Analyzing Cloud Network Security using PROMETHEE Multicriteria Decision-Making Approach

[1]Shaik Jaffar Hussain, [2]Dr. S. Bhuvaneswari

[1]Research Scholar, Dr. M.G.R Educational and Research Institute University, Chennai.

Email: jaffar.thebest@gmail.com

[2]Associate Professor, Dr. M.G.R Educational and Research Institute University, Chennai.
Email: sbhuvaneswari.899@rediffmail.com

Article Info
Page Number: 01 - 14
Publication Issue:
January-February 2015

Article History
***Article Received**: 14 March 2014*
***Revised**: 27 May 2014*
***Accepted**: 16 October 2014*
***Publication**: 01 January 2015*

Abstract

Cloud computing has gained widespread popularity as a paradigm. Many new services have surfaced within cloud environments, with many people now using cloud networks. Given the coexistence of diverse hosts and network setups within a cloud network, safeguarding each component from potential threats is imperative. Cloud computing represents the next evolutionary step in network computing, as it facilitates providing software and hardware resources and services via the Internet on demand. Unquestionably, security stands out as a major apprehension in cloud computing. Virtualization constitutes a pivotal aspect of cloud computing. This paper focuses on bolstering the security of virtual networks operating within virtualized environments. To address this, we introduce an innovative framework designed to offer monitoring services tailored to expansive and dynamically changing cloud networks. As per prior research, evaluating security poses challenges that encompass assessing the security of the power control process and determining the security level associated with each control phase. To address these intricate challenges, an approach integrating the technique known as "order preference by similarity to ideal solution" (PROMETHEE) within a framework of multiple criteria decision-making (MCDM) is introduced. This method is utilized to conduct a comprehensive security risk assessment for communication networks operating within energy management and control systems (EMCS). The methodology primarily revolves around quantifying security measures for each stage of control. To attribute significance to security vulnerability factors identified through the protection analysis model, a unified MCDM approach incorporating PROMETHEE is put forth. To illustrate this process, a hypothetical scenario involving six communication networks within a power management system is formulated to execute the security evaluation. The outcomes validate the efficacy of this particular approach to security assessment.

Keywords: Cloud network; security risk; multiple criteria decision-making; power control system

INTRODUCTION

"Cloud Computing" refers to IT services such as infrastructure, platforms, or applications that can be accessed and utilized over the Internet. This involves the utilization of various resources, which are measured and subsequently billed based on the extent of their usage. Cloud computing offers a framework that facilitates easy and instant access to a communal reservoir of flexible computing resources, including networks, servers, storage, and applications. These resources can be allocated with limited interaction from the service provider and minimal management efforts. The emerging paradigm of cloud computing addresses the need to manage the rapid proliferation of internet-connected devices and the processing of vast volumes of data. Google, for instance, has introduced the Map Reduce framework to process substantial data volumes using standard hardware resources. The fundamental characteristics of cloud computing can be summarized as follows. Firstly, it encompasses a broad ecosystem comprising many physical hosts and virtual machines (VMs). As an illustration, a study highlighted that Amazon EC2 Cloud operates with almost half a million physical hosts.

Furthermore, each of these hosts caters to multiple virtual machines. Assuming an average of ten virtual machines per host, the Amazon EC2 Cloud manages nearly five million virtual machines. Secondly, configuring a cloud computing environment is intricate. The management of such a network requires careful consideration of the substantial count of diverse networked physical and virtual machines and the diverse array of cloud consumers or tenants who may necessitate greatly varied networking setups. Thirdly, cloud computing demonstrates a high degree of dynamism. An important feature of cloud computing is its capability to provide services on demand. This implies that if a particular service experiences a surge in demand, the cloud computing environment will deploy additional VMs to accommodate the increased demand. Consequently, Virtual machines housed within a physical host can be dynamically triggered, removed, or transferred to other physical hosts. Cloud network security constitutes an all-encompassing structure encompassing methods, technologies, and regulations of utmost importance to protect networks and data in cloud computing environments. As enterprises increasingly adopt cloud services for their IT infrastructure, the assurance of security within these digital realms takes on primary significance. This realm addresses the unique blend of challenges and benefits intrinsic to cloud computing, wherein data and applications are hosted on external servers supervised by third-party service providers. Essential components encompass adhering to the shared responsibility model, which clearly outlines security obligations between cloud providers and clients, as well as the effective management of multi-tenancy to segregate user data. Ensuring data security involves employing encryption for both storage and transmission, establishing strong identity and access management protocols, segmenting networks, and implementing defensive systems such as intrusion detection, prevention mechanisms, and DDoS protection.

