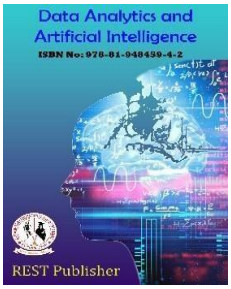
Data Analytics and Artificial Intelligence

Vol: 4(3), 2024

REST Publisher; ISBN: 978-81-948459-4-2

Website: http://restpublisher.com/book-series/daai/

DOI: https://doi.org/10.46632/daai/4/3/5



Ensuring Data Security in Cloud Computing: A VIKOR-Based Analysis

***A. Yashmeen, R. Latha**

St Peters Institute for Higher Education and Research, Chennai, Tamil Nadu, India.

* Corresponding Author Email: Yashmeen92@gmail.com

Abstract: *Introduction: Cloud computing has transformed the IT industry by providing scalable and on-demand access to computing resources and redefining traditional infrastructure approaches. Its virtualized architecture offers flexibility, cost savings, and improved reliability. However, with increasing adoption, security concerns have intensified, making it necessary to address vulnerabilities in data protection, access control, and multi-tenancy. Research significance: This research is important as organizations increasingly adopt cloud-based technologies, and as they thoroughly examine cloud computing security. By addressing issues such as data security vulnerabilities, multi-tenancy challenges, and access control, the study provides valuable insights to secure cloud environments, ensure secure implementation, and support the advancement of this transformative technology. Methology: alternatives: Proximity to Users, Diversity of Services, Availability Zones (AZs), Cost and Performance Considerations, Regulatory Compliance. Evaluation criteria Distance from Consumer, Available Services, Performance Rating, Data Transfer Latency. Result: According to the results, Regulatory Compliance ranked highest, while Proximity to Users ranked lowest.*

Conclusion: According to the VIKOR method approach, regulatory compliance has the highest value for cloud computing security.

Keywords: *Cloud computing, Identity management, Automatic delivery, Application Management, Traditional defense mechanisms, Multi-Criteria Decision Making (MCDM), VIKOR method, Service Level Agreements (SLA).*

1. INTRODUCTION

Numerous cloud computing security issues are the subject of an expanding body of research. Research often focuses on certain areas of cloud security, including vulnerabilities at the platform layer (including virtualization, network, or general software layers), issues with multi-level access and aggregated user data, access control, identity management, and more. According to recent NIST draft research, businesses should take into account a number of security concerns and considerations when preparing to implement a public cloud environment. [1] More effective application management is possible due to the highly virtualized and standardized infrastructures found in cloud computing. Due to its great scalability, programs can be made available to a wider audience. The cloud guarantees a high level of service and is highly reliable and fault-tolerant. It provides flexibility because capital and operating costs for resources arise only when needed. Cloud computing is an on-demand service that automatically provides the necessary processing power. [2] A new information system (IS) architecture called cloud computing, dubbed the computing of the future, is forcing consumers to rethink how they view browsers, operating systems, and client-server architectures. It has freed users from hardware dependencies and reduced client-side requirements and complexity. As cloud computing becomes more popular, concerns are growing about the security risks posed by adopting this new strategy. As the characteristics of this new deployment model differ significantly from traditional systems, the effectiveness and efficiency of conventional security practices are being re-evaluated. [3] Cloud computing is like the early electrical revolution. Similar to how homes, businesses, and cities moved from generating their own electricity to connecting to a large, centralized electrical grid maintained by utilities, cloud computing allows users to access a vast network of resources that are controlled and distributed over the Internet. This shift enables greater accessibility, reliability, and scalability, which also provides significant cost benefits to all its customers. [4] This approach is extended by contemporary edge computing, which, thanks to advances in virtualization, makes it easier to install and run various applications on edge servers. The decentralized nature of this paradigm is different from the security tactics often used in distributed computing. Additionally, since data may travel through multiple decentralized, Internet-connected centers before reaching the cloud, encryption mechanisms must be included. When determining security strategies, device-based edge centers are particularly important. Storing information at the edge makes it possible to shift the responsibility for data security from

