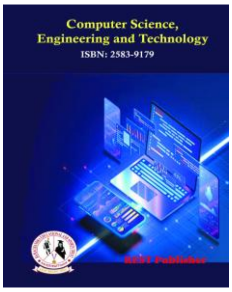
Computer Science, Engineering and Technology

Vol: 1(3), September 2023

REST Publisher; ISSN: 2583-9179 (Online)

Website: https://restpublisher.com/journals/cset/

DOI: https://doi.org/10.46632/cset/1/3/1



The Analysis of Cyber security in Intelligent Transportation Systems Using Multi-Objective Optimization on the Basis of Ratio Analysis (MOORA) Method

Anuj Khanna

Krishna Institute of Technology, Kanpur, India.

Corresponding Author Email: anujk.gkv@gmail.com

Abstract. *Cyber security has become a critical concern in today's interconnected world, with the escalating frequency and sophistication of cyber threats. To effectively protect digital assets and sensitive information, organizations must adopt robust cybersecurity systems. The Multi-Objective Optimization on the basis of Ratio Analysis (MOORA) method has emerged as a promising approach for evaluating and improving cybersecurity systems.This research presents an innovative application of the MOORA method to enhance cybersecurity systems. The MOORA method is a Multi-Criteria Decision Analysis (MCDA) technique that enables decision-makers to rank alternatives based on multiple criteria, ultimately aiding in selecting the most suitable solution. In the context of cybersecurity, various evaluation criteria are considered, such as threat detection accuracy, incident response time, scalability, resource utilization, and cost-effectiveness.Through the integration of the MOORA method, this study offers a systematic and quantitative assessment of cybersecurity systems, addressing the limitations of traditional evaluation techniques that often overlook the complexity of cyber threats. By prioritizing the criteria most relevant to an organization's specific needs and risk profile, decision-makers can make informed choices about investing in the right cybersecurity measures.The practical implementation of the proposed MOORA-based cybersecurity system is demonstrated using real-world data from a diverse set of organizations. The results showcase the effectiveness of the method in guiding cybersecurity decision-making, leading to the identification of optimal solutions that strike the best balance between performance, cost, and resource allocation.The alternatives are A1 is Providing only essential information and continuing to use the service or product, A2 is Giving wrong or partially wrong information as personal data (misinformation), A3 is Closing the account, disposing of, or deactivating the smart device or application and A4 limiting the use of the application, financial institution, or device. The Evaluation parameters are C1 is Low trust in the firm, device, or application, C2 is Poor referrals or negative word-of-mouth from previous users about the service or app, C3 is Negative previous online experience, C4 is Being tech-savvy, experienced, and knowledgeable about recent trends in data privacy and cybersecurity, C5 is The firm or institution not meeting essential privacy and security expectations, such as privacy policies, notices (cookies), seals, etc and C6 is Perceiving that the benefits outweigh the risks of disclosing information.The final result is Limit the use of application, financial institution or device, etc (A4) is got first rank and Provision of strictly necessary Information and continue the use of service or product (A1) is got lowest rank.*

Keywords: *MCDM method, Cybersecurity, Cyber Attacks, Generative Adversarial Networks (GANs), Physical Security.*

1. INTRODUCTION

Governments are increasingly recognizing the social and financial significance of cybersecurity. This recognition is evident in the US, where cyberattacks cost approximately $100 billion annually, and the cybersecurity market is estimated at around $170 billion per year. While the focus has primarily been on technical solutions to address cybersecurity challenges, there is a lack of attention on the ethical issues that arise from it.The ethical importance of cybersecurity is paramount because the technologies involved significantly impact human well-being. Modern human organizations heavily rely on data accessibility and system integrity, which cybersecurity aims to protect. Consequently, ethical dilemmas arise in the field, such as whether to pay hackers for encrypted data access in ransomware situations or to engage in intentional deception through social engineering during penetration testing.Despite acknowledging the ethical concerns in cybersecurity, there is a lack of consensus on the most suitable conceptual framework to approach these issues. The paper under review explores a relatively new and crucial application of Generative Adversarial Networks (GANs) in the cybersecurity domain. GANs have demonstrated remarkable effectiveness in generating high-quality and lifelike images, making them a significant asset in various applications, including those related to cybersecurity. The review primarily covers two essential areas:

1. Research investigations employing Generative Adversarial Networks (GANs) to enhance the effectiveness of Cybersecurity systems.
2. Studies exploring the utilization of GANs in adversarial attacks targeting Cybersecurity systems.