Additionally, organizations must maintain compliance with industry regulations, establish robust backup and disaster recovery strategies, and address security challenges linked to containerization and the orchestration of micro services. A comprehensive approach to cloud network security requires active collaboration with cloud providers, ongoing adaptability, and a vigilant security-oriented perspective to combat evolving threats effectively. Selecting the appropriate cloud architecture based on business requirements is of utmost importance. There are three configurations available: public, private, and hybrid. The key to successful cloud implementation lies in identifying the right fit. Failing to choose a suitable cloud model might expose businesses to significant risks. Larger corporations often opt for private clouds due to their substantial data needs, while smaller organizations utilize public clouds. Meanwhile, some companies adopt a balanced approach by selecting hybrid clouds. Cloud network security is an intricate and ever-evolving domain that necessitates a blend of technological solutions, best practices, and a strong security-oriented perspective. Effective management requires close collaboration with cloud providers and proactively adapting security strategies to address emerging threats and vulnerabilities.

1. CLOUD NETWORK SECURITY

In a communication network, several critical factors contribute to its efficient and secure functioning. The Communication Protocol serves as a set of guidelines that govern how individuals exchange information using various physical changes. This protocol outlines communication procedures, syntax, semantics, synchronization, and error recovery mechanisms. Node Security is essential for wireless sensor networks (WSNs), comprised of sensor nodes linked through radio connections, aiming to maintain their uncompromised functionality despite potential security threats. Network monitoring entails the supervision and administration of computer networks, involving responsibilities such as identifying faults, enhancing processes, deploying, and upholding service quality. Cryptography is crucial in ensuring communications and information security by utilizing codes to restrict access solely to authorized entities. Lastly, a Security Policy offers a comprehensive framework detailing access restrictions, policy implementation, and fundamental infrastructure, which is crucial for maintaining a secure and regulated enterprise network environment. Integrating cloud-based systems, facilitated by significant automation, has paved the way for the immediate monitoring of energy-consuming equipment like HVAC systems. This development is anticipated to propel the expansion of the U.S. The Energy Management Systems (EMS) industry is poised for growth over the next eight years. EMS solutions are pivotal in supervising, optimizing, and conserving energy across various end-user sectors, from residential and industrial to manufacturing. These sectors encompass power and energy, telecommunications, information technology, production, retail, business enterprises, and healthcare. The United States witnesses dynamic shifts in power consumption patterns and the potential for improved efficiency within these industries. These factors contribute to an upsurge in product demand during the projected period.

Moreover, the focus on reducing carbon footprints and utilizing waste heat in operations is projected to stimulate the demand for economical and advanced components within Energy Management Systems (EMS) in the years ahead. The United States is witnessing increased research and development endeavors to commercialize exceptionally efficient technologies, thus generating substantial opportunities for industry participants. However, in the realm of cyber security, the Energy Management and Control Systems (EMCS) sector remains notably deficient. Utilizing readily accessible networking technologies has created a range of contemporary and intricate control systems. Despite improvements in understanding these systems from a cyber security perspective, they still necessitate concerted efforts and collaboration among numerous stakeholders to guard against malicious actors with harmful intentions effectively. Entities responsible for critical infrastructure must ensure the robust protection of operational technology, irrespective of its age, against potential compromises. Regulatory bodies consistently require robust cyber security measures for all energy management control technologies. Establishing a robust risk management system is imperative for any organization. This study evaluated the security risk associated with Energy Management and Control Systems (EMCS) using the PROMETHEE approach. This approach is recommended for decision-making scenarios where specific details about input criteria might be unclear, yet the criteria hold equal significance. The upcoming sections of the study are organized as follows: Section 2 offers an in-depth literature review that delves into security risk assessment for communication networks within energy management and control systems.

Furthermore, a noteworthy technique in Multiple Criteria Decision-Making (MCDM), specifically PROMETHEE, is introduced to address security risk assessment challenges. In the context of related research, Song et al. conducted a comprehensive review of the characteristics of nuclear power plant control and instrumentation technologies. This review also underscores the essential considerations required when conducting cybersecurity risk assessments aligned with the lifecycle of instrumentation and control devices. The study emphasized vital steps and considerations for conducting cybersecurity risk assessments of instrumentation and control systems throughout different stages, such as system design, element development, and device procurement. These six steps encompassed (1) system characterization and cybersecurity modeling; (2) assessment of resources and impacts; (3) evaluation of threats; (4) assessment of vulnerabilities; (5) establishment of security control architecture. To address security assessment's complexities, Liu et al. [16] introduced attack scenarios combined with a Multiple Criteria Decision-Making (MCDM) approach. The comprehensive security evaluation was partitioned into two distinct sections.

