International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 10
***Article Received:** 24 August 2023 **Revised:** 12 October 2023 **Accepted:** 25 October 2023*

Evaluation of Cloud-Based Cyber Security System

Ananda Ravuri[1], Dr. Raghu Kumar Lingamallu[2], Dr. S Arvind[3], Dr. P. Srinivasa Rao[4], Veeraswamy Ammisetty[5]
[1]Senior Software Engineer Intel corporationHillsboro, Oregon 97124 USA
Mail : Ananda.ravuri@intel.com , ananda.ravuri@gmail.com
[2]Assistant Professor Department of CSE, KG Reddy College of Engineering and Technology, Chilkur Village,Hyderabad - 501504
Mail : lrgupta528@gmail.com
[3] Professor, Department of Computer Science Engineering Hyderabad Institute of Technology and Management Mail : scarvi@rediffmail.com
[4]Associate Professor Department of Computer Science & Engineering Vaasireddy Venkatadri Institute of Technology, Namburu, Guntur
Mail: psr.srinivas999@gmail.com
[5]Associate Professor, Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur Andhra Pradesh, India.
Mail: ammisetty.veeraswamy@gmail.com

Abstract

Cloud-based cyber security systems leverage the power of cloud computing to protect digital assets from cyber threats. By utilizing remote servers and advanced algorithms, these systems provide real-time monitoring, threat detection, and incident response. They offer scalable solutions, enabling businesses to adapt to evolving threats and handle increasing data volumes. Cloud-based security systems provide benefits such as reduced infrastructure costs, continuous updates and patches, centralized management, and global threat intelligence. They protect against various attacks, including malware, phishing, DDoS, and unauthorized access. With their flexibility, reliability, and ease of deployment, cloud-based cyber security systems are becoming essential for organizations seeking robust protection in today's interconnected digital landscape. The research significance of cloud-based cyber security systems lies in their ability to address the growing complexity and scale of cyber threats in today's digital landscape. By leveraging cloud computing, these systems offer several key advantages for researchers and organizations: Scalability: Cloud-based systems can scale resources on-demand, allowing researchers to handle large volumes of data and analyze complex threat patterns effectively. Cost-efficiency: The cloud eliminates the need for extensive on-premises infrastructure, reducing costs associated with hardware, maintenance, and upgrades. Researchers can allocate resources based on their needs, optimizing cost-effectiveness. Real-time monitoring and threat detection: Cloud-based systems provide real-time monitoring of network traffic, enabling quick identification of suspicious activities and potential threats. Researchers can leverage advanced analytics and machine learning algorithms to enhance threat detection capabilities. Collaboration and knowledge sharing: Cloud platforms facilitate collaboration among researchers and organizations by enabling the sharing of threat intelligence, best practices, and research findings. Compliance and regulatory requirements: Cloud platforms often offer built-in compliance features and tools to meet regulatory requirements, assisting researchers in adhering to data protection and privacy standards. Overall, the research significance of cloud-based cyber security systems lies in their ability to provide scalable, cost-effective, and advanced security capabilities, empowering researchers to mitigate evolving cyber threats and protect sensitive data and systems effectively. We will be using Weighted Product Methodology (WPM) which is a decision-making technique that assigns weights to various criteria and ranks alternatives based on their weighted scores. It involves multiplying the ratings of each criterion by their corresponding weights and summing them up to determine the overall score. This method helps prioritize options and make informed decisions in complex situations. Taken of Operational, Technological, Organizational Recorded Electronic Delivery, Recorded Electronic Deliver, Blockchain technology, Database security, Software updates, Antivirus and antimalware The Organizational cyber security measures comes in last place, while Technological cyber security measures is ranked top and Operational measures comes in between the above two in second place. In conclusion, a cloud-based cyber security system revolutionizes the way organizations safeguard their digital assets. By utilizing remote servers, advanced algorithms, and real-time monitoring, it offers scalable and robust protection against evolving threats. With features like threat detection, data encryption, and centralized management, it ensures enhanced security, agility, and efficiency. Embracing a cloud-based approach empowers organizations to stay ahead in the ever-changing landscape of cyber security, effectively safeguarding their critical data and infrastructure.

Keywords: Cloud Computing, Cyber Security, network security.