The term "Cybersecurity" is a broad concept that involves the study and development of security protocols to protect digital systems connected over the internet. This review focuses on studies related to securing systems from adversarial attacks using a GAN (Generative Adversarial Network) or being attacked using a GAN. As today's digital systems are accessible over the internet, cybersecurity policies are essential for safeguarding these applications and the data they generate.Such as unauthorized access, viruses, and privacy breaches. These applications play a crucial role in detecting and identifying attacks, thereby safeguarding the underlying network-based systems and preventing potential physical damage or data manipulation. Cyber-attacks can originate internally or externally, and cybersecurity applications employ known signatures or analyze system behaviors to detect and identify these attacks.Among the detection methods, the signature-based approach relies on knowledge-based databases, which necessitate manual updates. Consequently, these cybersecurity applications are unsuitable for real-time applications and systems. The main contributions of this paper are yet to be presented,

1. The aim is to give a concise overview of AI-driven cybersecurity, which caters to the current needs of intelligent cybersecurity services and management. To achieve this, we will initially provide a brief review of existing methods and systems in the cybersecurity domain. This review serves to both motivate our study and establish the significance of the term "AI-driven cybersecurity."
2. We will introduce the concept of security intelligence modeling, which incorporates a range of AI-based techniques. These methods will be explored in the context of our specific objectives.
3. Lastly, we will delve into various research directions that fall within the scope of our study. These research directions are intended to guide and inspire cybersecurity researchers for future investigations in this domain.

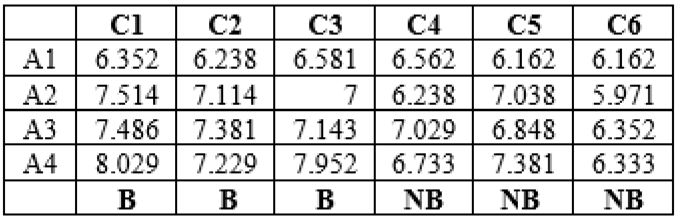
Due to the increasing frequency of cyber incidents, microgrid operators need to be vigilant and develop a clear understanding of cybersecurity risks in microgrid operations. It is essential to implement effective countermeasures. Cyber risk assessment offers a systematic and repeatable method to quantify cybersecurity concerns. The results of this assessment provide insights into the microgrid's cybersecurity posture and enable the implementation of measures to mitigate potential cyber incidents effectively. Continuous assessment is necessary to address the ever-evolving cyber threats facing microgrid operations.In recent years, research on Intrusion Detection Systems (IDS) has advanced. However, they are less effective in identifying novel or zero-day attacks, which are common in ICSs. Anomaly-based IDSs, on the other hand, establish a baseline of accepted network behaviour and can detect new attacks based on deviations from this baseline. Hence, they are better suited for identifying unknown threats.Introducing technologies not originally designed for time-critical areas or from domains unrelated to users' physical security in Intelligent Transportation Systems (ITS) increases their vulnerability to cyberattacks. However, borrowing technologies from various IoT sub-areas is a natural progression. Some innovative technologies have found applications in ITS, while others are yet to be experimented with in this context. The multidimensional nature of ITS requires a diverse range of approaches to achieve cybersecurity objectives.