2. PROMETHEE METHOD

Within the spectrum of superior techniques on a global scale, PROMETHEE Techniques stand out prominently. The heightened popularity of these techniques is greatly influenced by the existence of an exceptionally user-friendly software application known as PROMCALC-PROMETHEE computation. This software has significantly contributed to elevating their recognition. Professionals are increasingly adopting PROMCALC to manage situations that encompass multiple criteria. However, it's important to note that not all users understand the underlying implications of the model assumptions inherent in PROMETHEE approaches. In this article, we briefly address the shortcomings associated with various PROMETHEE techniques that users should be mindful of and avoid. The field of manufacturing technologies persists in experiencing gradual yet innovative transformations. The rapid evolution of manufacturing technology necessitates swift responses from manufacturing businesses. Within manufacturing sectors, the selection of appropriate production plans is imperative. Factors such as product designs, production procedures, work piece and tool materials, machinery, and equipment are considered to address the challenges. Presently, many intricate choices are available, making the selection process arduous. To make informed decisions, understanding the prerequisites for environmentally friendly choices, current and future actions being taken, variables influencing the overall production environment, individual selection methodologies, and exploring diverse techniques and approaches is crucial[17-19]. The focus is on developing methodologies primarily aimed at addressing extensive challenges related to manufacturing systems' design, planning, and management. The central objective of this study is to demonstrate and validate the effectiveness of the PROMETHEE technique, especially in scenarios involving flexible criteria that lack precision. To improve the precision of quality specifications, an estimated cost evaluation is integrated into the concept of fuzzy transition degrees.

Furthermore, to ascertain the relative significance of the criteria, the study employs a combination of the Analytical Hierarchy Process (AHP). The subsequent section presents an advanced PROMETHEE approach for prioritization within a manufacturing context. PROMETHEE holds substantial significance as a large-scale methodology that evaluates various options based on criteria in multicriteria decision-making contexts. This approach is notable for incorporating numerous non-binding preferences, which assist in ranking alternatives through judgment. This research paper introduces the application of PROMETHEE to select environmentally conscious suppliers. This is carried out while taking into account uniform preference functions. Comparative results are presented to evaluate the influence of different aspiration levels on the ultimate preference. The core elements of the challenge related to prioritizing green suppliers encompass seven criteria about economic and environmental factors, four suppliers, and five decision-makers. Data were collected through direct engagements with decision-makers, utilizing a five-item Likert scale. Employing a steady preference structure, the PROMETHEE algorithm was applied, and the results emphasize that Supplier A1 stands out as a significantly favored option. The comparative analysis consistently underscores Supplier A1 as the preferred choice, irrespective of variations in preference levels. To accomplish the distinct objectives of this research, data was sourced from the annual reports of diverse private sector cloud network security. In pursuit of the specific goals outlined in this study, information was extracted from the annual reports of individual cloud network security within the private sector. Primary data for the study was collected from cloud network security employees, primarily to employ the PROMETHEE methodology. Within this approach, arbitrary weights for the variables were ascertained. The performance of the cloud network security was subsequently evaluated and ranked using the PROMETHEE methodology. These methodologies offer versatility in addressing various factors and achieving specific objectives. The selection of cloud network security was made following considering the institutions' homogeneity and the number of decision-making units (2001). A total of 5 cloud networks constituted the decision-making bodies for this study. A comprehensive overview of the analytical Multiple Criteria Decision-Making (MCDM) methods employed in this study will be provided [24].

3. RESULT AND DISCUSSION

Table 1. Decision matrix

	Communication Protocol	Node Security	Network Monitoring	Cryptography	Security Policy
CN1	6.143	6.257	6.6	5.971	5.286

CN2	5.4	5.686	5.4	5.571	5.171
CN3	5.343	5.686	5.229	5.514	5.343
CN4	5.686	6.086	6.086	5.857	5.971
CN5	5.971	6.371	6.314	6.143	6.486
Max	6.143	6.371	6.6	6.143	6.486
Min	5.343	5.686	5.229	5.514	5.171
max-Min	0.8	0.685	1.371	0.629	1.315

The provided decision matrix, encompassing Communication Protocol, Node Security, Network Monitoring, Cryptography, and Security Policy factors across scenarios CN1 to CN5, offers a comprehensive assessment of their significance and performance. Each cell's numerical value reflects the evaluation score, signifying a factor's perceived importance or effectiveness within a specific case. The "Max" row showcases the peak scores attained by each factor, underscoring their highest potential impact. Conversely, the "Min" row illustrates the least scores attributed to each factor, indicating their minimum potential influence. Notably, the "max-Min" row calculates the range between maximum and minimum scores, unveiling the extent of performance variations across cases. In essence, this matrix enables a systematic comparison of factors' roles in diverse scenarios, shedding light on consistent contributions and the degree of variability in their impacts.

