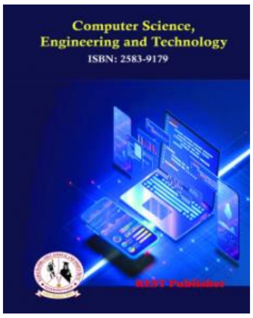
Computer Science, Engineering and Technology

Vol: 1(2), June 2023

REST Publisher; ISSN: 2583-9179 (Online)

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

DOI: https://doi.org/10.46632/cset/1/2/6



Optimizing Cloud Computing Networks in Information Security Controls using COPRAS Method

Madhusudhan Dasari sreeramulu

Leading financial institution, USA.

Corresponding Author Email: dsmadhu007@gmail.com

Abstract: *The emergence of cloud computing networks has led to a sharp rise in the frequency of cyberattacks. As a result, networks' appropriate security has become an issue for organisations. Organisations' information security advisors must make difficult and complex choices when evaluating and choosing information security measures that allow for the protection of their assets and resources. Controls for information security must be chosen depending on the proper level of security. However, choosing them requires a thorough examination into the organization's vulnerabilities, risks, and threats as well as taking into account the organization's budgetary and implementation limits. By suggesting a formalised method, the Complex Proportional Assessment (COPRAS) Method, this research aimed to enhance the information security control analysis process. This method was used to rank and choose the most pertinent collection of information security controls to meet an organization's information security needs. In order to determine which information security measures are most suited for an organisation, we contend that the prioritisation of those controls using the (COPRAS) Method results in an effective and economical assessment and evaluation of those controls. In order to implement security and privacy successfully, an organisation with a network connected with the cloud needs to evaluate and prioritise the information security measures. The organisation intends to exert as much effort as possible to analyse ISCs, which are crucial for risk management, in this situation with few resources. For organisations, choosing the right information security policies is a serious and crucial issue. This section's goal is to select the top ISCs from a list of available options. The organisation wants to include all necessary factors that might be used in the selection of security controls. Implementation time (C1), effectiveness (C2), risk (C3), budgetary restrictions (C4), exploitation time (C5), maintenance cost (C6), and mitigation time (C7) are the seven key factors used by the decision makers' team to select and evaluate ISCs. By using the COPRAS METHOD, the Information Security Control 2 received the top ranking and the Information Security Control 5 received the bottom ranking. Implementation time (C1), Effectiveness (C2), Risk (C3), Budgetary Constraints (C4), Exploitation time (C5), Maintenance cost (C6), and Mitigation time (C7) are the evaluation factors.*

Keywords*: *cloud computing, Information Security, Effectiveness, Risk and control selection.

1. INTRODUCTION

With the advent of cloud computing (CC), business models that offer "information technology (IT) as a service" as opposed to "IT as a product" underwent a fundamental shift. Significant energy savings for data centres without sacrificing service level agreements (SLAs) are a great way to motivate them economically and environmentally. [1] Resources, services, and data are delivered over the internet in the cloud computing paradigm. Cloud computing enables users to access and use a shared pool of computing resources housed on distant data centres as opposed to local servers or individual PCs. [2]. Servers, storage, databases, networking,

software, analytics, and other resources are among them. The following are the main elements of cloud computing:
1. On-demand self-service: Without the assistance of the service provider, users can deploy, configure, and manage resources (such as virtual machines or storage).
2. Wide-ranging network access: Cloud services are available online and may be used by a variety of gadgets, including computers, tablets, and smartphones.
3. Resource pooling: Providers make use of multi-tenant architectures, which let numerous clients share the same physical resources while virtualization maintains some level of user segregation.
4. Quick elasticity: Depending on demand, resources can be easily scaled up or down. Users only pay for the resources they use, increasing them during periods of high activity and reducing them during periods of low activity.
5. Measurable service: Resource utilisation is automatically controlled and optimised by cloud computing technologies. Users receive transparent and flexible pricing based on the computer resources they use. [3]