2. MATERIALS AND METHOD

MOORA is a versatile technique for multi-criteria decision-making, capable of thoroughly evaluating alternatives in the face of diverse and numerous influential factors. It is among the effective multi-objective optimization methods used to address complex decision-making challenges. The main objective of MOORA is to choose the optimal option by taking into account a group of contradictory criteria, both favorable and unfavorable.Compared to other decision-making methods, MOORA offers several advantages for instance, certain Multi-Criteria Decision Making (MCDM) techniques offer benefits like decreased mathematical computations. This approach, alternatively, involves considering multiple factors or criteria simultaneously to make decisions or achieve the best possible outcomes, involves simultaneously optimizing multiple conflicting attributes, all subject to specific constraints.MOORA's applications are wide-ranging and extend to resolving conflicting and intricate problems in the supply chain domain, this involves three crucial aspects: selecting the optimal warehouse locations, choosing the right suppliers, and making decisions regarding product/process design. In such scenarios, optimal decisions are crucial, and MOORA proves beneficial in making appropriate rankings and selections among a variety of available options.Linguistic variables of these attributes are transformed into crisp values to remove any fuzziness. The method involves measuring outcomes for each alternative, and objective outcomes serve as the basis for comparing choices and ultimately arriving at the best selection.In manufacturing environments, MOORA, as a multi-objective optimization technique, has demonstrated its effectiveness in addressing a wide range of intricate decision-making challenges, showcasing its success in numerous scenarios.The MOORA method is utilized to address decision-making challenges related to fleet management issues. It employs a decision matrix to assess alternative options based on various attributes or objectives. MOORA offers advantages such as faster computation and requiring fewer parameters.However, some existing methods are complex and challenging to implement due to their reliance on extensive mathematical knowledge and sensitivity to criteria weights and normalization procedures. To meet these requirements, the paper proposes two algorithms of Multi-Criteria Decision Making (MCDM) that extend the MOORA method to handle uncertain and qualitative information in a Possibility-Fuzzy (PF) environment.The contributions of the paper are twofold: First, it introduces MOORA under PF environments to extend its applicability beyond crisp data. Furthermore, the suggested approach has the capability to address both quantitative and qualitative data, which are frequently encountered in MCDM (Multi-Criteria Decision Making) situations. Multi-objective optimization involves optimizing conflicting objectives simultaneously while considering constraints. Brauers introduced MOORA, a multi-objective optimization technique ideal for addressing intricate decision-making challenges in the manufacturing domain.In the context of seaport planning simulation, the objectives and alternatives were determined to fit the scope of the study. MOORA was chosen despite violating the fourth condition because it met all other criteria, including the seventh condition to some extent.

3. RESULT AND DISCUSSION

TABLE 1. Cyber Security System using MOORA method



	C1	C2	C3	C4	C5	C6
A1	6.352	6.238	6.581	6.562	6.162	6.162
A2	7.514	7.114	7	6.238	7.038	5.971
A3	7.486	7.381	7.143	7.029	6.848	6.352
A4	8.029	7.229	7.952	6.733	7.381	6.333
	B	B	B	NB	NB	NB

Shows the table 1. Cyber Security System. The alternatives are A1 is Providing only essential information and continuing to use the service or product, A2 is Giving wrong or partially wrong information as personal data (misinformation), A3 is Closing the account, disposing of, or deactivating the smart device or application and A4 limiting the use of the application, financial institution, or device. The Evaluation parameters are C1 is Low trust in the firm, device, or application, C2 is Poor referrals or negative word-of-mouth from previous users about the service or app, C3 is Negative previous online experience, C4 is Being tech-savvy, experienced, and knowledgeable about recent trends in data privacy and cybersecurity, C5 is The firm or institution not meeting essential privacy and security expectations, such as privacy policies, notices (cookies), seals, etc and C6 is Perceiving that the benefits outweigh the risks of disclosing information.