1. INTRODUCTION

A network-based architecture with a focus on sharing processing resources is called cloud computing. Users can access cloud resources as needed through a service model. A large number of users can share resources in cloud systems, and the system's capacity can be enhanced effectively by adding more hardware to handle rising load [5]. Cloud computing refers to a method that provides convenient, on-demand access to shared resources through a pool of configurable computing resources such as networks, servers, storage, applications, and services. This approach allows for rapid provisioning and release of resources with minimal effort and interaction from the service provider. Cloud computing offers benefits such as massive scalability, improved user experience, and cost efficiencies driven by the Internet. However, it also presents security challenges, making businesses more susceptible to cyber attacks due to the concentration of digital assets. Historically, studies on cloud computing security primarily focused on data and information security. However, recent research has expanded to explore the interactions between people, software, and services on the Internet, known as cyber security or cyberspace security. The private sector's ownership of critical infrastructure (CI) components, combined with the potential consequences on national security, the economy, and individual well-being, highlights the significance of securing these systems. While cyber attacks typically have limited effects, the risks associated with digital practices and information security have led CI to offer insurance service options, influencing decision-making processes for technological strategies such as cloud computing deployments, risk migrations, and data outsourcing. To address these challenges, we propose an architecture based on cloud computing that enables the storage of large volumes of threat monitoring and detection data. This architecture aims to facilitate effective threat detection and scene investigation, ultimately enhancing cyber security situation awareness for large company networks. The integration of AI and cyber security involves three components. The first involves using AI for cyber security, the second involves using AI for cyber security, and the third involves identifying privacy attacks brought on by AI.[7] Several governmental organisations have recently begun making significant investments in IT and cybersecurity education and training. The need for highly skilled cybersecurity specialists is soaring and is expected to do so for a very long time.[8 Moreover, as the main objective of cloud computing is to provide applications and services to users via the internet, it is susceptible to various security risks both from within and outside the system. These risks include threats such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, which are specifically designed to disrupt or damage subscriber data.10] as well as various benefits like cost savings and flexible and effective resource use. By dynamically raising the number of DDoS mitigation instances, for instance, it is feasible to quickly and adaptably respond to the intense assault traffic in the case of a distributed denial of service (DDoS) attack. Additionally, the deployment of numerous security functions created by various security solution suppliers is made easier by this cloud-based security service paradigm.[11] For conducting cyber security management, a cloud computing system based on the MapReduce framework is utilised, which may speed up the processing of enormous network traffic data[12]. The outcomes of the framework demonstrate that the network's performance has improved as a result of the application of the suggested multi-agent techniques[13]. Blocking unauthorized disclosure of the information of CC service users is necessary for confidentiality. Users must pay cloud providers to provide confidentiality; nevertheless, in CC, the emphasis is on resource authentication (e.g., requiring a username and password for each user). Additionally, availability refers to the user's capacity to use the system in the manner they would expect.[14] Because of data centralization and standardised architecture, cloud deployments frequently include cutting-edge security tools.Cloud providers may concentrate all of their security resources on protecting the cloud architecture thanks to the homogeneous resource pooling structure of the cloud[17]. This results in the total security features of virtualization technology being added on top of the already-existing security challenges and problems with cloud computing. In a cloud computing architecture, the cloud service provider and the cloud users are shown in Figure 1 as a typical cloud-based scenario.[18]

2. MATERIALS & METHOD

Operational: In the context of cyber security systems, operational refers to the ongoing activities and processes that ensure the effective functioning and protection of an organization's IT infrastructure. It involves tasks such as monitoring network traffic, managing security incidents, implementing access controls, conducting regular vulnerability assessments, and maintaining incident response plans, all aimed at safeguarding systems and data from potential threats and breaches.

Technological: In the realm of cyber security systems, technological refers to the use of advanced tools, technologies, and solutions to protect digital assets. This includes utilizing firewalls, intrusion detection systems, encryption algorithms, authentication mechanisms, and security software. Technological measures are designed to mitigate risks, detect and respond to threats, and fortify the overall resilience of a system against cyber-attacks and vulnerabilities.

Organizational: Organizational, in the context of cyber security systems, refers to the strategic and operational measures implemented by an organization to address cyber threats. This includes establishing policies, procedures, and guidelines for information security, conducting employee training and awareness programs, defining roles and responsibilities, implementing incident response plans, and creating a culture of security awareness throughout the organization to protect against cyber risks and promote a secure computing environment.

