Journal of Intelligent Decision Support System (IDSS) 6 (3) (2023), pp. 155-159

Published by: Institute of Computer Science (IOCS)

Journal of Intelligent Decision Support System (IDSS)

Journal homepage: www.idss.iocspublisher.org

Decision making for network security with simple additive weighting method

Andi Zulherry

Data Science, Fakultas Ilmu Komputer Dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara, Medan, Indonesia

Article Info

Article history:

Received Sept 15, 2023
Revised Sept 17, 2023
Accepted Sept 18, 2023

Keywords:

Decision Making;
Network Security;
Security Criteria;
Security Solution Evaluation;
Simple Additive Weighting (SAW).

ABSTRACT

In an increasingly complex digital era, network security has become a crucial aspect in maintaining data integrity, confidentiality, and availability. Effective decision-making methods to select the right network security solution are becoming increasingly important. This article describes the application of the Simple Additive Weighting method as a support tool in the context of decision-making for network security. In the presented case study, three network security solutions are evaluated based on four important criteria: data encryption level, threat detection, access management, and network performance. The SAW method is used to assign weights to each criterion and generate a ranking of solutions based on the final score. The results show that SAW provides a clear and structured view of the network security solution that best fits the user's needs and priorities. The conclusion of this research is that the SAW method can be used as a useful tool in making informed decisions in the context of network security. SAW allows organizations to adjust their priorities by setting the appropriate criteria weights, thus enabling the selection of solutions that are best suited to the unique needs of each organization. In an era of ever-evolving cyber threats, the ability to make effective decisions in the face of security challenges is becoming increasingly important, and the SAW method can be a valuable tool in achieving that goal.

Corresponding Author:

Andi Zulherry,
Data Science, Fakultas Ilmu Komputer Dan Teknologi Informasi,
Universitas Muhammadiyah Sumatera Utara,
Jl. Kapten Muchtar Basri No.3, Glugur Darat II, Kota Medan, Sumatera Utara, 20238, Indonesia.
Email: andizulherry@umsu.ac.id

Introduction

In the turbulent digital age, network security has become a top priority for organizations and individuals (Mahendra et al., 2022; Munaroh et al., 2021; Yohaness, 2020). Increasingly complex information technology has brought great benefits, but it has also opened the door to more sophisticated and diverse cyber threats (Muljani & Ellitan, 2019; Omolara et al., 2022; Prinsloo et al., 2019; Tabrizchi & Kuchaki Rafsanjani, 2020). Network security is at the core of maintaining the integrity, confidentiality and availability of highly valuable data (Bian et al., 2020; Makhdoom et al., 2020). To overcome this challenge, organizations and individuals must be able to make wise decisions in choosing the network security solution that best suits their needs (He et al., 2021; Li & Liu, 2021; Tawalbeh et al., 2020).

In this context, effective decision-making methods are essential. Along with the development of technology, methods such as Simple Additive Weighting have become useful tools in aiding informed

decision making (Alizadeh et al., 2020; Namany et al., 2019; Siksnelyte-Butkiene et al., 2020). This article will describe the application of the SAW method in the context of decision-making for network security (Büyüközkan & Güler, 2020; Rathee, Ahmad, et al., 2020; Rathee, Garg, et al., 2020). In the presented case study, we will evaluate several network security solutions based on predefined criteria and use SAW to provide a clear view of the solution that best fits the needs and priorities. Thus, this article will illustrate how SAW can be used as an effective tool to ensure robust network security amidst growing cyber threats.

The ever-evolving digital age has opened up new opportunities and challenges in the world of network security (Kiradoo, 2023). Companies and organizations have to face various types of cyber threats, ranging from hacking attacks to sophisticated malware attacks (Lallie et al., 2021; Sadiku et al., 2020). Therefore, good decision-making in choosing a network security solution is key to maintaining the continuity of business operations and protecting sensitive data.

The Simple Additive Weighting method is one of the decision-making methods that can provide an objective view in comparing alternatives based on various predetermined criteria. In the context of network security, criteria such as data encryption level, threat detection, access management, and network performance can have different priority levels. By using SAW, organizations can set the weight on each criterion according to its importance, thus enabling more informed decision-making (Indriyanti et al., 2019; Irawan, 2020).

This research will discuss the practical steps in applying SAW for network security decision making. We will also present the results of evaluating network security solutions based on case examples, providing a deeper understanding of how SAW can be used in real situations. With the increasing complexity of cyber threats, the use of SAW methods is becoming increasingly relevant and beneficial to those responsible for maintaining network security. With a proper understanding of this method, it is expected that organizations can improve their security levels and face network security challenges with more confidence.

