). Improve web application security: Threats and countermeasures. Chapter 1: Web application security fundamentals. https://docs.microsoft.com/en-us/previous-versions/msp np/ff648636(v=pandp.10)?redirectedfrom=MSDN

17. Miraz M. H. and Ali M. (1 January, 2018) "Applications of Blockchain Technology beyond Cryptocurrency", Annals of Emerging Technologies in Computing (AETiC), vol. 2, pp. 1–6. Available: http://aetic.theiaer.org/archive/v2/v2n1/p1.html

18. P. K. Gade and M. Osuri (2014). Evaluation of Multi Criteria Decision Making Methods for Potential Use in Application Security. Master Thesis, School of Computing at Blekinge Institute of Technology.

19. Peter S. Excell. (3 July, 2018). "The British Electronics and Computing Industries: Past, Present and Future", Annals of Emerging Technologies in Computing (AETiC), vol. 2, pp. 45–52. Available: http://aetic.theiaer.org/archive/v2/v2n3/p5.html

20. R. Kumar, A.I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, and A. A. Khan (2020). An Integrated Approach of Fuzzy Logic, AHP and TOPSIS for Estimating Usable-Security of Web Applications. IEEE Access, vol 8, pp. 50944 – 50957, 2020, Digital Object Identifier 10.1109/ACCESS.2020.2970245.

21. R. Kumar, A. Baz, H. Alhakami, W. Alhakami, A. Agrawal, R.A. Khan (2021). A hybrid fuzzy rule-based multi-criteria framework for sustainablesecurity assessment of web application. Published by Elsevier B.V. on behalf of Faculty of Engineering, Ain Shams University. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/ https://doi.org/10.1016/j.asej.2021.01.003 2090-4479/

22. Roy, B. (2005). Paradigms and challenges. In J. Figueira, S. Greco, & M. Ehrgott (Eds.), Multiplecriteria decision analysis. State of the art surveys (pp. 3–24). New York, NY: Springer.
23. The Biggest Cyber Threats to Watch Out for in 2019, (20 April, 2020) [online]. Available at: https://www. Securitymagazine.com/articles/89581-the-biggest-cyber-threats-to-watch-out-forin-2019
24. Zavadskas, E. K., Turskis, Z., & Kildienė, S. (2014). State of art surveys of overviews on MCDM/MADM methods. Technological and Economic Development of Economy, 20, 165–179.