Copyright@ REST Publisher

service providers to end users. [5] A network-based technology called cloud computing was developed to share computing resources. By using the Internet, it attempts to hide its complexity from users. The technology and software used in data centers to support web-based applications delivered as services is called cloud computing. Cloud providers disperse computing resources across a network infrastructure using virtualization technologies and self-service features. A physical server hosts multiple virtual machine types that form the basic foundation of cloud environments. [6] Cloud computing combines various technologies, such as web services, virtualization, and multi-tenancy, to make virtualized resources available to users. Web applications are essential to manage and use cloud services delivered over the Internet. Client processes are executed in a virtualized environment using physical resources. By assigning virtual processes from multiple users to the same logically distinct physical servers, a multi-tenant cloud environment is created. While cloud computing offers numerous benefits, there are also disadvantages, and security is paramount. [7] Regardless of the technology used, the most important component of IT security is still data. This also applies to cloud computing, which presents additional security challenges due to its decentralized and multi-tenant architecture. Every cloud service provider (CSP) must implement appropriate security protocols for each phase of the data lifecycle, which includes creation, storage, use, distribution, and destruction. When a service is under increasing pressure, the cloud computing operating system responds by deploying more service instances to meet the increasing processing power demand. [8] A new computing paradigm called cloud computing provides reliable, on-demand access to resources spread across a large geographic area. The information technology (IT) industry has been greatly impacted by the recent emergence of cloud computing, with large companies such as Google, Amazon, and Microsoft offering incredibly stable, reliable, and cost-effective cloud platforms. Meanwhile, organizations are rethinking their business strategies to take advantage of this new paradigm. Despite its growth, cloud computing still faces many challenges. [9] Cloud computing security encompasses all the measures needed to ensure the security of cloud computing environments. Cloud computing security encompasses all aspects of computer security, although many of these issues are not specific to the cloud, such as the potential for attacks regardless of where the data is stored. This includes creating secure designs, mitigating vulnerabilities, protecting against viruses, and placing access controls. However, cloud computing has several unique security features. [10] Many argue that cloud computing has made significant progress in the field of distributed systems in recent years, and that the relationship between cloud computing and BFT (Byzantine Fault Tolerance) has been explored. Furthermore, the "purely academic interest" of cloud services in BFT is often cited. According to these claims, cloud computing is not exclusive to any one cloud. Rather, the term "cloudy sky" refers to a wide range of cloud shapes and forms with various applications. [11] One of the most important technology topics in today's world is cloud computing. IT, business operations, software engineering, and data storage have all been greatly impacted. Cloud computing allows for capacity expansion without the need for expensive equipment, software, or employee training. According to NIST, "Cloud computing is a model for delivering convenient, bundled resources with ubiquitous, on-demand access that can be easily delivered through a variety of service provider interfaces." [12] Many providers now define cloud computing in different ways. Therefore, cloud security or security issues are inevitable in cloud computing. The phrase “cloud security” encompasses a wide range of laws, tools, and precautions to protect data, applications, and cloud computing infrastructure. Along with other security concerns in cloud computing systems, it includes privacy protection, data encryption, and resource availability protection against security threats. For a cloud computing system to last long, each of these issues must be addressed and resolved appropriately. [13] Cloud computing enables providers to provide space to users on their physical systems and lease their services on an hourly basis. However, users of these services face a number of security risks. Examples of potential risks include malicious use, insecure interfaces, and vulnerabilities, according to research conducted by the Cloud Security Alliance. These risks are related to cloud computing and application programming interfaces (APIs). [14] Although SaaS is not often specifically mentioned, these publications generally address security concerns related to cloud computing. We would like to emphasize that the structure of our search string is the result of a learning process that includes looking at synonyms used in the literature and testing with different keyword combinations that cover many aspects of cloud security requirements. [15] Customers can flexibly expand their capabilities with cloud computing without having to build new infrastructure, hire more employees, or purchase new software licenses. Much like an electrical grid does, it uses an application to distribute shared resources, software, infrastructure, and data to computers and other devices over a network, typically the Internet. [16] As needed, it makes sense to shift from a deployment strategy to a distribution and consumption strategy. Working with external cloud service providers and specialized suppliers to manage cloud governance challenges is critical, as is establishing and enforcing a specific cloud service level agreement (SLA) to address potential security trust issues. Given how cloud technologies are evolving and how much demand there is, the lack of expertise in cloud security management is acute. [17] The industry standard for service-oriented computing is cloud computing, which provides computing infrastructure and solutions as a service. It has changed how computing resources are used and compressed. One of the key benefits of cloud computing is the ability to test new concepts and applications with minimal risk; this was not possible before the introduction of cloud technology. Because of this, many cloud service providers now offer a variety of applications that vary in size, type, and requirements. [18] The idea of cloud computing is to provide a shared set of computing resources (including networks, servers, storage, applications, and services) that can be reconfigured on demand. These resources require little management or interaction with service providers and can be provisioned and deployed quickly. A complete summary of cloud computing environments, which highlights the different models and key features of each. [19]. Cloud computing