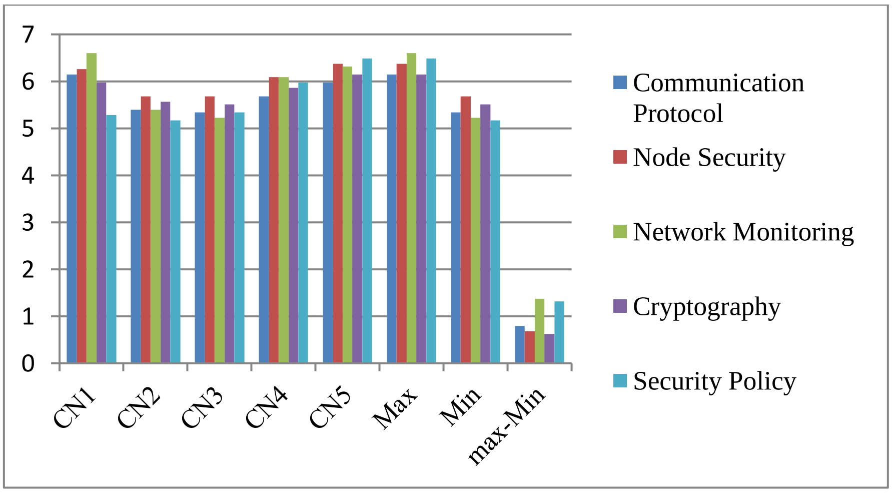

Figure 1. Decision matrix

Figure 1 presents a decision matrix that assesses and quantifies the importance or performance of various factors (Communication Protocol, Node Security, Network Monitoring, Cryptography, and Security Policy) across different cases (CN1 to CN5).

Table 2. Normalized Matrix

	Memory management	Process management	Storage management	protection and security	Software Features
CN1	1	0.8336	1	0.72655	0.0875
CN2	0.07125	0	0.1247	0.09062	0
CN3	0	0	0	0	0.1308
CN4	0.42875	0.5839	0.6251	0.54531	0.6084
CN5	0.785	1	0.7914	1	1

Table 2 presented a normalized matrix featuring factors like Memory Management, Process Management, Storage Management, Protection and Security, and Software Features across cases CN1 to CN5. It provides a balanced perspective on their relative importance or performance. Each cell's value signifies the scaled evaluation of a specific factor within a particular scenario. In CN1, Memory Management, Storage Management, and Protection and Security all attain high normalized scores, highlighting their significance in this context. Conversely, CN2 exhibits notably low Memory Management and Storage Management scores, implying a relatively diminished role in this case. CN3 underscores minimal involvement across all factors except for Storage Management. Notably, CN4 demonstrates a balanced allocation of importance to Memory Management, Process Management, Storage Management, Protection and Security, and Software Features. Finally, CN5 showcases near-maximal normalized scores for Process Management, Storage Management, Protection and Security, and Software Features, emphasizing their critical roles. This normalized matrix enables a more equitable comparison of factor impacts across diverse cases, offering insights into their varying degrees of influence and contribution.

TABLE 3. Pairwise Comparison

	Memory management	**Process management**	**Storage management**	**protection and security**	**Software Features**
D12	0.92875	0.8336	0.8753	0.63593	0.0875
D13	1	0.8336	1	0.72655	-0.043
D14	0.57125	0.2496	0.3749	0.18124	-0.521
D15	0.215	-0.1664	0.2086	-0.2734	-0.913
D21	-0.9288	-0.8336	-0.875	-0.6359	-0.087
D23	0.07125	0	0.1247	0.09062	-0.131
D24	-0.3575	-0.5839	-0.5	-0.4547	-0.608
D25	-0.7138	-1	-0.667	-0.9094	-1
D31	-1	-0.8336	-1	-0.7266	0.0433
D32	-0.0713	0	-0.125	-0.0906	0.1308
D34	-0.4288	-0.5839	-0.625	-0.5453	-0.478
D35	-0.785	-1	-0.791	-1	-0.869
D41	-0.5713	-0.2496	-0.375	-0.1812	0.5209