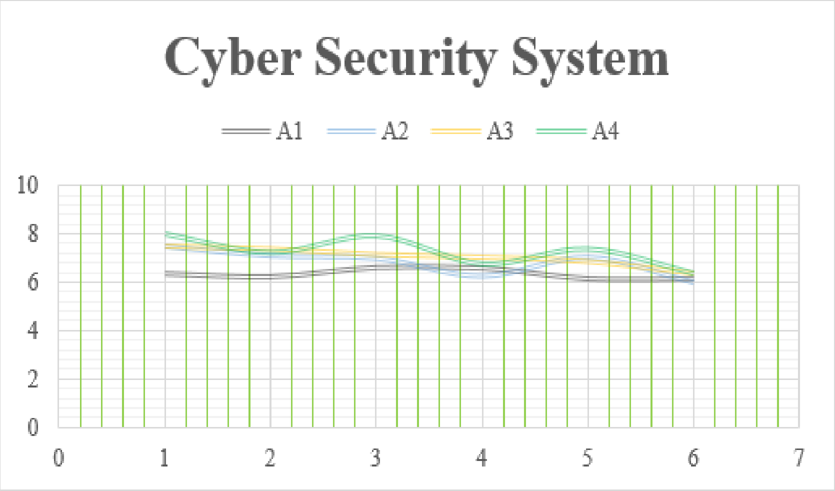


FIGURE 1. Cyber security system using MOORA Method

Shows the figure 1. Cyber Security System. The alternatives are A1 is Providing only essential information and continuing to use the service or product, A2 is Giving wrong or partially wrong information as personal data (misinformation), A3 is Closing the account, disposing of, or deactivating the smart device or application and A4 limiting the use of the application, financial institution, or device. The Evaluation parameters are C1 is Low trust in the firm, device, or application, C2 is Poor referrals or negative word-of-mouth from previous users about the service or app, C3 is Negative previous online experience, C4 is Being tech-savvy, experienced, and knowledgeable about recent trends in data privacy and cybersecurity, C5 is The firm or institution not meeting essential privacy and security expectations, such as privacy policies, notices (cookies), seals, etc and C6 is Perceiving that the benefits outweigh the risks of disclosing information.

TABLE 2. Divide and Sum

	Divide and Sum					
A1	40.3479	38.9126	43.3096	43.0598	37.9702	37.9702
A2	56.4602	50.6090	49.0000	38.9126	49.5334	35.6528
A3	56.0402	54.4792	51.0224	49.4068	46.8951	40.3479
A4	64.4648	52.2584	63.2343	45.3333	54.4792	40.1069
	217.3131	196.2592	206.5663	176.7126	188.8780	154.0779

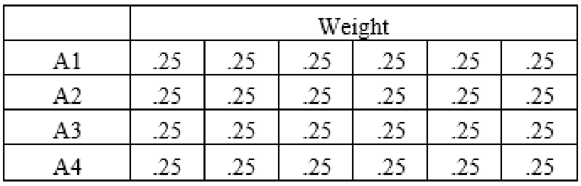
Table 2 illustrates the application of the Divide and Sum matrix formula utilized for this particular dataset.

TABLE 3. Normalized Data

	Normalized Data					
A1	.4309	.4453	.4579	.4936	.4484	.4964
A2	.5097	.5078	.4870	.4693	.5121	.4810
A3	.5078	.5269	.4970	.5288	.4983	.5117
A4	.5447	.5160	.5533	.5065	.5371	.5102

Shows the table 2 normalized data matrix, The A1, A2, A3 and A4 there are alternatives, C1, C2, C3, C4, C5 and C6 there are evaluation parameter. we calculate the weighted normalized values by multiplying each normalized value with its corresponding weight.

TABLE 4. Weight



	Weight					
A1	.25	.25	.25	.25	.25	.25
A2	.25	.25	.25	.25	.25	.25
A3	.25	.25	.25	.25	.25	.25
A4	.25	.25	.25	.25	.25	.25

Shows the table 4. Cyber security system weight is same

TABLE 5. Weighted normalized decision matrix

	Weighted normalized decision matrix					
A1	.1077	.1113	.1145	.1234	.1121	.1241
A2	.1274	.1270	.1218	.1173	.1280	.1203
A3	.1270	.1317	.1242	.1322	.1246	.1279
A4	.1362	.1290	.1383	.1266	.1343	.1275