security is evolving with the risks, as these risks are often detected too late to stop the events. Due to its disruptive nature, complex architecture, and shared resources, cloud computing poses unique and serious risks to all stakeholders. All parties involved must acknowledge these risks and take appropriate action. To effectively mitigate risk, security must be embedded into every layer of a cloud computing platform using cutting-edge technology and industry best practices. Cloud users, providers, brokers, carriers, auditors, and others must put in place the necessary security measures to protect the platform from serious, often business-critical risks. According to a recent survey, the industry believes that security engineering provides the best practices, methods, and approaches for building secure systems. [20] In contrast to previous contributions, this work provides a comprehensive assessment of cloud security issues, defenses, and security designs (such as intrusion detection and prevention systems) with a parametric analysis. We classify security concerns using a component-based taxonomy that takes into account network, virtual machines, storage, and cloud-based applications. Various trusted cloud computing options are also explored, along with compliance concerns related to current standards, legislation, and regulations. Furthermore, we provide a brief summary of upcoming security issues and potential fixes. [32]

2. MATERIALS AND METHODS

Given conflicting criteria, the VIKOR technique attempts to rank and select options. It finds a compromise solution that balances the decision-making process by maximizing the group utility for the majority and minimizing the unhappiness for the opposing party. In an improved version, weight stability intervals and trade-offs are added to the VIKOR approach to increase its adaptability and versatility. VIKOR is based on an aggregation function that evaluates "proximity to the ideal" using linear normalization. In contrast, the TOPSIS method uses vector normalization and creates two reference points. In contrast to VIKOR's approach, TOPSIS ignores the relative importance of distances from these reference points. [21] Several studies that analyze test results using VIKOR and its variants were evaluated, as was the use of the VIKOR approach to determine student graduation grades in business programs. These studies demonstrate the ability of VIKOR to capture multiple preferences across a variety of study types, demonstrating its continued applicability. Many criteria, qualities, and alternatives are more easily accounted for in this study due to the stepwise application of the VIKOR approach. Models are ranked and selected using the VIKOR approach according to multiple criteria. [22] The VIKOR technique is used for benchmarking studies in the hotel industry. In this context, an intelligent approach is presented to evaluate the performance of Iranian cement companies. This approach mixes fuzzy logic with the AHP method. The proposed method facilitates the assessment of financial success. Using VIKOR to handle complex decision-making problems with competing criteria in a multi-criteria decision-making process allows decision-makers to optimize complex systems and obtain a final answer. [23] In a multi-attribute decision-making (MADM) dilemma, partner selection takes into account both qualitative and quantitative aspects. Therefore, there are several justifications for selecting an alternative using MADM techniques. The main goal of MADM techniques is to select the best option from a set of candidates, taking into account the decision maker's preferences among several competing qualitative and quantitative factors. [24] The purpose of this study is to introduce the use of aggregation operators used in the VIKOR method and propose an IOWA-based VIKOR (IOWA-VIKOR) strategy for multi-criteria decision making, taking into account the complex mindset of the decision maker. The IOWASD aggregation operator consists of a parameterized family of standardized distance aggregation operators ranging from the minimum to the maximum standardized distance. The IOWA operator of the VIKOR technique can improve the decision-making process by accepting the complex thinking (or various levels of complexity) of the decision maker. [25] When describing the difference or similarity between two estimates, projection provides a more complete approach than distance. However, there are some shortcomings in the projection model of PFSs. Although no study has established the concept of image fuzzy entropy, the entropy weighting method is a useful tool for determining objective weights. In addition, projection may be a more appropriate method than distance, which is used to measure the proximity to the optimal solution by conventional fuzzy VIKOR. However, no study has combined VIKOR techniques with projection in the setting of fuzzy images. In light of this study, it is proposed to solve these problems and develop a more complete MCDM. [26] Since it is difficult to ascertain the exact values of properties when selecting materials, it is more reasonable to consider them as interval numbers. It has been emphasized how important it is for engineering design to understand the differences in material properties, manufacturing tolerances, and service loading situations. Standards for materials and industrial processes outline the boundaries of property variation. However, since manufactured materials vary between batches and manufacturers, materials engineers must be cautious when reporting material properties. [27] A recently proposed MCDM technique, VIKOR, is used to solve risk problems in a fuzzy environment and identify the most important failure modes for corrective actions. The VIKOR approach focuses on ranking and selecting from a set of possibilities when criteria are not in agreement. It searches for a compromise that is acceptable to the decision maker. Fuzzy set theory and the VIKOR technique are used to solve risk assessment problems in FMEA. [28] Unlike ordinary fuzzy sets, IFS theory does not restrict the sum of the membership degree and the non-membership degree to one. This forward definition successfully handles the situation when the decision maker is hesitant to provide precise estimates. The intuitionistic ambiguity index, also known as the hesitation measure, is a measure of the decision maker's uncertainty. In this sense, IFSs provide a more complete way of understanding uncertainty than traditional fuzzy sets. Due to this property of IFSs, VIKOR has been adapted for use in situations involving intuitionistic ambiguity. [29] The weights derived from these