Recorded Electronic Delivery: Recorded Electronic Delivery (RED) is a secure method used in cyber security systems for transmitting electronic records. It ensures the authenticity, integrity, and confidentiality of data during transmission. By employing encryption, digital signatures, and secure protocols, RED safeguards sensitive information from unauthorized access, tampering, or interception, ensuring secure and reliable electronic delivery of records in various sectors like legal, financial, and government.

Recorded Electronic Deliver: Recorded Electronic Delivery (RED) is a method used in cyber security systems for securely transmitting electronic records. It ensures the integrity, authenticity, and confidentiality of sensitive information during transmission. RED employs encryption, digital signatures, and secure protocols to protect data from interception, tampering, and unauthorized access, ensuring secure and reliable electronic delivery of records in various domains like healthcare and finance.

Blockchain technology Database security: Blockchain technology enhances database security in cyber security systems. It provides a decentralized and immutable ledger that records and verifies transactions. By eliminating a central point of failure, it reduces the risk of data tampering and unauthorized access. The transparent and auditable nature of blockchain adds an extra layer of trust and integrity to database management, enhancing overall security.

Software updates: Software updates play a crucial role in cyber security systems. Regular updates help patch vulnerabilities, fix bugs, and address security flaws in software. By keeping software up to date, users ensure they have the latest defenses against emerging threats, reducing the risk of successful cyberattacks and enhancing overall system security and protection.

Antivirus and antimalware: Antivirus and antimalware are vital tools in a cyber security system. Antivirus software specifically targets and neutralizes computer viruses, while antimalware provides broader protection against various malicious software, such as worms, trojans, spyware, and other types of malware. Both help safeguard systems by detecting, quarantining, and removing threats to prevent potential damage or unauthorized access.

Method:

By Bridgeman (1922), the Weighted Product Method had been developed. Although the method has not been widely used, Yoon and Hwang (1995) claim that it has sound logic and is computationally simple.[1] WPM are frequently used to describe scoring techniques. The Bridgeman-proposed weighted aggregated sum product assessment (WASPAS) is a member of the more recent generation of MCDM techniques. With this approach, well-known weighted sum model (WSM) and weighted product model (WPM) methodologies are combined in a novel way.[3] In instances with dynamic environments, it enables excellent ranking accuracy. Since it can be difficult for consumers to describe their degree of happiness or dissatisfaction with the cloud service providers with respect to the qualities, there is generally confusion in the crisp data.[4]. The methodology was used in actual cyberattacks, especially the widespread attacks on Estonia and Iran, and the outcomes of the evaluation of the cyberattacks were given.[5] WPM normalises the performance values of alternatives using equations. It uses many formulae to calculate the scores of the choices. Using the descending order of their overall score, WPM rates the options. [10]. In this model, the attribute values are the CSP performance in each measure that is recorded in the history log, while the weights are the QoS preferences supplied by the requesting user.[11] One benefit of WPM is its applicability in both single- and multi-dimensional MADMs. The drawback is that there is no solution with an equal weight of the choice vectors instead of actual values[12]. The AHP approach is used to determine the relative weights of the various criteria. As a result, the WPM approach is used to rank the candidate networks. Fuzzy logic uses a combination of neural networks and utility functions to choose a network. The suggested approach makes use of a fuzzy neural network to gather network-, user-, and terminal-related input criteria and assess each access network's performance [14]. T Multiple Criteria Decision Making (MCDM) models and fuzzy synthetic decision-making are the foundation of several service selection methodologies. [21] The outcomes of our evaluation of the cloud services we chose revealed that our model outperformed existing MDMC methodologies like TOPSIS, WPM, and the original AHP [17], very successfully captured the BDTP, guaranteed Big Data QoS, and scaled with the growing number of cloud providers. Through a variety of cloud services from numerous CSPs, WPM, the SAW, and imposed QoS requirements of Big Data workflows were used [16]. Similar to WSM is the Weighted Product Method (WPM). The primary distinction is that multiplication is required in WPM rather than addition. [18] WPM should be used to promote strict cybersecurity regulations, according to further research.[13] When choosing a cloud-based cybersecurity system, organizations can make educated selections by adhering to the Weighted Product Methodology. A solution that best satisfies the organization's cybersecurity goals is chosen through the methodical evaluation of several criteria and their respective weights.[25]