D42	0.3575	0.5839	0.5004	0.45469	0.6084
D43	0.42875	0.5839	0.6251	0.54531	0.4776
D45	-0.3563	-0.4161	-0.166	-0.4547	-0.392
D51	-0.215	0.1664	-0.209	0.27345	0.9125
D52	0.71375	1	0.6667	0.90938	1
D53	0.785	1	0.7914	1	0.8692
D54	0.35625	0.4161	0.1663	0.45469	0.3916

Table 3 provides a pairwise comparison matrix that offers a detailed analysis of the relative strengths between factors, such as Memory Management, Process Management, Storage Management, Protection and Security, and Software Features, based on various comparisons denoted by the combinations (Dij). Positive values suggest the first factor's superiority over the second, while negative values imply the opposite. A value of 0 signifies an equal influence. For instance, in comparison to D12, Memory Management is moderately stronger than Process Management. Contrastingly, in comparison to D21, Process Management holds less weight than Memory Management. Evaluating across cases, the matrix underscores the nuanced relationships between these factors. In summary, this pairwise comparison matrix aids in understanding the intricate interplay and relative importance of these factors in a structured manner.

TABLE 4. Preference Value

weight aged	0.2336	0.165	0.3355	0.102	0.042	
D12	0.217	0.138	0.2937	0.065	0.004	0.717
D13	0.2336	0.138	0.3355	0.074	0	0.781
D14	0.1334	0.041	0.1258	0.019	0	0.319
D15	0.0502	0	0.07	0	0	0.12
D21	0	0	0	0	0	0
D23	0.0166	0	0.0418	0.009	0	0.068
D24	0	0	0	0	0	0
D25	0	0	0	0	0	0
D31	0	0	0	0	0.002	0.002
D32	0	0	0	0	0.006	0.006
D34	0	0	0	0	0	0
D35	0	0	0	0	0	0
D41	0	0	0	0	0.022	0.022
D42	0.0835	0.096	0.1679	0.046	0.026	0.42
D43	0.1002	0.096	0.2097	0.056	0.02	0.482
D45	0	0	0	0	0	0
D51	0	0.027	0	0.028	0.039	0.094
D52	0.1667	0.165	0.2237	0.093	0.042	0.691
D53	0.1834	0.165	0.2655	0.102	0.037	0.753
D54	0.0832	0.069	0.0558	0.153	0.04	0.4

The presented preference value matrix, incorporating weighted values and comparisons (Dij) between factors, offers insights into the relative prioritization of these factors based on their pairwise comparisons. The "weight aged" row provides the assigned weights to each factor (Memory Management, Process Management, Storage Management, Protection and Security, and Software Features), indicating their significance. Each subsequent row represents a comparison result, denoting the preference values. For instance, in the D12 comparison, Memory Management is preferred over Process Management, with a preference value of 0.717. Similarly, in D13, Memory Management is favored over Process Management, but with a higher preference value of 0.781. Conversely, in D14, Process Management is given a lower preference value of 0.041 than Memory Management. These preference values reflect the degree of favorability or superiority of one factor over another based on the comparison results and the assigned weights. This preference value matrix aids in understanding the hierarchy of these factors according to their relative importance and the results of pairwise comparisons. It helps in making informed decisions by quantifying the preferences among different factors.

TABLE 5. Pairwise comparisons

	CN1	CN2	CN3	CN4	CN5	Sum
CN1	0	0.717	0.781	0.319	0.12	1.937
CN2	0	0	0.068	0	0	0.068
CN3	0.002	0.006	0	0	0	0.008
CN4	0.022	0.42	0.482	0	0	0.924
CN5	0.094	0.691	0.753	0.4	0	1.938
Sum	0.118	1.834	2.084	0.719	0.12	

The provided matrix, Table 5, illustrates the cumulative results of preference values among different cases (CN1 to CN5). Each cell's value represents the sum of preference values, indicating how favorably one case is preferred over another based on the pairwise comparisons and their corresponding preference values from Table 4. The rows and columns correspond to the individual cases and the total sums. For example, the cell in the first row and first column (CN1) has a value of 0, as a case is not compared against itself. The sum of preference values in each row (except the last row) indicates the overall favorability of that particular case over the other cases. The "Sum" row at the bottom provides the totals for each column, showcasing the cumulative favorability of each case over all other cases based on the preference values. Overall, this matrix consolidates the individual preference values into a comprehensive overview, allowing for identifying cases that are more preferred or favored based on the collective results of pairwise comparisons.