ratings are established using a fuzzy AHP approach. The VIKOR approach is then used to rank the various alternatives by adding these weights. However, unlike the previously mentioned models, our approach assumes that the data used to evaluate the performance of the alternatives is random. Using our approach, decision makers can determine the relative importance of the ranking criteria of the alternatives whose performance is represented by random data. [30]. The VIKOR approach finds a solution that is close to and compatible with the best choice by ranking the options. It shows that VIKOR is a multi-criteria decision-making technique that allows the proximity between ideal and anti-ideal alternatives to be evaluated simultaneously using a straightforward computational process. The currently published literature indicates that several authors have used the VIKOR approach in a comparative manner in their research. [31]

Cloud Geographical Regions (CGR) refer to specific locations where cloud service providers, like Amazon Web Services (AWS), establish their data centers to offer cloud computing services.

Proximity to Users: To reduce latency and improve service performance, CGRs are deployed close to end customers. This is essential for applications that need to process data in real time and respond quickly.

Diversity of Services: Typically, each CGR offers a variety of services such as networking, storage, and processing power. Since different services may be available in different CGRs, users can choose the area that best suits their needs.

Availability Zones (AZs): Typically, each CGR offers a variety of services such as networking, storage, and processing power. Since different services may be available in different CGRs, users can choose the area that best suits their needs.

Cost and Performance Considerations: Depending on local infrastructure, energy costs, and operating costs, different CGRs may charge different prices for their services. When choosing a CGR for their applications, users often have to weigh performance against cost.

Regulatory Compliance: Some organizations may be required to follow specific rules when processing and storing data. Choosing a CGR located in a specific country or region can help you meet these legal obligations.

Evaluation Parameters

Benefit Parameters (Higher values are better)

- S1: Number of Available Services
- S2: Service Performance Rating

Non-Benefit Parameters (Lower values are better)

- C1: Distance from Consumer
- C2: Data Transfer Latency

3. ANALYSIS AND DISSECTION

TABLE 1. Cloud Computing Security

	Determination of best and worst value			
	Distance from Consumer	Available Services	Performance Rating	Data Transfer Latency
Proximity to Users	50	5	4.7	100
Diversity of Services:	40	4	4.5	90
Availability Zones (AZs)	60	6	4.9	110
Cost and Performance Considerations	30	3	4	80
Regulatory Compliance	70	7	4.8	120
Best	30	7	4.9	80
worst	70	3	4	120

When determining the best and worst values based on the provided metrics, several aspects are taken into account, such as accessibility to users, service diversity, availability zones (AZs), cost-performance balance, and regulatory compliance. Numerical rankings for attributes including data transfer latency, performance ratings, available services, and distance from customers are used to evaluate each category. Best Deal: The best balance between price, performance, legal compliance, and service quality determines the best value. The data shows that being close to users results in a low distance score (30), good service diversity (7), efficient latency (80), and excellent performance (4.9). These characteristics combine to create a very favorable choice because it reduces delays, ensures high compliance, and offers a variety of services. Poor value: Low performance, extensive customer distances, inefficient cost-performance alignment, and limited services are characteristics of poor value. Along with low service variety (3), moderate performance (4.0),

and high latency (120), regulatory compliance (70) performs poorly. This configuration is the best choice as it identifies serious shortcomings in the effective delivery of high-quality services..