Shows the table 5 Weighted normalized decision matrixThe alternatives are A1 is Providing only essential information and continuing to use the service or product, A2 is Giving wrong or partially wrong information as personal data (misinformation), A3 is Closing the account, disposing of, or deactivating the smart device or application and A4limiting the use of the application, financial institution, or device. The Evaluation parameters are C1 is Low trust in the firm, device, or application, C2 is Poor referrals or negative word-of-mouth from previous users about the service or app, C3 is Negative previous online experience, C4 is Being tech-savvy, experienced, and knowledgeable about recent trends in data privacy and cybersecurity, C5 is The firm or institution not meeting essential privacy and security expectations, such as privacy policies, notices (cookies), seals, etc and C6 is Perceiving that the benefits outweigh the risks of disclosing information.

TABLE 6. Assessment value and Rank

	Assessment value	Rank
A1	-0.0261	4
A2	0.0105	2
A3	-0.0018	3
A4	0.0150	1

Shows the table 6 assessment values and their corresponding ranks for four items (A1, A2, A3, and A4) in cyber security system using MOORA method. The assessment values represent some numerical evaluations, and the rank indicates their relative positions based on those values. A4 has the highest assessment value (0.0150) and is ranked first. A2 has the second-highest assessment value (0.0105) and is ranked second. A3 has the third-highest assessment value (-0.0018) and is ranked third. A1 has the lowest assessment value (-0.0261) and is ranked fourth.

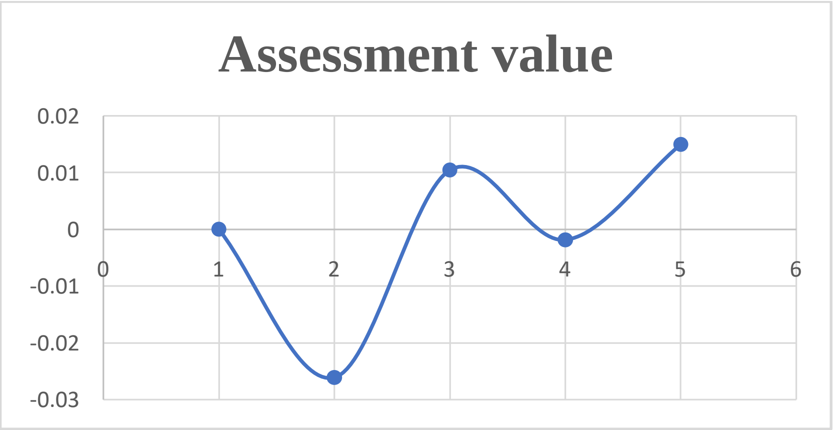


FIGURE 2. Assessment value

Shows the figure 2 assessment value of cyber security system.A4 has the highest assessment value (0.0150),A2 has the second-highest assessment value (0.0105), A3 has the third-highest assessment value (-0.0018), A1 has the lowest assessment value (-0.0261).

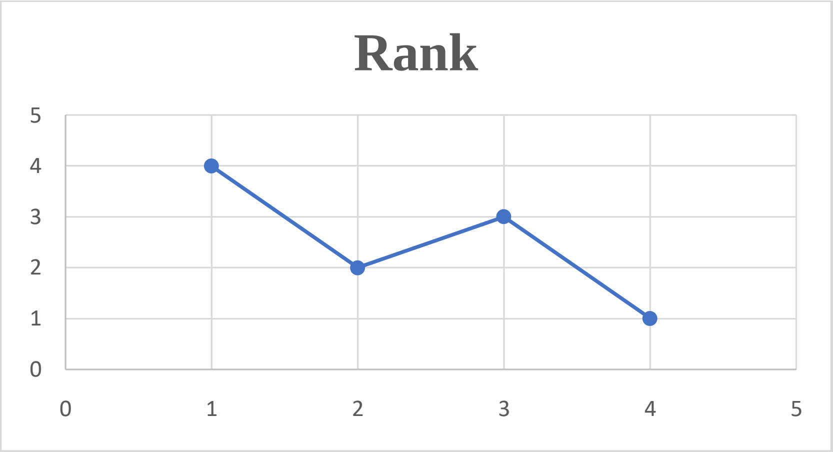


FIGURE 3. Cyber security system final result

Shows the figure 3. Cyber security system final result of ranking. The top-ranked criterion is "A4: Restrict the use of application, financial institution, device, etc." while the lowest-ranked criterion is "A1: Provide only essential information and maintain the usage of the service or product".