Article Received: *24 August 2023* ***Revised:*** *12 October 2023* ***Accepted:*** *25 October 2023*

3. RESULT & DISCUSSION:

TABLE 1. Cloud Based Cyber Security System

Group of Cybersecurity Measures	**Recorded Electronic Delivery**	**Recorded Electronic Deliver**	**Blockchain technology**	**Database security**	**Software updates**	**Antivirus and antimalware**
Operational	3.1905	2.8571	2.6667	3.2857	3.8571	2.4286
Technological	4.1429	4.0476	3.2857	3.1905	3.0476	2.9048
Organizational	2.9523	2.5714	4.4286	3.2238	2.8095	3.381

Table 1 shows Alternative: Operational, Technological, Organizational & Evaluation: Recorded Electronic Delivery, Recorded Electronic Deliver, Blockchain technology, Database security, Software updates, Antivirus and antimalware parameters. Recorded Electronic Delivery is Showing the Highest value: Technological - 4.1429 is Showing the Lowest value: Organizational - 2.9523. Recorded Electronic Deliver: is Showing the Highest value: Technological - 4.0476 is Showing the Lowest value: Organizational - 2.5714. Blockchain technology is Showing the Highest value: Organizational - 4.4286 is Showing the Lowest value: Technological - 3.2857. Database security is Showing the Highest value: Organizational - 3.2238 is Showing the Lowest value: Technological - 3.1905. Software updates is Showing the Highest value: Operational - 3.8571 is Showing the Lowest value: Technological - 3.0476 Antivirus and antimalware is Showing the Highest value: Organizational - 3.381 is Showing the Lowest value: Technological - 2.9048