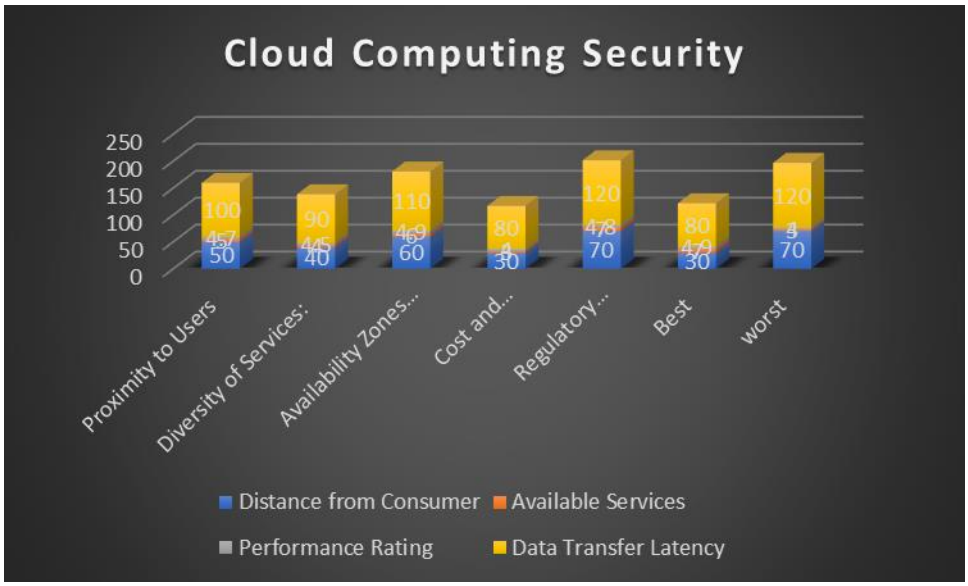


FIGURE 1. Cloud Computing Security

The key metrics that affect cloud computing performance and efficiency are depicted in the "Cloud Computing Security" diagram. These components include cost-performance balance, availability zones (AZs), diversity of services, proximity to users, and regulatory compliance. Data transfer latency, performance ratings, available services, and distance from customers are the parameters examined. Proximity to users strikes the optimal overall balance, with short distance from customers (50), adequate service availability (5), good performance (4.7), and relatively low data transfer latency (100). This combination demonstrates an effective technique for reducing delays without sacrificing service quality. Unlike proximity to users, the diversity of services implies a slightly larger distance (40) and fewer services are provided (4). Its latency (90) and performance rating (4.5) are still good, however, ensuring a good level of performance and reliability. It performs better in terms of regulatory compliance (7) and maintains strong performance (4.8) in terms of available services, but performs poorly in terms of consumer proximity (70). However, its overall performance is reduced by its high latency (120). Excellent performance (4.9), low latency (80), wide service diversity (7), and excellent consumer proximity (30) all contribute to the highest value. Conversely, the system's inefficiency is shown by the worst values, which include high latency (120), limited services (3), average performance (4.0), and long distance (70).

TABLE 2. Culculation Sj and Rj

	Culculation Sj and Rj			
Cost and Performance Considerations	0.125	0.125	0.0555556	0.125
Diversity of Services	0.0625	0.1875	0.1111111	0.0625
Availability Zones (AZs)	0.1875	0.0625	0	0.1875
Cost and Performance Considerations	0	0.25	0.25	0
Regulatory Compliance	0.25	0	0.0277778	0.25

The contributions of the components, including S j and R j calculation, cost and performance concerns, service diversity, availability zones (AZs), and regulatory compliance, are examined in Table 2. A comparative assessment is possible by assigning numerical values to each element indicating its importance in the different dimensions. With a slightly lower number in one column (0.0556), cost and performance considerations consistently show scores of 0.125 in most columns. This indicates a consistent but mild impact on overall performance, which does not fluctuate greatly. With a low value of 0.0625 in one column and a significant contribution of 0.1875 in another column, service diversity exhibits high variability. Its chosen value is highlighted by this variation, which makes it important in some contexts but less important in others. Availability Zones (AZs) show a mixed trend, with a high score of 0.1875 in some aspects and a low score of 0 in others. This trend indicates that while availability zones do not always contribute to all attributes, they are significant in certain settings. While it drops to 0.0278 in one column, regulatory compliance has the highest values (0.25) in many. Its overall impact is significant, highlighting its important function in ensuring reliability and security.

Copyright@ REST Publisher

TABLE 3. Sj & Rj

	Sj	Rj
Cost and Performance Considerations	0.4305556	0.125
Diversity of Services:	0.4236111	0.1875
Availability Zones (AZs)	0.4375	0.1875
Cost and Performance Considerations	0.5	0.25
Regulatory Compliance	0.5277778	0.25
S+ R+	0.4236111	0.125
S- R-	0.5277778	0.25

Based on the information in Table 3, I will illustrate the Sj and Rj values across several measures to demonstrate how well a cloud service provider is performing. According to the report, regulatory compliance performs significantly better across all criteria, with a maximum Sj score of 0.5277778. With an Sj score of 0.5, cost and performance factors follow, showing excellent success in this area as well. Availability Zones (AZs) receive a moderate score of 0.4375, while the cost and performance variables (which appear twice) and service type have low Sj values of 0.4236111 and 0.430556, respectively. The most important components of the assessment, as indicated by the Rj values, are performance and cost issues, with regulatory compliance, which have the highest weight (0.25). Service diversity and availability zones share the second most important position (Rj values of 0.1875), while another criterion has the lowest weight (0.125). Regulatory compliance performs best overall when considering both scores and weights. The range of performance across all criteria is shown by the minimum S+ R+ value of 0.4236111 and the maximum S-R-value of 0.5277778.