TABLE 6. Positive flow, Negative Flow, and Net flow

	positive flow	**Negative Flow**	**Net flow**
CN1	0.3874	0.0236	0.3638
CN2	0.0136	0.3668	-0.3532

CN3	0.0016	0.4168	-0.4152
CN4	0.1848	0.1438	0.041
CN5	0.3876	0.024	0.3636

Table 6 comprehensively assesses the interactions between different cases (CN1 to CN5) through the lenses of positive flow, negative flow, and net flow. Positive flow quantifies the aggregated positive impact each case exerts on the others, offering insight into which cases are generally preferred by their counterparts. Conversely, negative flow encapsulates a case's collective negative impact on others, reflecting scenarios where certain cases are less favored. The net flow, resulting from the subtraction of negative flow from positive flow, offers a holistic evaluation of a case's desirability, considering its positive and negative influences. This combination of flow metrics allows for a nuanced understanding of how cases interact within the context of preferences, facilitating decision-making and prioritization based on the net impact a case has on the overall system. In the context of the table's values, each case (CN1 to CN5) is evaluated in terms of its positive, negative, and net flow, revealing the intricate dynamics of preferences among them. CN1 exhibits a positive flow of 0.3874, indicating its cumulative favorable impact on other cases, coupled with a minor negative flow of 0.0236, resulting in a net flow of 0.3638.

In contrast, CN2 showcases a positive flow of 0.0136 but a notably higher negative flow of 0.3668, yielding a negative net flow of -0.3532. CN3 demonstrates a subtle positive flow of 0.0016 but a relatively more significant negative flow of 0.4168, culminating in a net flow of -0.4152. CN4 boasts a positive flow of 0.1848 and a slightly smaller positive-negative flow of 0.1438, contributing to a net flow of 0.041. Lastly, CN5 features a positive flow of 0.3876 but experiences a minor negative flow of 0.024, yielding a positive net flow of 0.3636. This net flow metric encapsulates the comprehensive impact of both positive and negative influences, providing a holistic gauge of a case's desirability. Cases with higher positive net flows are generally more favored due to their positive impact on others. In comparison, those with higher negative net flows are comparatively less preferred, reflecting their tendency to incur more negative influences.

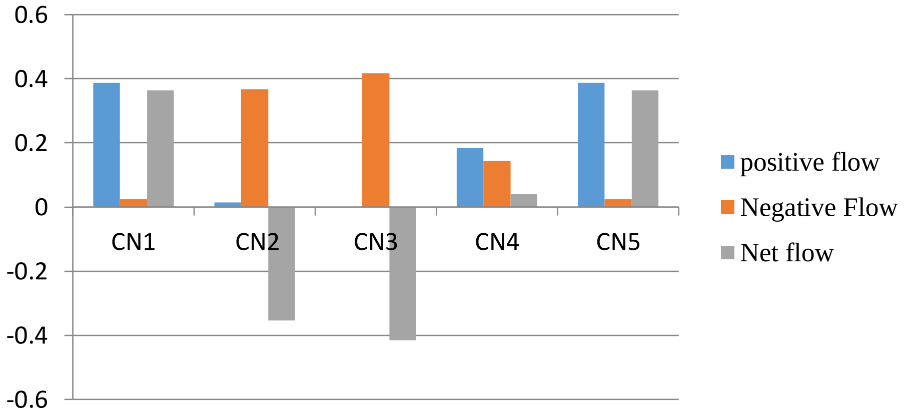

FIGURE 2. Positive flow, Negative Flow, and Net flow

This Figure 2 net flow metric encapsulates the comprehensive impact of both positive and negative influences, providing a holistic gauge of a case's desirability. Cases with higher positive net flows are generally more favored due to their positive impact on others. In comparison, those with higher negative net flows are comparatively less preferred, reflecting their tendency to incur more negative influences.

TABLE 6. Rank

	Rank
Cloud network 1	1
Cloud network 2	4
Cloud network 3	5
Cloud network 4	3
Cloud network 5	2

Table 6 presents a structured hierarchy of ranked positions for distinct cloud network cases (CN1 to CN5), offering insights into their relative desirability based on net flow values. Cloud Network 1 (CN1) secures the top position, reflecting its most favorable status among all cases. In contrast, Cloud Network 3 (CN3) occupies the fifth rank, signifying a relatively less preferred position. Cloud Network 2 (CN2), despite its lower ranking in fourth place, maintains a notable position. Cloud Network 4 (CN4) ranks third, while Cloud Network 5 (CN5) claims the second. These rankings, determined by the net flow values from the prior analysis, emphasize that a lower rank corresponds to greater favorability. Such rankings provide decision-makers with a concise overview of case preferences, aiding in selecting and prioritizing cloud network options based on their cumulative positive and negative impacts.