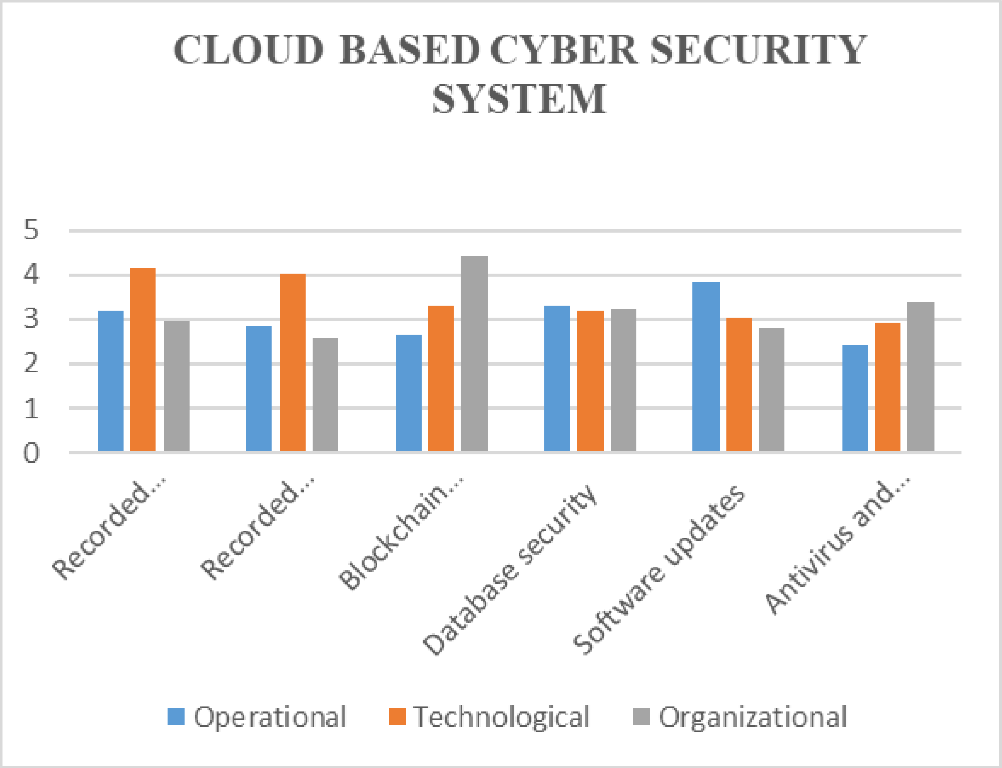

FIGURE 1. Cloud Based Cyber Security System

Figure 1 shows Alternative: Operational, Technological, Organizational & Evaluation: Recorded Electronic Delivery, Recorded Electronic Deliver, Blockchain technology, Database security, Software updates, Antivirus and antimalware parameters. Recorded Electronic Delivery is Showing the Highest value: Technological - 4.1429 is Showing the Lowest value: Organizational - 2.9523. Recorded Electronic Deliver: is Showing the Highest value: Technological - 4.0476 is Showing the Lowest value: Organizational - 2.5714. Blockchain technology is Showing the Highest value: Organizational - 4.4286 is Showing the Lowest value: Technological - 3.2857. Database security is Showing the Highest value: Organizational - 3.2238 is Showing the Lowest value: Technological -

3.1905. Software updates is Showing the Highest value: Operational - 3.8571 is Showing the Lowest value: Technological - 3.0476 Antivirus and antimalware is Showing the Highest value: Organizational - 3.381 is Showing the Lowest value: Technological - 2.9048

TABLE 2. Performance Value

Performance value					
0.770	0.706	0.602	1.000	1.000	1.000
1.000	1.000	0.742	0.971	0.790	0.836
0.713	0.635	1.000	0.981	0.728	0.718

Table 2 shows performance value of alternative and evaluation parameters is showing the Operational Highest value: 1.000 is showing the Lowest value: 0.602. Technological is showing the Highest value: 1.000 is showing the Lowest value: 0.742 Organizational is showing the Highest value: 1.000 is showing the Lowest value: 0.635.

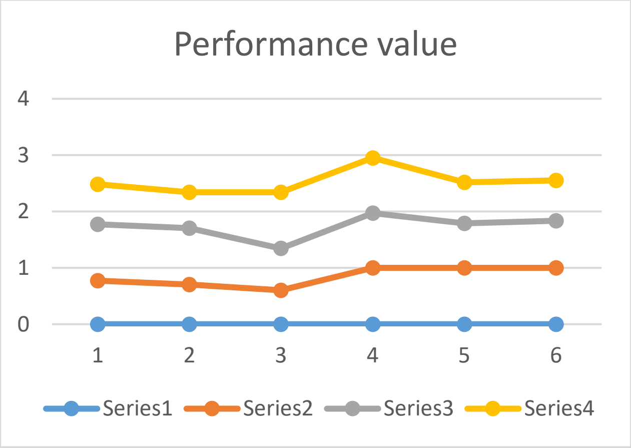

FIGURE 2. Performance Value

Figure 2 Table 2 shows performance value of alternative and evaluation parameters is showing the Operational Highest value: 1.000 is showing the Lowest value: 0.602. Technological is showing the Highest value: 1.000 is showing the Lowest value: 0.742 Organizational is showing the Highest value: 1.000 is showing the Lowest value: 0.635.

TABLE 3. Weight

Weights					
0.167	0.167	0.167	0.167	0.167	0.167
0.167	0.167	0.167	0.167	0.167	0.167
0.167	0.167	0.167	0.167	0.167	0.167
0.167	0.167	0.167	0.167	0.167	0.167
0.167	0.167	0.167	0.167	0.167	0.167

Table 3 Weight shows the informational set for the weight all same value 0.167.

TABLE 4. Weighted Normalised Decision Matrix

Weighted Normalised Decision Matrix					
0.957	0.944	0.919	1.000	1.000	1.000

1.000	1.000	0.951	0.995	0.962	0.971
0.945	0.927	1.000	0.997	0.949	0.946

Table 4 shows the weighted normalized decision matrix of alternative and evaluation parameters Operational is showing the Highest value: 1.000 is showing the Lowest value: 0.919 is showing the Technological Highest value is showing the 1.000 Lowest value: 0.951. Organizational Highest value: 1.000 is showing the Lowest value: 0.927.