TABLE 4. Culculation Qj

	Culculation Qj
Cost and Performance Considerations	0.033333
Diversity of Services	0.25
Availability Zones (AZs)	0.316667
Cost and Performance Considerations	0.866667
Regulatory Compliance	1

I demonstrate the relative importance and ranking of several factors that appear in a cloud service provider rating using the Qj calculations in Table 4. With a flawless Qj score of 1, regulatory compliance stands out as the most important component, indicating that it is the most important component of the rating system. With a high score of 0.866667, cost and performance concerns come in second place, making them the most important criteria. Given these high scores, these two components should be prioritized when making decisions. Service Type is at 0.25 and Availability Zones (AZs) have a moderate Qj value of 0.316667 in the mid-range. These scores indicate that, while these characteristics are significant, they are not as significant as the first two criteria. The second entry for cost and efficiency considerations is interesting, but it has a low score of 0.033333. This means that distinct aspects or contexts of cost and efficiency are assessed independently. The wide range of Qj values between 0.033333 and 1 shows that the criteria are clearly ranked in order of importance, with cost and efficiency concerns and a component of regulatory compliance outweighing the other components in the assessment framework.

TABLE 5. Rank

	Rank
Cost and Performance Considerations	5
Diversity of Services	4
Availability Zones (AZs)	3
Cost and Performance Considerations	2
Regulatory Compliance	1

In Table 5 of the ranking data, I will demonstrate the hierarchical importance of several factors that appear to be a framework for evaluating cloud service providers. With a rank of 1, regulatory compliance ranks first and has become the most important factor in the evaluation process. This is consistent with the growing importance of compliance in cloud services, especially in regulated industries. Cost and performance concerns come in second place, meaning that financial performance and efficiency measures are second in the decision-making hierarchy. Availability Zones (AZs) came in third, indicating that redundancy and geographic distribution are not the best objectives, but rather have a moderate impact. In fourth place, the diversity of services is shown, which indicates that while the type of service is important, other criteria are of greater importance. It is interesting to see the reappearance of cost and efficiency issues in 5th place, which would indicate that they are assessed differently and given less weight. It is clear that regulatory compliance and

Copyright@ REST Publisher

key cost-effectiveness indicators are given priority over infrastructure provision and service diversity in this ranking system. A comprehensive assessment of the various aspects of financial and performance criteria is indicated by the dual appearance of cost and efficiency components in the various rankings.

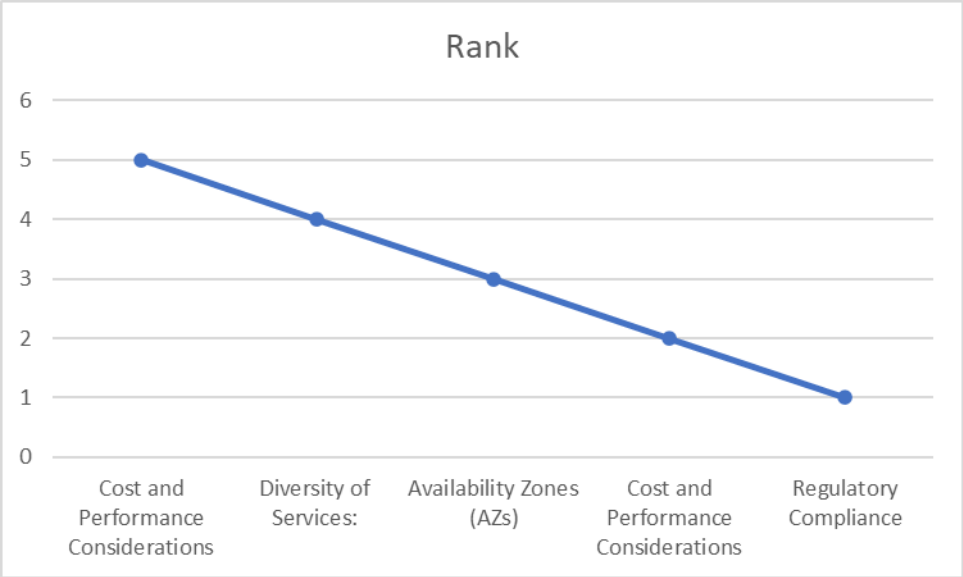


FIGURE 2. Rank

Figure 2: Ranking Analysis This figure shows the relative relevance and effectiveness of several factors used to evaluate a cloud service provider, such as availability zones (AZs), diversity of services, cost and performance considerations, and regulatory compliance. Cost and performance factors rank highest, highlighting their importance in influencing the performance of cloud services. It is a key component of the evaluation due to its powerful performance and significant weight. The importance of providing a wide range of services that are tailored to user demands is reflected in the second-place ranking for diversity of services. Third place goes to availability zones (AZs), indicating its moderate importance. Although it makes a significant contribution in some situations, its impact is less reliable than other variables. The cost and efficiency factors are in second and fourth place, respectively, indicating that although this criterion is significant, its influence varies depending on the evaluation component. Finally, of all the factors, regulatory compliance has the lowest overall influence, ranking fifth. However, its key role in safety and standards compliance remains essential, as seen by its excellent performance in other situations