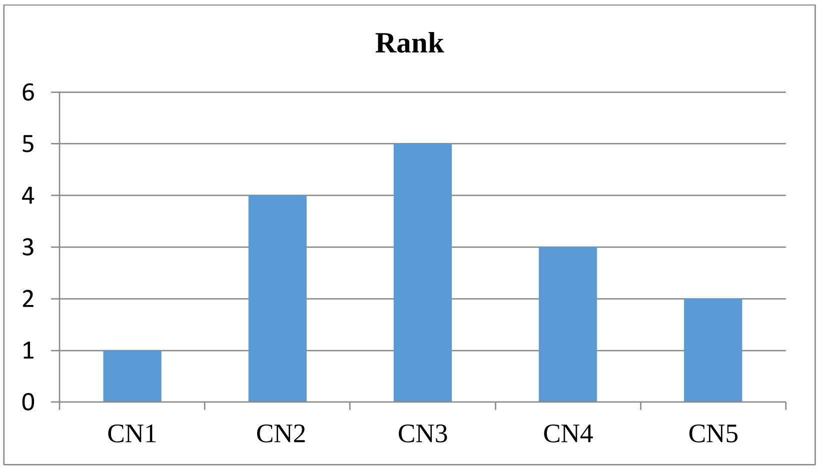

FIGURE 3. Ranking

Figure 3 shows that Cloud Network 1 (CN1) secures the top position, reflecting its most favorable status among all cases. In contrast, Cloud Network 3 (CN3) occupies the fifth rank, signifying a relatively less preferred position. Cloud Network 2 (CN2), despite its lower ranking in fourth place, maintains a notable position. Cloud Network 4 (CN4) ranks third, while Cloud Network 5 (CN5) claims the second.

4. CONCLUSION

In conclusion, the comprehensive analysis presented in this study encompasses various facets of evaluating cloud network cases (CN1 to CN5) within the context of their desirability and performance. Through a multi-faceted approach that includes pairwise comparisons, preference values, and flow metrics, we have gained valuable insights into the relative strengths and weaknesses of different factors and cases. The pairwise comparison matrix allowed us to assess the relative importance of factors, contributing to a systematic understanding of their significance. The derived preference values provided a numerical representation of the favorability of one case over another, aiding in decision-making and prioritization. Moreover, the calculation of positive, negative, and net flow unveiled the intricate interplay of case preferences, offering a holistic view of how cases influence each other positively and negatively. Ranking the cloud network cases based on net flow values highlighted the relative desirability of each case. Cloud Network 1 (CN1) emerged as the most favored, while Cloud Network 3 (CN3) obtained a lower rank due to its comparatively lower desirability. The rankings serve as a valuable tool for decision-makers seeking to optimize their choices in line with the cumulative impact of the analyzed factors. This study has provided valuable insights into assessing and prioritizing cloud network cases, offering a structured methodology that can guide informed decision-making processes. The combination of methodologies allows for a comprehensive evaluation, enhancing our understanding of the complex interactions and dynamics among factors and cases.

REFERENCES

[1]. He, Xiangjian, Thawatchai Chomsiri, Priyadarsi Nanda, and Zhiyuan Tan. "Improving cloud network security using the Tree-Rule firewall." *Future generation computer systems* 30 (2014): 116-126.'

[2]. Shin, Seungwon, and Guofei Gu. "CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)." In *2012 20th IEEE international conference on network protocols (ICNP)*, pp. 1-6. IEEE, 2012.

[3]. Wu, Hanqian, Yi Ding, Chuck Winer, and Li Yao. "Network security for virtual machine in cloud computing." In *5th International conference on computer sciences and convergence information technology*, pp. 18-21. IEEE, 2010.

[4]. Schoo, Peter, Volker Fusenig, Victor Souza, Márcio Melo, Paul Murray, Hervé Debar, Houssem Medhioub, and Djamal Zeghlache. "Challenges for cloud networking security." In *Mobile Networks and Management: Second International ICST Conference, MONAMI 2010, Santander, Spain, September 22-24, 2010, Revised Selected Papers 2*, pp. 298-313. Springer Berlin Heidelberg, 2011.

[5]. Waziri, Victor O., and Joseph Ojeniyi. "Network security in cloud computing with elliptic curve cryptography." (2013).

[6]. Xu, Le, Dijiang Huang, and Wei-Tek Tsai. "Cloud-based virtual laboratory for network security education." *IEEE Transactions on Education* 57, no. 3 (2013): 145-150.

[7]. Sari, Arif. "A review of anomaly detection systems in cloud networks and survey of cloud security measures in cloud storage applications." *Journal*

of Information Security 6, no. 02 (2015): 142.