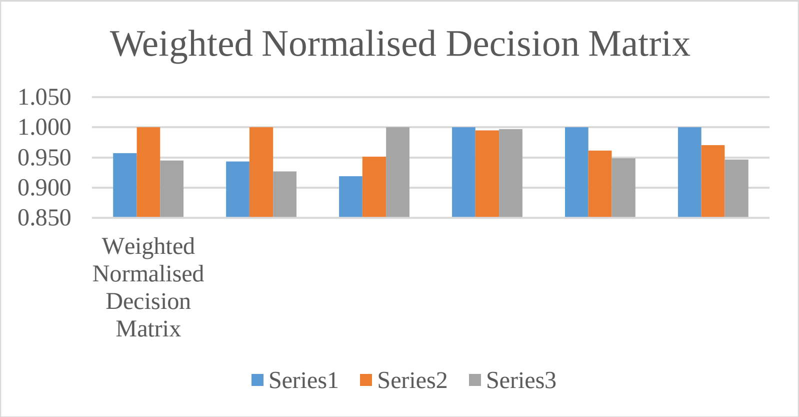

FIGURE 3. Weighted Normalized Decision Matrix

Figure 3 shows the weighted normalized decision matrix of alternative and evaluation parameters Operational is showing the Highest value: 1.000 is showing the Lowest value: 0.919 is showing the Technological Highest value is showing the 1.000 Lowest value: 0.951. Organizational Highest value: 1.000 is showing the Lowest value: 0.927.

Table 5. Preference Score & Rank

	Preference score	**Rank**
Operational	0.830166064	2
Technological	0.883598261	1
Organizational	0.784105569	3

Table 5 shows the Preference Score & Rank of alternative and evaluation parameters the weighted normalized decision matrix provided, we can identify the highest and lowest values within Operational Highest value: 1.000 Lowest value: 0.919 Technological Highest value: 1.000 Lowest value: 0.951 Organizational Highest value: 1.000 Lowest value: 0.927.

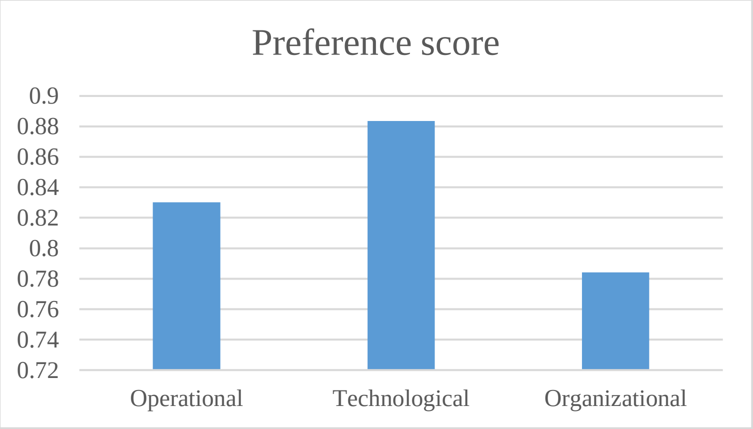

FIGURE 4. Preference score

***Article Received:** 24 August 2023 **Revised:** 12 October 2023 **Accepted:** 25 October 2023*

Figure 4 show the preference scores provided, we can identify the highest and lowest values. Technological is showing the Highest value: 0.883598261 Organizational is showing the Lowest value: 0.784105569

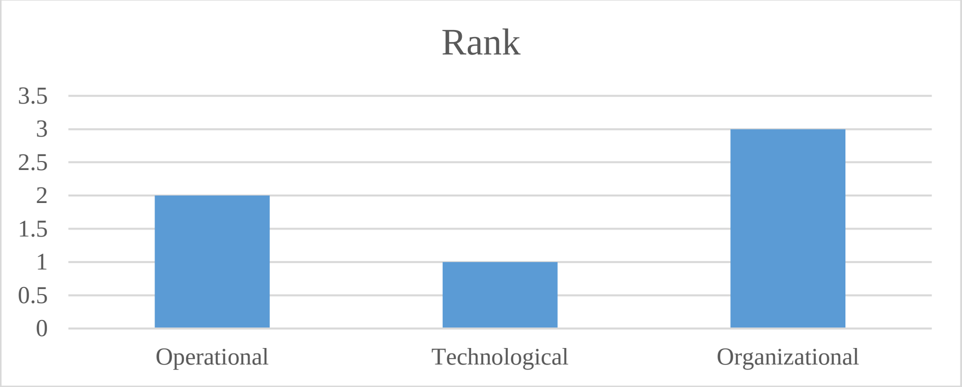

FIGURE 5. Rank

Figure 5 show the preference scores provided, we can identify the highest and lowest values. Technological is showing the Highest rank and Organizational is showing the Lowest rank.