4. CONCLUSION

Cloud computing has quickly become a revolutionary paradigm for service-based computing, providing organizations and individuals with scalable, efficient, and adaptive solutions. It improves access and reliability by providing computing resources on demand, eliminating the need for expensive infrastructure investments. Despite rapid adoption, cloud security remains a major concern as serious security issues have emerged. These security challenges, which range from site-level risks such as virtualization and network security to more complex issues such as multi-tenant systems, data protection, and access control, have attracted a lot of attention from researchers and businesses. Although cloud computing has many advantages, it also poses special security threats due to its decentralized architecture and reliance on shared resources. Ensuring data security at every stage of its lifecycle, including creation, storage, use, and destruction, is still very difficult. Strong security measures must be taken as cloud platforms expand, with an emphasis on secure communication protocols, identity management, and encryption. To properly manage these risks, all parties involved - cloud service providers, users, and auditors - must implement comprehensive security measures. In addition, as cloud computing has grown, conventional security practices have been rethought. The shift from physical, on-premises computing systems to cloud-based infrastructure has made many traditional security measures less effective, forcing the development of new methods for creating secure virtualized environments. As cloud technologies continue to evolve, the integration of other technologies such as edge computing further complicates security issues, necessitating creative approaches to securing distributed systems. Security should be a top priority as more organizations adopt cloud computing for its operational benefits. To preserve trust and realize the full potential of cloud computing, it is essential that cloud environments are secure and compliant with legal and regulatory requirements. As these technologies advance, security must be built into every cloud architecture layer, using cutting-edge techniques and best practices to mitigate risks. Ultimately, while cloud computing has many benefits, its security issues must be addressed quickly to ensure its continued success and widespread adoption.

Copyright@ REST Publisher

REFERENCES

[1]. Sengupta, Shubhashis, Vikrant Kaulgud, and Vibhu Saujanya Sharma. "Cloud computing security--trends and research directions." In 2011 IEEE World Congress on Services, pp. 524-531. IEEE, 2011.

[2]. Liu, Wentao. "Research on cloud computing security problem and strategy." In 2012 2nd international conference on consumer electronics, communications and networks (CECNet), pp. 1216-1219. IEEE, 2012.

[3]. Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no. 3 (2012): 583-592.

[4]. Tripathi, Alok, and Abhinav Mishra. "Cloud computing security considerations." In 2011 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), pp. 1-5. IEEE, 2011.

[5]. Butt, Umer Ahmed, Muhammad Mehmood, Syed Bilal Hussain Shah, Rashid Amin, M. Waqas Shaukat, Syed Mohsan Raza, Doug Young Suh, and Md Jalil Piran. "A review of machine learning algorithms for cloud computing security." Electronics 9, no. 9 (2020): 1379.

[6]. Sabahi, Farzad. "Cloud computing security threats and responses." In 2011 IEEE 3rd International Conference on Communication Software and Networks, pp. 245-249. IEEE, 2011.

[7]. Ali, Mazhar, Samee U. Khan, and Athanasios V. Vasilakos. "Security in cloud computing: Opportunities and challenges." Information sciences 305 (2015): 357-383.

[8]. Basu, Srijita, Arjun Bardhan, Koyal Gupta, Payel Saha, Mahasweta Pal, Manjima Bose, Kaushik Basu, Saunak Chaudhury, and Pritika Sarkar. "Cloud computing security challenges & solutions-A survey." In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), pp. 347-356. IEEE, 2018.

[9]. Verma, Amandeep, and Sakshi Kaushal. "Cloud computing security issues and challenges: a survey." In Advances in Computing and Communications: First International Conference, ACC 2011, Kochi, India, July 22-24, 2011, Proceedings, Part IV 1, pp. 445-454. Springer Berlin Heidelberg, 2011.

[10]. Ryan, Mark D. "Cloud computing security: The scientific challenge, and a survey of solutions." Journal of Systems and Software 86, no. 9 (2013): 2263-2268.

[11]. AlZain, Mohammed A., Eric Pardede, Ben Soh, and James A. Thom. "Cloud computing security: from single to multi-clouds." In 2012 45th Hawaii International Conference on System Sciences, pp. 5490-5499. IEEE, 2012.

[12]. Singh, Saurabh, Young-Sik Jeong, and Jong Hyuk Park. "A survey on cloud computing security: Issues, threats, and solutions." Journal of Network and Computer Applications 75 (2016): 200-222.