Three basic models are generally used to classify cloud computing services:
1. Infrastructure as a Service (IaaS): Over the internet, IaaS offers virtualized computing resources. Pay-as-you-go users can rent virtual computers, storage, and networking equipment. Users have the most control and flexibility under this approach since they are in charge of administering the operating systems, applications, and data.
2. Platform as a Service (PaaS): PaaS gives programmers a platform and setting for creating, deploying, and managing applications without having to deal with the complexities of infrastructure administration. Databases, operating systems, middleware, and development tools are all included.
3. Software as a Service (SaaS): SaaS is a subscription-based online delivery method for software applications. These programmes can be accessed and used by users via a web browser without the need to locally install or maintain the software. There are several benefits to cloud computing, including affordability, scalability, flexibility, and accessibility. It has completely changed how organisations and individuals approach computers because it makes advanced technology more accessible without requiring significant up-front investments in infrastructure and hardware. Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and others are significant cloud service providers.[4] Information security controls are precautions taken to guard against unauthorised access to, use of, disclosure of, disruption of, alteration of, or destruction of information and information systems. These controls assist organisations in protecting their sensitive information, preserving the information's confidentiality, integrity, and accessibility, and mitigating various security risks. Controls for information security may be of a technical, administrative, or physical type and are created to address certain security goals. [5]Here are a few typical categories of information security measures:
Limiting and controlling who has access to certain resources, data, or systems are access controls. This comprises permission techniques (such as access rights, privileges), as well as authentication procedures (such as passwords, multi-factor authentication).Data is converted into unintelligible formats through encryption employing cryptographic methods. It makes sure that data is secure and secured even if it is intercepted. Network security tools called firewalls keep an eye on and regulate both inbound and outbound network traffic.They serve as barriers, limiting unauthorised access and associated dangers, between trusted internal networks and unreliable external networks. Systems called intrusion detection and prevention systems (IDPS) keep an eye on system and network activity for indications of unauthorised access, abuse, or malicious activity. They are able to instantly recognise and thwart such attempts. Technologies for data loss prevention (DLP) assist in preventing the loss, leak, or access by unauthorised users of sensitive data. To implement data security policies, they keep an eye on data that is in use, in motion, and at rest. Regular security awareness training informs staff members on possible security dangers, safe practises, and how to spot and handle security events. Backup and recovery from disaster In the event of data loss due to unintentional deletion, hardware failure, or cyberattacks, regular data backups and disaster recovery strategies ensure that crucial data may be restored. [7] Vulnerability management and patching Maintaining vulnerabilities and regularly upgrading software and programmes with the most recent security patches assist stop the exploitation of recognised security flaws. Controls for physical security Physical security measures, such as access control systems, video monitoring, and secure facility design, safeguard physical resources and assets. Response to Incident Plan A security breach or incident response plan describes the procedures to be done, guaranteeing a coordinated and efficient response to reduce damage and recover swiftly.[8] Monitoring and Auditing System and network activity auditing and monitoring on a regular basis aid in the detection of potential security events and policy violations. Controls for information security should be customised to each organization's unique requirements and dangers A thorough and effectively implemented set of controls aids in preserving the privacy, accuracy, and accessibility of sensitive data, preserving the organization's standing, and safeguarding its resources.[9] Businesses now have a viable alternative to the on-premise IT infrastructure in the form of cloud computing (CC). Our understanding of how to obtain computer resources with a high degree of adaptability, availability, and minimal administrative work has altered as a result. [11]. Users can access information and overcome technological boundaries thanks to cloud computing. With cloud computing, the need to maintain technical infrastructure disappears as cloud