4. CONCLUSION

In conclusion, cloud-based cyber security systems have become an indispensable component of modern digital defense strategies. They offer a wide array of benefits, including scalability, flexibility, and advanced threat protection, making them an attractive option for organizations of all sizes. One of the key advantages of cloud-based cyber security systems is their scalability. Cloud providers can rapidly allocate resources based on demand, allowing organizations to scale their security infrastructure up or down as needed. This scalability ensures that organizations can effectively handle sudden spikes in network traffic and adapt to evolving threats without investing in additional hardware or personnel. Cloud-based cyber security systems also excel in advanced threat protection. Leveraging machine learning algorithms and artificial intelligence, these systems can analyze vast amounts of data in real-time, detecting and mitigating emerging threats promptly. Additionally, cloud providers often have access to global threat intelligence networks, allowing them to proactively defend against new attack vectors and share insights with their customers. However, it's essential for organizations to consider certain factors when implementing cloud-based cyber security systems. They should carefully evaluate the security measures offered by cloud providers, ensuring they meet compliance requirements and align with their specific needs. Organizations must also establish robust access controls, encryption mechanisms, and monitoring procedures to maintain data privacy and integrity. In conclusion, cloud-based cyber security systems offer a compelling solution to protect organizations against evolving cyber threats. The scalability, flexibility, advanced threat protection, and offloading of maintenance burdens make them a valuable asset in today's dynamic digital landscape. By leveraging the power of the cloud, organizations can enhance their security posture, focus on their core competencies, and confidently navigate the ever-changing cyber security landscape.

REFERENCES

[1]. Pipyros, Kosmas, Christos Thraskias, Lilian Mitrou, Dimitris Gritzalis, and Theodoros Apostolopoulos. "A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual." Computers & Security 74 (2018): 371-383.

[2]. Alam, Khubaib Amjad, Rodina Ahmed, Faisal Shafique Butt, Soon-Gohn Kim, and Kwang-Man Ko. "An uncertainty-aware integrated fuzzy AHP-WASPAS model to evaluate public cloud computing services." Procedia Computer Science 130 (2018): 504-509.

[3]. Gireesha, Obulaporam, Nivethitha Somu, Kannan Krithivasan, and Shankar Sriram VS. "IIVIFS-WASPAS: an integrated multi-criteria decision-making perspective for cloud service provider selection." Future Generation Computer Systems 103 (2020): 91-110.

[4]. Abdel-Basset, Mohamed, Abduallah Gamal, Karam M. Sallam, Ibrahim Elgendi, Kumudu Munasinghe, and Abbas Jamalipour. "An Optimization Model for Appraising Intrusion-Detection Systems for Network Security Communications: Applications, Challenges, and Solutions." Sensors 22, no. 11 (2022): 4123.

[5]. Hussain, Abid, Jin Chun, and Maria Khan. "A novel customer-centric Methodology for Optimal Service Selection (MOSS) in a cloud environment." Future Generation Computer Systems 105 (2020): 562-580.

[6]. El Kassabi, Hadeel T., and Mohamed Adel Serhani. "De-centralized reputation-based trust model to discriminate between cloud providers capable of processing big data." In 2017 IEEE International Congress on Big Data (BigData Congress), pp. 266-273. IEEE, 2017.

[7]. Skondras, Emmanouil, Angelos Michalas, and Dimitrios D. Vergados. "Mobility management on 5g vehicular cloud computing systems." Vehicular Communications 16 (2019): 15-44.

[8]. Serhani, Mohamed Adel, H. A. Kassabi, and Ikbal Taleb. "Towards an efficient federated cloud service selection to support workflow big data requirements." Advances in Science, Technology and Engineering Systems Journal 3, no. 5 (2018): 235-247.

[9]. Serhani, Mohamed Adel, Hadeel T. El Kassabi, and Ikbal Taleb. "Quality profile-based cloud service selection for fulfilling big data processing requirements." In 2017 IEEE 7th International Symposium on Cloud and Service Computing (SC2), pp. 149-156. IEEE, 2017.