Method

The problem solving of Decision Support System for Network Security with Simple Additive Weighting method involves several key steps. Here is a step-by-step guide to implementing SAW in a decision support system for network security.

1. Identify Network Security Criteria, is to identify the criteria to be used in the evaluation of network security. Criteria include data encryption level, threat detection, access management, network performance.
2. Determination of Criteria Weights, assigns a relative weight to each criterion. This weight reflects the level of importance or priority of each criterion in the context of network security. These weights are usually expressed in the form of decimal numbers whose total equals 1 (0.2 for encryption level, 0.3 for threat detection, 0.2 for access management, 0.3 for performance).
3. Data Collection and Evaluation of Alternatives, Data required to evaluate different network security alternatives. Alternatives are different security solutions, different network configurations, or different security measures. Then, evaluate each alternative based on predefined criteria.
4. Data Normalization, Data normalization is required if the criteria used have different scales. Normalization is done to convert data into a uniform range so that it can be compared.
5. Calculation of Alternative Scores, Calculate alternative scores for each criterion by multiplying the normalized value of the criteria by the weight of the corresponding criteria. Then, sum up the scores for all criteria for each alternative.
6. Ranking Alternatives, rank alternatives based on the scores calculated in the previous step. The alternative with the highest score will get the top rank and is considered the best choice in the context of network security.
7. Providing Recommendations, The decision support system must be able to provide recommendations to decision makers based on alternative rankings. This recommendation can be accompanied by an analysis that supports the decision.

This process can be the basis for developing a decision support system for network security with

the SAW method. It is important to involve network security experts and integrate their understanding in determining appropriate criteria and weights.

Results and Discussions

Application of the Simple Additive Weighting method for decision making in the context of network security. This study will evaluate three different network security solutions (Solution A, Solution B, and Solution C) based on four predefined security criteria, namely:

Data Encryption Level (Weight = 0.3): A higher data encryption level indicates a better level of security. Threat Detection (Weight = 0.2): The ability to quickly detect cyber threats. Access Management (Weight = 0.2): The effectiveness of access management in preventing unauthorized access. Network Performance (Weight = 0.3): Higher network performance is desirable, but must be balanced with security. Below is a table with the scores and ratings for each solution:

Table 1. Scores and rankings for each solution

Criteria	Solution A	Solution B	Solution C
Encryption Level	90	80	70
Threat Detection	85	70	90
Access Management	70	90	75
Network Performance	80	70	85

In this table, scores are measured on a scale of 0 to 100, where higher values indicate better performance in each criterion.

Calculation of the final score and ranking for each solution:

Solution A Final Score:
Final Score = (0.3*90) + (0.2*85) + (0.2*70) + (0.3*80) = 27 + 17 + 14 + 24 = 82

Solution B Final Score
Final Score = (0.3*80) + (0.2*70) + (0.2*90) + (0.3*70) = 24 + 14 + 18 + 21 = 77

Solution C Final Score
Final Score = (0.3*70) + (0.2*90) + (0.2*75) + (0.3*85) = 21 + 18 + 15 + 25 = 79

Rank the solutions based on their final score: Solution A has a final score of 82. Solution C has a final score of 79. Solution B has a final score of 77. Solution A (Final Score: 82), is the best choice because it has a high level of data encryption, good threat detection capabilities, and reasonably good network performance, while maintaining reasonably effective access management. Solution C (Final Score: 79), has a moderate level of data encryption, good threat detection, and moderately high network performance, but moderately good access management. Solution B (Final Score: 77), has a moderately high level of data encryption, but its threat detection and network performance are lower than Solutions A and C. However, its access management is very effective. However, the access management is very effective

Conclusions

In the previous discussion, Solution A, which received the highest rating in the SAW evaluation, offered a good balance between the predefined security criteria, including data encryption level, threat detection, access management, and network performance. This indicates that Solution A is the best choice in this context. However, it is important to remember that each organization or situation may have different needs and priorities. SAW provides the flexibility to adjust the weight of criteria according to each user's priorities. Solution B, despite getting a lower ranking, stands out in strong access management, which may be a priority for some organizations. The key to using the SAW method is that