service providers take on the responsibility for system maintenance and data protection. “The term "cloud computing" describes both the hardware and system software in the data centres that host the applications that are provided as services via the Internet”.[11] The enormous development and expansion of cloud computing demand effective and precise methods for choosing cloud service providers, since careful provider selection is crucial to raising the level of confidence between customers and providers. Information security is gaining significance every day and is the cornerstone of cloud networks that are connected with an organization's wireless sensor networks. By assessing information security risks and maintaining the confidentiality, integrity, and availability of resources, information security decision-makers' primary goal is to secure cloud networks, WSNs, and the organization's assets. [9–11]. Numerous risk assessment frameworks rely on appropriate rules and qualitative approaches. As a result, evaluating ISCs based on these risk assessment frameworks takes longer and costs more. An organization's information system should ultimately aim to streamline decision-making and enhance all activities. The assessment of security threats related to corporate operations has traditionally involved information security risk management (ISRM). Additionally, it assessed which information security rules were the most essential. [12,13]. Information security professionals used to select all forms of ISCs without taking risks, attacks, costs, effectiveness, mitigation time, exploitation time, and maintenance time into account. [14]. It might be difficult and complicated to evaluate and choose the best information security controls for an integrated cloud network from the available information security standards. Choosing the best group of ISCs to provide the necessary security against threats is not well covered in baseline guidelines. It goes without saying that this collection of ISCs should satisfy organisations' needs for security and privacy. Organisational demands and associated security considerations must guide the selection of ISCs. The organization's information security policy must include a list of controls that can provide the necessary privacy and security protection, as well as security requirements. The confidence required for cloud networks can be established if a group of ISCs has undergone a thorough evaluation and been proven to meet the demands of an organisation. Additionally, an organisation must make sure the best collection of ISCs is correctly identified, installed, and operated via the risk management processes [19]

2. METHODOLOGY

Evaluation preference:

1. The implementation time: The implementation time for information security controls can vary significantly depending on several factors, including the complexity of the controls, the size and nature of the organization, the existing infrastructure, and the level of security required. Here are some considerations that can impact the implementation time. The scope and complexity of the information security controls being implemented play a crucial role. Simple controls, such as enabling two-factor authentication for user accounts, can be implemented relatively quickly. On the other hand, more complex controls, like setting up a comprehensive data loss prevention (DLP) system or building a robust incident response plan, may require more time and effort. The availability of resources, both in terms of skilled personnel and financial budget, can affect the implementation time. Adequate resources and expertise may expedite the implementation process. Planning and Preparation proper planning and preparation are essential before implementing security controls. This includes conducting a risk assessment, identifying security requirements, and creating a roadmap for implementation. Taking the time to plan can lead to a smoother and more effective implementation process. Existing Infrastructure and Systems is the state of the organization's existing infrastructure and systems can impact implementation time. Integrating security controls into legacy systems or complex IT environments may take longer compared to implementing controls in modern and more standardized environments. If the implementation is driven by specific compliance regulations or industry standards, the organization must ensure that all the necessary requirements are met. This may involve additional time for documentation and validation**.**

2. Effectiveness: The capacity of security measures and controls to accomplish their intended goals in preserving the confidentiality, integrity, and availability of information and information systems is referred to as effectiveness in information security**.** An effective information security program ensures that appropriate safeguards are in place to defend against potential threats, vulnerabilities, and attacks, and it involves continuously evaluating and improving security measures to keep up with evolving risks and challenges. Here are some key aspects of effectiveness in information security Risk Management: An effective information security program is risk-based. It involves identifying and assessing potential risks to information and systems, prioritizing them based on their impact and likelihood, and implementing controls to mitigate or manage those risks. Risk management helps allocate resources to areas where they are most needed, making the overall security approach more efficient. Comprehensive Security Controls: An effective security strategy encompasses a wide range of security controls, including technical, administrative, and physical measures. These controls should be appropriate for the organization's specific needs and risk profile, addressing potential threats from both internal and external sources. Continuous Monitoring and Assessment: Effective information security requires continuous monitoring of systems and network activities to identify and respond to security incidents promptly. Regular security assessments, such as vulnerability assessments and penetration testing, help identify weaknesses and provide insights for improvement. Security Awareness and Training: Employees play a crucial role in information security. A successful programme involves security awareness training for every employee to advise them of security best practises, social engineering threats, and secure information handling procedures.