[13]. Zhang, Ni, Di Liu, and Yunyong Zhang. "Research on cloud computing security." In 2013 International Conference on Information Technology and Applications, pp. 370-373. IEEE, 2013.

[14]. Alouffi, Bader, Muhammad Hasnain, Abdullah Alharbi, Wael Alosaimi, Hashem Alyami, and Muhammad Ayaz. "A systematic literature review on cloud computing security: threats and mitigation strategies." Ieee Access 9 (2021): 57792-57807.

[15]. Iankoulova, Iliana, and Maya Daneva. "Cloud computing security requirements: A systematic review." In 2012 Sixth International Conference on Research Challenges in Information Science (RCIS), pp. 1-7. IEEE, 2012.

[16]. Radwan, Tarek, Marianne A. Azer, and Nashwa Abdelbaki. "Cloud computing security: challenges and future trends." International Journal of Computer Applications in Technology 55, no. 2 (2017): 158-172.

[17]. Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith. "The management of security in cloud computing." In 2010 Information Security for South Africa, pp. 1-7. IEEE, 2010.

[18]. Srinivasan, Madhan Kumar, K. Sarukesi, Paul Rodrigues, M. Sai Manoj, and P. Revathy. "State-of-the-art cloud computing security taxonomies: a classification of security challenges in the present cloud computing environment." In Proceedings of the international conference on advances in computing, communications and informatics, pp. 470-476. 2012.

[19]. Ramachandra, Gururaj, Mohsin Iftikhar, and Farrukh Aslam Khan. "A comprehensive survey on security in cloud computing." Procedia Computer Science 110 (2017): 465-472.

[20]. Khan, Minhaj Ahmad. "A survey of security issues for cloud computing." Journal of network and computer applications 71 (2016): 11-29.

[21]. Shahzad, Farrukh. "State-of-the-art survey on cloud computing security challenges, approaches and solutions." Procedia Computer Science 37 (2014): 357-362.

[22]. Opricovic, Serafim, and Gwo-Hshiung Tzeng. "Extended VIKOR method in comparison with outranking methods." European journal of operational research 178, no. 2 (2007): 514-529.

[23]. Siregar, Dodi, Heri Nurdiyanto, S. Sriadhi, Diana Suita, Ummul Khair, Robbi Rahim, Darmawan Napitupulu et al. "multi-attribute decision making with VIKOR method for any purpose decision." In Journal of Physics: Conference Series, vol. 1019, p. 012034. IOP Publishing, 2018.

[24]. Rezaie, Kamran, Sara Saeidi Ramiyani, Salman Nazari-Shirkouhi, and Ali Badizadeh. "Evaluating performance of Iranian cement firms using an integrated fuzzy AHP–VIKOR method." Applied Mathematical Modelling 38, no. 21-22 (2014): 5033-5046.

[25]. Alimardani, Maryam, Sarfaraz Hashemkhani Zolfani, Mohammad Hasan Aghdaie, and Jolanta Tamošaitienė. "A novel hybrid SWARA and VIKOR methodology for supplier selection in an agile environment." Technological and economic development of economy 19, no. 3 (2013): 533-548.

[26]. Liu, Hu-Chen, Ling-Xiang Mao, Zhi-Ying Zhang, and Ping Li. "Induced aggregation operators in the VIKOR method and its application in material selection." Applied Mathematical Modelling 37, no. 9 (2013): 6325-6338.

Copyright@ REST Publisher

[27]. Wang, Le, Hong-yu Zhang, Jian-qiang Wang, and Lin Li. "Picture fuzzy normalized projection-based VIKOR method for the risk evaluation of construction project." Applied Soft Computing 64 (2018): 216-226.
[28]. Jahan, Ali, and K. L. Edwards. "VIKOR method for material selection problems with interval numbers and target-based criteria." Materials & Design 47 (2013): 759-765.
[29]. Liu, Hu-Chen, Long Liu, Nan Liu, and Ling-Xiang Mao. "Risk evaluation in failure mode and effects analysis with extended VIKOR method under fuzzy environment." Expert Systems with Applications 39, no. 17 (2012): 12926-12934.
[30]. Devi, Kavita. "Extension of VIKOR method in intuitionistic fuzzy environment for robot selection." Expert Systems with Applications 38, no. 11 (2011): 14163-14168.
[31]. Tavana, Madjid, Reza Kiani Mavi, Francisco J. Santos-Arteaga, and Elahe Rasti Doust. "An extended VIKOR method using stochastic data and subjective judgments." Computers & Industrial Engineering 97 (2016): 240-247.
[32]. Kumar, Manish, and Cherian Samuel. "Selection of best renewable energy source by using VIKOR method." Technology and Economics of Smart Grids and Sustainable Energy 2 (2017): 1-10.

Copyright@ REST Publisher