4. CONCLUSION

In summary, the implementation of the Cybersecurity System using the method represents a significant advancement in safeguarding our digital landscape. Given the escalating complexity of cyber threats and their potential consequences for individuals, organizations, and nations, a robust cybersecurity system is essential in the digital age. The MOORA method has proven effective in evaluating and prioritizing security measures, simultaneously addressing multiple objectives such as threat detection efficiency, response time, resource allocation, and cost-effectiveness. This approach ensures a well-balanced and optimized cybersecurity strategy.Through the application of the MOORA method, organizations can now identify and deploy the most appropriate combination of security solutions tailored to their specific needs and risk profile. This leads to enhanced resilience in their digital infrastructure, facilitating efficient detection and mitigation of cyber threats. Nevertheless, it is crucial to recognize that cybersecurity is an ongoing process. As technology evolves, so do cyber threats. Regular updates and continuous monitoring of the Cybersecurity System are crucial to remain ahead of malicious actors. Additionally, fostering collaboration between public and private sectors, promoting information sharing, and conducting proactive research are vital in maintaining a strong defense against cyber-attacks.The ultimate outcome is that "Limiting the usage of applications, financial institutions, devices, etc. (A4)" obtained the highest rank, while "Providing strictly necessary information and maintaining the use of service or product (A1)" received the lowest rank.

REFERENCE

[1]. Cruz, Tiago, Luis Rosa, Jorge Proença, LeandrosMaglaras, Matthieu Aubigny, Leonid Lev, Jianmin Jiang, and Paulo Simões. "A cybersecurity detection framework for supervisory control and data acquisition systems." IEEE Transactions on Industrial Informatics 12, no. 6 (2016): 2236-2246.
[2]. Formosa, Paul, Michael Wilson, and Deborah Richards. "A principlist framework for cybersecurity ethics." Computers & Security 109 (2021): 102382.
[3]. Yinka-Banjo, Chika, and Ogban-AsuquoUgot. "A review of generative adversarial networks and its application in cybersecurity." Artificial Intelligence Review 53 (2020): 1721-1736.
[4]. Usman, Muhammad, Mian Ahmad Jan, Xiangjian He, and Jinjun Chen. "A survey on representation learning efforts in cybersecurity domain." ACM Computing Surveys (CSUR) 52, no. 6 (2019): 1-28.
[5]. Sarker, Iqbal H., Md Hasan Furhad, and Raza Nowrozy. "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions." SN Computer Science 2 (2021): 1-18.
[6]. Kim, Jinsu, and Namje Park. "Blockchain-based data-preserving AI learning environment model for AI cybersecurity systems in IoT service environments." Applied Sciences 10, no. 14 (2020): 4718.

[7]. King, Zoe M., Diane S. Henshel, Liberty Flora, Mariana G. Cains, Blaine Hoffman, and Char Sample. "Characterizing and measuring maliciousness for cybersecurity risk assessment." Frontiers in psychology 9 (2018): 39.

[8]. Khorrami, Farshad, Prashanth Krishnamurthy, and Ramesh Karri. "Cybersecurity for control systems: A process-aware perspective." IEEE Design & Test 33, no. 5 (2016): 75-83.

[9]. Bhamare, Deval, MaedeZolanvari, AimanErbad, Raj Jain, Khaled Khan, and Nader Meskin. "Cybersecurity for industrial control systems: A survey." computers & security 89 (2020): 101677.

[10]. Li, Zhiyi, Mohammad Shahidehpour, and Farrokh Aminifar. "Cybersecurity in distributed power systems." Proceedings of the IEEE 105, no. 7 (2017): 1367-1388.