3. Risk in information security controls: Risk in information security controls refers to the potential for vulnerabilities, threats, or weaknesses to impact the effectiveness of security measures and expose information and information systems to harm. Even though information security controls are put in place to mitigate risks, they are not immune to vulnerabilities themselves. Understanding and managing these risks is critical to ensuring the overall effectiveness of the security program. Here are some common risks associated with information security controls are Implementation and Configuration Errors**:** Misconfigurations or errors during the implementation of security controls can lead to unintended consequences, rendering the controls less effective or even introducing new vulnerabilities. Inadequate Coverage: Incomplete or insufficient security controls may leave certain aspects of the information environment unprotected, providing opportunities for attackers to exploit weaknesses. Complexity and Interdependencies: Complex security controls may introduce unintended interactions or dependencies that can create vulnerabilities or impact the overall system stability. Obsolete Technology: Outdated or unsupported security technologies may have known vulnerabilities that attackers can exploit, reducing the effectiveness of these controls. Human Error and Insider Threats: Human error, accidental actions, or malicious intent from insiders can undermine the effectiveness of security controls and compromise information security. False Sense of Security: Over-reliance on specific security controls without considering the broader security posture may lead to a false sense of security, leaving blind spots that attackers can exploit. Emerging Threats: The threat landscape is constantly evolving, and new threats may emerge that existing controls are not designed to handle. Failure to Update and Patch: Systems and security measures may become vulnerable to known exploits if security updates and patches are not applied. Resource Limitations: Insufficient resources, including budget constraints and lack of skilled personnel, can impact the deployment and maintenance of security controls. Integration Challenges: Integrating various security technologies and tools can be complex and may result in gaps or inefficiencies in the security posture. Compliance Gaps: Failure to align security controls with relevant regulatory requirements or industry standards can lead to compliance gaps.

4. Budgetary constraints: Budgetary constraints can pose significant challenges when it comes to implementing and maintaining effective information security controls. Adequate funding is essential to deploy appropriate security measures, acquire necessary technologies, hire skilled personnel, and support ongoing security operations. When budget limitations are present, organizations may need to make strategic decisions to balance their security needs with available resources. Here are some common issues and strategies related to budgetary constraints in information security controls are Resource Allocation: With limited funds, organizations need to prioritize their security investments. Conducting a thorough risk assessment can help identify critical areas that require immediate attention and allocate resources accordingly. Cost-Benefit Analysis: When considering security controls and technologies, organizations should conduct cost-benefit analyses to determine the most effective solutions within their budgetary limits. It's essential to evaluate whether the expected security benefits outweigh the costs. Open-Source Solutions: In some cases, open-source security solutions can provide cost-effective alternatives to commercial products. However, thorough evaluation and consideration of support and maintenance aspects are necessary. Managed Security Services**:** Outsourcing some aspects of security to managed security service providers (MSSPs) can be more cost-effective for smaller organizations that may not have the resources to build and maintain an in-house security team. Security Awareness Training: Investing in security awareness training for employees can be a cost-effective measure to improve overall security posture, as human error is a common factor in security incidents.

5. Exploitation time: Exploitation time, in the context of information security, refers to the duration between the identification of security vulnerability or weakness and the successful exploitation of that vulnerability by an attacker. It represents the window of opportunity during which a system or application is at risk before the vulnerability is patched or mitigated. The exploitation time can vary widely based on several factors, including Public Disclosure: security vulnerability's exploitation time may be shortened if it is revealed to the public or detailed in a security advisory. The vulnerability's severity and the potential consequences for the target system may affect how quickly attackers prioritise exploiting the vulnerability. Availability of Exploit Code: If exploit code or tools to leverage the vulnerability are readily available or shared within the cybercriminal community, attackers can use them more quickly. Security Posture of the Target: The security measures and controls in place on the target system play a significant role. A well-secured system may be more challenging to exploit, thereby increasing the exploitation time.

5. Maintenance costs: Maintenance costs in information security controls refer to the ongoing expenses associated with operating, updating, and managing security measures to ensure their continued effectiveness. These costs are essential for maintaining a strong security posture and protecting information and information systems from evolving threats and vulnerabilities. Some factors that contribute to maintenance costs in information security controls include Security Software and Hardware Updates: Regular updates and patches are required for security software, firewalls, intrusion detection/prevention systems, antivirus solutions, and other security tools. These updates ensure that the security controls stay current and effective against new threats.