[10]. Rao, Ch Maheswara, and K. Venkatasubbaiah. "Application of WSM, WPM and TOPSIS Methods for the Optimization of Multiple Responses." International journal of hybrid information technology 9, no. 10 (2016): 59-72.

[11]. Kamble, Sachin Gorakh, Kinhal Vadirajacharya, and Udaykumar Vasudeo Patil. "Decision making in power distribution system reconfiguration by blended biased and unbiased weightage method." Journal of Sensor and Actuator Networks 8, no. 2 (2019): 20.

[12]. Kamali Saraji, Mahyar, Dalia Streimikiene, and Grigorios L. Kyriakopoulos. "Fermatean fuzzy CRITIC-COPRAS method for evaluating the challenges to industry 4.0 adoption for a sustainable digital transformation." Sustainability 13, no. 17 (2021): 9577.

[13]. Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." (2011).

[14]. Takahashi, Takeshi, Youki Kadobayashi, and Hiroyuki Fujiwara. "Ontological approach toward cybersecurity in cloud computing." In Proceedings of the 3rd international conference on Security of information and networks, pp. 100-109. 2010.

[15]. Tissir, Najat, Said El Kafhali, and Noureddine Aboutabit. "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal." Journal of Reliable Intelligent Environments 7 (2021): 69-84.

[16]. Thuraisingham, Bhavani. "Cyber security and artificial intelligence for cloud-based internet of transportation systems." In 2020 7th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2020 6th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 8-10. IEEE, 2020.

[17]. Salah, Khaled, Mohammad Hammoud, and Sherali Zeadally. "Teaching cybersecurity using the cloud." IEEE Transactions on Learning Technologies 8, no. 4 (2015): 383-392.

[18]. Jouini, Mouna, Anis Ben Aissa, L. Ben Arfa Rabai, and Ali Mili. "Towards quantitative measures of Information Security: A Cloud Computing case study." International Journal of cyber-security and digital forensics (IJCSDF) 1, no. 3 (2012): 248-262.

[19]. Hyun, Sangwon, Jinyong Kim, Hyoungshick Kim, Jaehoon Jeong, Susan Hares, Linda Dunbar, and Adrian Farrel. "Interface to network security functions for cloud-based security services." IEEE Communications Magazine 56, no. 1 (2018): 171-178.

[20]. Xu, Guobin, Wei Yu, Zhijiang Chen, Hanlin Zhang, Paul Moulema, Xinwen Fu, and Chao Lu. "A cloud computing based system for cyber security management." International Journal of Parallel, Emergent and Distributed Systems 30, no. 1 (2015): 29-45.

[21]. Tariq, Muhammad Imran, Shahzadi Tayyaba, Muhammad Usman Hashmi, Muhammad Waseem Ashraf, and Natash Ali Mian. "Agent based information security threat management framework for hybrid cloud computing." IJCSNS 17, no. 12 (2017): 57.

[22]. Alhenaki, Lubna, Alaa Alwatban, Bashaer Alamri, and Noof Alarifi. "A survey on the security of cloud computing." In 2019 2nd international conference on computer applications & information security (ICCAIS), pp. 1-7. IEEE, 2019.

[23]. Fischer, Eric. "Cybersecurity Issues and Challenges." LIBRARY OF CONGRESS WASHINGTON DC, 2017.

[24]. Bhardwaj, Akashdeep, and Sam Goundar. "A framework to define the relationship between cyber security and cloud performance." Computer Fraud & Security 2019, no. 2 (2019): 12-19.

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

[26]. Bhamare, Deval, Maede Zolanvari, Aiman Erbad, Raj Jain, Khaled Khan, and Nader Meskin. "Cybersecurity for industrial control systems: A survey." computers & security 89 (2020): 101677.

[27]. Ahmed, Monjur, and Mohammad Ashraf Hossain. "Cloud computing and security issues in the cloud." International Journal of Network Security & Its Applications 6, no. 1 (2014): 25.

[28]. Ugale, Bhushan A., Piyush Soni, Tsering Pema, and Anirudha Patil. "Role of cloud computing for smart grid of India and its cyber security." In 2011 Nirma University International Conference on Engineering, pp. 1-5. IEEE, 2011