[11]. Asghar, Muhammad Rizwan, Qinwen Hu, and SheraliZeadally. "Cybersecurity in industrial control systems: Issues, technologies, and challenges." Computer Networks 165 (2019): 106946.

[12]. Mecheva, Teodora, and Nikolay Kakanakov. "Cybersecurity in intelligent transportation systems." Computers 9, no. 4 (2020): 83.

[13]. Dabbagh, Rahim, and Samuel Yousefi. "A hybrid decision-making approach based on FCM and MOORA for occupational health and safety risk analysis." Journal of safety research 71 (2019): 111-123.

[14]. Dey, Balaram, BipradasBairagi, Bijan Sarkar, and Subir Sanyal. "A MOORA based fuzzy multi-criteria decision-making approach for supply chain strategy selection." International Journal of Industrial Engineering Computations 3, no. 4 (2012): 649-662.

[15]. Ghoushchi, Saeid Jafarzadeh, Samuel Yousefi, and Mohammad Khazaeili. "An extended FMEA approach based on the Z-MOORA and fuzzy BWM for prioritization of failures." Applied soft computing 81 (2019): 105505.

[16]. Chand, Mahesh, Neha Bhatia, and Rajesh Kumar Singh. "ANP-MOORA-based approach for the analysis of selected issues of green supply chain management." Benchmarking: An International Journal 25, no. 2 (2018): 642-659.

[17]. Rane, Santosh B., Prathamesh RamkrishanaPotdar, and Suraj Rane. "Data-driven fleet management using MOORA: a perspective of risk management." Journal of Modelling in Management 16, no. 1 (2021): 310-338.

[18]. Pérez-Domínguez, Luis, Luis Alberto Rodríguez-Picón, Alejandro Alvarado-Iniesta, David Luviano Cruz, and Zeshui Xu. "MOORA under Pythagorean fuzzy set for multiple criteria decision making." Complexity 2018 (2018).

[19]. Mangalan, Anil Varghese, Sandeep Kuriakose, Hashim Mohamed, and Amitava Ray. "Optimal location of warehouse using weighted MOORA approach." In 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), pp. 662-665. IEEE, 2016.

[20]. Brauers, Willem K., and Edmundas K. Zavadskas. "Robustness of the multi-objective MOORA method with a test for the facilities sector." Technological and economic development of economy 15, no. 2 (2009): 352-375.

[21]. Ginevicius, Romualdas, Willem Karel M. Brauers, and ValentinasPodvezko. "Regional development in Lithuania considering multiple objectives by the MOORA method." Technological and Economic Development of Economy 16, no. 4 (2010): 613-640.

[22]. Gadakh, V. S., Vilas Baburao Shinde, and N. S. Khemnar. "Optimization of welding process parameters using MOORA method." The International Journal of Advanced Manufacturing Technology 69 (2013): 2031-2039.

[23]. Sahu, Anshuman Kumar, Siba Sankar Mahapatra, Suman Chatterjee, and Joji Thomas. "Optimization of surface roughness by MOORA method in EDM by electrode prepared via selective laser sintering process." Materials Today: Proceedings 5, no. 9 (2018): 19019-19026.

[24]. P. M. Bhagwat, M. Ramachandran, Chinnasami Sivaji, P. Sudha, “Weighted Sum Model (WSM) for Evaluating Turbocharged Stratified Injection”, REST Journal on Advances in Mechanical Engineering, 2(2), June (2023):30-37.

[25]. Brauers, Willem Karel M. "Multi-objective seaport planning by MOORA decision making." Annals of Operations Research 206 (2013): 39-58.

[26]. Brauers, Willem Karel M. "Multi-objective contractor’s ranking by applying the MOORA method." Journal of Business Economics and management 4 (2008): 245-255.

[27]. Tanselİç, Yusuf, and SeblaYıldırım. "MOORA-based Taguchi optimisation for improving product or process quality." International Journal of Production Research 51, no. 11 (2013): 3321-3341.