Subscription and Licensing Fees: Many security solutions, especially cloud-based services and third-party security tools, require subscription or licensing fees. These costs are recurring and contribute to the ongoing maintenance of the security infrastructure. Technical Support: Organizations may need technical support agreements with vendors or service providers to troubleshoot and resolve issues with security controls. Technical support costs are often based on the level of service required.

7. Mitigation time: Mitigation time in information security controls refers to the duration taken to address and resolve security vulnerabilities or incidents once they have been identified. It represents the time taken from the detection of a security issue to the successful implementation of measures to mitigate or remediate the problem.

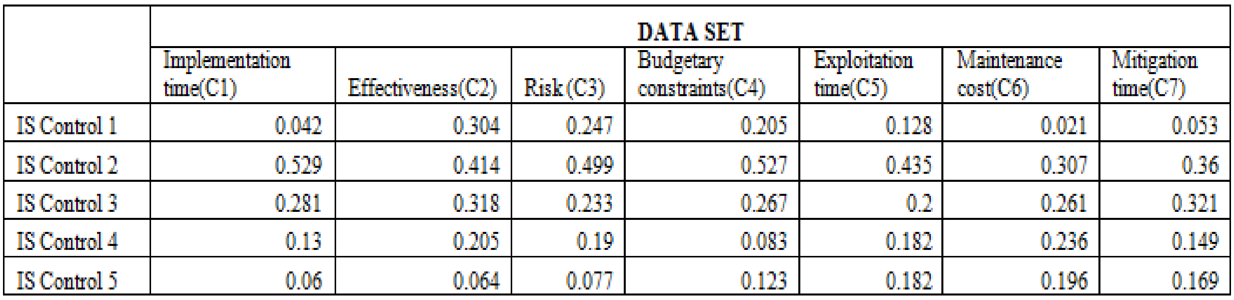
The mitigation time is a critical aspect of information security, as a shorter mitigation time reduces the window of opportunity for attackers to exploit vulnerabilities or carry out successful cyber attacks. A longer mitigation time can increase the risk of significant damage, data breaches, or system compromises.