it provides a structured framework for evaluating solutions based on relevant criteria. This helps to avoid making decisions based on intuition alone or ad hoc decisions that may be less effective in the face of complex network security threats. In addition, the implementation of SAW also allows organizations to continuously monitor and evaluate their security solutions. By updating criteria weights or replacing existing solutions, organizations can improve their network security levels according to changing threats and business needs. In an era where cyberattacks are increasingly sophisticated and companies rely on their networks for various aspects of business, the use of the SAW method can be an invaluable tool in ensuring security and continuity of operations. With proper customization, this method can be used to make more informed and effective decisions in protecting critical systems and data from cyber threats. For future research development, it is recommended to focus on developing more sophisticated and responsive network security evaluation methods. Research can focus on integrating artificial intelligence (AI) and machine learning to predict and address cyber threats in real-time. Additionally, it is important to explore new ways to measure and assess the effectiveness of security solutions, including methods such as SAW that can be tailored to the unique needs of each organization. Research should also consider the impact of evolving regulations in the cybersecurity world, such as data protection laws and privacy policies, and how evaluation methods can help organizations better comply with those regulations. Finally, research can help identify new trends in cyberattacks and develop innovative security strategies to deal with evolving threats.

References

Alizadeh, R., Soltanisehat, L., Lund, P. D., & Zamanisabzi, H. (2020). Improving renewable energy policy planning and decision-making through a hybrid MCDM method. *Energy Policy*, *137*, 111174.

Bian, T., Xiao, X., Xu, T., Zhao, P., Huang, W., Rong, Y., & Huang, J. (2020). Rumor detection on social media with bi-directional graph convolutional networks. *Proceedings of the AAAI Conference on Artificial Intelligence*, *34*(01), 549–556.

Büyüközkan, G., & Güler, M. (2020). Smart watch evaluation with integrated hesitant fuzzy linguistic SAW-ARAS technique. *Measurement*, *153*, 107353.

He, W., Zhang, Z. J., & Li, W. (2021). Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. *International Journal of Information Management*, *57*, 102287.

Indriyanti, A. D., Prehanto, D. R., Prismana, I., Sujatmiko, B., & Fikandda, J. (2019). Simple Additive Weighting algorithm to aid administrator decision making of the underprivileged scholarship. *Journal of Physics: Conference Series*, *1402*(6), 66070.

Irawan, Y. (2020). Decision support system for employee bonus determination with web-based simple additive weighting (SAW) method in PT. Mayatama Solusindo. *Journal of Applied Engineering and Technological Science (JAETS)*, *2*(1), 7–13.

Kiradoo, G. (2023). Exploring the Opportunities and Challenges for Entrepreneurs in Industry 4.0. *Current Topics on Business, Economics and Finance*, *2*, 180–196.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186.

Mahendra, G. S., Wali, M., Idwan, H., Listartha, I. M. E., Yuliastuti, G. E., Sasongko, D., & Saskara, G. A. J. (2022). Keamanan Komputer'. *Galiono Digdaya*.

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J., & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*, *88*, 101653.

Muljani, N., & Ellitan, L. (2019). The importance of information technology implementation in facing industrial revolution 4.0: Case study of banking industry. *International Journal of Trend in Scientific Research and Development (IJTSRD)*, *4*(1), 409–413.

Munaroh, L., Amrozi, Y., & Nurdian, R. A. (2021). Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001: 2013. *Technomedia Journal*, *5*(2 Februari), 167–181.

Namany, S., Al-Ansari, T., & Govindan, R. (2019). Sustainable energy, water and food nexus systems: A focused review of decision-making tools for efficient resource management and governance. *Journal of Cleaner Production*, *225*, 610–626.

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. *Computers & Security*, *112*, 102494.

Prinsloo, J., Sinha, S., & von Solms, B. (2019). A review of industry 4.0 manufacturing process security risks. *Applied Sciences*, *9*(23), 5105.

Rathee, G., Ahmad, F., Iqbal, R., & Mukherjee, M. (2020). Cognitive automation for smart decision-making in industrial internet of things. *IEEE Transactions on Industrial Informatics*, *17*(3), 2152–2159.

Rathee, G., Garg, S., Kaddoum, G., & Choi, B. J. (2020). Decision-making model for securing IoT devices in smart industries. *IEEE Transactions on Industrial Informatics*, *17*(6), 4270–4278.

Sadiku, M. N. O., Fagbohungbe, O. I., & Musa, S. M. (2020). Artificial intelligence in cyber security. *International Journal of Engineering Research and Advanced Technology*, *6*(05), 1–7.

Siksnelyte-Butkiene, I., Zavadskas, E. K., & Streimikiene, D. (2020). Multi-criteria decision-making (MCDM) for the assessment of renewable energy technologies in a household: A review. *Energies*, *13*(5), 1164.

Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*, *76*(12), 9493–9532.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102.

Yohaness, F. (2020). Analisa Dan Perancangan Keamanan Jaringan Lokal Menggunakan Security Onion Dan Mikrotik. *Journal of Information System and Technology (JOINT)*, *1*(2), 37–61.