[8]. Chen, Zhen, Fuye Han, Junwei Cao, Xin Jiang, and Shuo Chen. "Cloud computing-based forensic analysis for collaborative network security management system." *Tsinghua science and technology* 18, no. 1 (2013): 40-50.

[9]. Chen, Zhen, Wenyu Dong, Hang Li, Peng Zhang, Xinming Chen, and Junwei Cao. "Collaborative network security in multi-tenant data center for cloud computing." *Tsinghua Science and Technology* 19, no. 1 (2014): 82-94.

[10]. Huang, Weili, and Jian Yang. "New network security based on cloud computing." In *2010 second international workshop on education technology and computer science*, vol. 3, pp. 604-609. IEEE, 2010.

[11]. Agarwal, Ashish, and Aparna Agarwal. "The security risks associated with cloud computing." *International Journal of Computer Applications in Engineering Sciences* 1, no. Special Issue on (2011): 257-259.

[12]. Inukollu, Venkata Narasimha, Sailaja Arsi, and Srinivasa Rao Ravuri. "Security issues associated with big data in cloud computing." *International Journal of Network Security & Its Applications* 6, no. 3 (2014): 45.

[13]. Seeber, Sebastian, and Gabi Dreo Rodosek. "Improving network security through SDN in cloud scenarios." In *10th International Conference on Network and Service Management (CNSM) and Workshop*, pp. 376-381. IEEE, 2014.

[14]. Basak, Debashis, Rohit Toshniwal, Serge Maskalik, and Allwyn Sequeira. "Virtualizing networking and security in the cloud." *ACM SIGOPS Operating Systems Review* 44, no. 4 (2010): 86-94.

[15]. Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." *arXiv preprint arXiv:1609.01107* (2016).

[16]. Albadvi, Amir, S. Kamal Chaharsooghi, and Akbar Esfahanipour. "Decision making in stock trading: An application of PROMETHEE." *European journal of operational research* 177, no. 2 (2007): 673-683.

[17]. De Keyser, Wim, and Peter Peeters. "A note on the use of PROMETHEE multicriteria methods." *European journal of operational research* 89, no. 3 (1996): 457-461.

[18]. Anand, Gapesh, and Rambabu Kodali. "Selection of lean manufacturing systems using the PROMETHEE." *Journal of modelling in management* (2008).

[19]. Briggs, Th, P. L. Kunsch, and Bertrand Mareschal. "Nuclear waste management: an application of the multicriteria PROMETHEE methods." *European Journal of Operational Research* 44, no. 1 (1990): 1-10.

[20]. Oberschmidt, Julia, Jutta Geldermann, Jens Ludwig, and Meike Schmehl. "Modified PROMETHEE approach for assessing energy technologies." *international Journal of energy sector management* (2010).

[21]. Athawale, Vijay Manikrao, Prasenjit Chatterjee, and Shankar Chakraborty. "Decision making for facility location selection using PROMETHEE II method." *International Journal of Industrial and Systems Engineering 1* 11, no. 1-2 (2012): 16-30.

[22]. Liao, Huchang, and Zeshui Xu. "Multicriteria decision making with intuitionistic fuzzy PROMETHEE." *Journal of Intelligent*

& Fuzzy Systems 27, no. 4 (2014): 1703-1717.

[23]. Halouani, Nesrin, Habib Chabchoub, and J-M. Martel. "PROMETHEE-MD-2T method for project selection." *European Journal of Operational Research* 195, no. 3 (2009): 841-849.

[24]. Chou, Tien-Yin, Wen-Tzu Lin, Chao-Yuan Lin, Wen-Chieh Chou, and Pi-Hui Huang. "Application of the PROMETHEE technique to determine depression outlet location and flow direction in DEM." *Journal of Hydrology* 287, no. 1-4 (2004): 49-61.

[25]. Gupta, Rajesh, Anish Sachdeva, and Arvind Bhardwaj. "Selection of logistic service provider using fuzzy PROMETHEE for a cement industry." *Journal of Manufacturing Technology Management* (2012).

[26]. Van Huylenbroeck, Guido. "The conflict analysis method: bridging the gap between ELECTRE, PROMETHEE and ORESTE." *European Journal of Operational Research* 82, no. 3 (1995): 490-502.

[27]. Turcksin, Laurence, Annalia Bernardini, and Cathy Macharis. "A combined AHP-PROMETHEE approach for selecting the most appropriate policy scenario to stimulate a clean vehicle fleet." *Procedia-Social and Behavioral Sciences* 20 (2011): 954-965