3. COMPLEX PROPORTIONALITY ASSESSMENT (COPRAS)

Complex proportionality assessment (COPRAS) the weighted mean and geometric integration operators integrate the pifss information. Then, to solve the decision problems COPRAS and integration operators basically two algorithms we create. +e COPRAS method zavadskas and introduced by many. Every compare alternative and benchmark weights taking into account their calculating priorities. In all such methods, to rank the given alternatives one of the most suitable methods COPRAS is and quantity and broadly to qualitative analysis is used. COPRAS method is engineering problems in computation time means less, more basic, good a comparative analysis of methods transparency and their graphical about co-strategies greater possibilities of understanding indicates. Hajiaka et al in literature, various of cobra's method in fuzzy environment there are many applications [13]. To enhance the evaluation efficiency of COPRAS, stochastic COPRAS (COPRAS-s) stochastic decision making named as complex using process proportionality rating (COPRAS) approach. In the COPRAS-s, scale significance performance of weights and alternatives a fixed number of values decision maker (dm) estimates minimum and maximum from a uniform distribution over a range of values by generating random numbers determined. Thus, the number of experts increased and different opinions because of the incorporation, the decision-making process done effectively[14]. Among these methods, cobras recent attracted more inquiries. As a compromise method, cobras' method is better rate of settlement and worse of the ratio for the best solution basically determines a solution. Unlike other madm methods, the copras method is step-by-step dependent on rankings and reasoning importance to make selection and both application degrees uses. Chatterjee et al conducted comparative analysis, ahp, others like vikor and topsis compared to methods, copras-based the technique requires less evaluation time, very straight forward and graphical explanation also shows high reliability. In literature, cobras have many uses [15]. This method is a fine-ideal answer and one associated with the terrible-perfect answer determines the solution, consequently a compromise mcdm method can be considered. First, the COPRAS system under deterministic conditions created for decision making. Uncertainty in decision making is a as an inevitable feature, of cobras method in this study an extended form is proposed [16]. Origin of cobras method is mcdm led to increased use of copras in javadskas et al. Cobras method selected for the project using residential appliances. Zavatskas and many others. In an environment of uncertainty combined grey-cobras contractors rated with approach. Korabe et al. The copras approach using industrial robots a formal selection was made. Yastani et al. Green suppliers qfd and copras for evaluation with integrated model created by zheng et al. For reluctant linguistic preferences by using copras assessment of severity of lung disease did vahdani et al. Gap with the COPRAS approach valued in an ambiguous context robots. Mousavi et al. Comparison with other mcdm methods for selection of auxiliary equipment by performance of the COPRAS approach researched. Chatterjee et al [17]. Theoretically sustainable eligibility of city cell for small city to evaluate, several criteria complex proportions with of assessment system (COPRAS) application is provided. the parameters efficient calculation and city of visualizing the abstract for purpose this time geography linked to information system [18]. COPRAS method of information can be processed from different angles. Exacerbation in copras patients indicators for assessment, the more they have values, patients better body status and price standards, the better the values they've, the poor bodily situation of sufferers which might be divided into benefit standards. Similarly, the cobras system is complex based on proportional calculation considering two criteria, this is much compared to other methods contains accurate information, the handling is cost criterion or this is a measure of goodness [19]. To achieve the ranking of alternatives, the value of each attribute should also contain their values and operational requirements to evaluate alternative to complement a decision-making process should be used. Available attribute data size or can be qualitative. Contradictory decision making is influenced by criteria to solve a selection trouble in situations madm approach COPRAS is useful. Here, the situation of device selection COPRAS explained and up to date ranking is executed by method. Using the proposed method, the rank received is very found to be reliable [20]. In this manuscript, known as if-COPRAS method many with intuitively ambiguous information criteria decision making (Mcdm) difficulty solving problems we use the proportional assessment (COPRAS) method we provide in this manner, a to estimate scale weights a new formula has been developed, in which objective weights are from a different measurement system are calculated. For this, the new parameter difference and entropy measures there are some desirable ones that have been explored properties are also discussed. Complex proportionality assessment (COPRAS) by coefficient of gray number (COPRAS-g) methods complex proportionality assessment material selection using this article attempts to address the issues, different at the same time subject selection criteria and considering their relative importance takes these two methods rankings obtained using the past almost with those obtained by the researchers confirm. Of accepted methods feasibility and applicability two cases to prove time examples are illustrated .

4. RESULT AND DISCUSSION

TABLE 1. Information security controls



	DATA SET						
	Implementation time(C1)	Effectiveness(C2)	Risk (C3)	Budgetary constraints(C4)	Exploitation time(C5)	Maintenance cost(C6)	Mitigation time(C7)
IS Control 1	0.042	0.304	0.247	0.205	0.128	0.021	0.053
IS Control 2	0.529	0.414	0.499	0.527	0.435	0.307	0.36
IS Control 3	0.281	0.318	0.233	0.267	0.2	0.261	0.321
IS Control 4	0.13	0.205	0.19	0.083	0.182	0.236	0.149
IS Control 5	0.06	0.064	0.077	0.123	0.182	0.196	0.169

In the given table 1, we have information on seven information security controls (IS Controls) and their corresponding scores for various parameters. The following parameters were measured: C1: Duration of implementation C2: Efficiency C3: Risk C4: Financial limitations C5: Time for exploitation C6: Maintenance expenses, and C7: Time for mitigation .In this data set, each IS Control is assigned a score between 0 and 1 for each parameter. The scores represent the relative performance or characteristics of each control for the corresponding parameter. For example, Control 1 has an implementation time score of 0.042, indicating it has a relatively short implementation time compared to other controls. Similarly, Control 2 has a risk score of 0.499, suggesting it carries a higher risk compared to other controls.

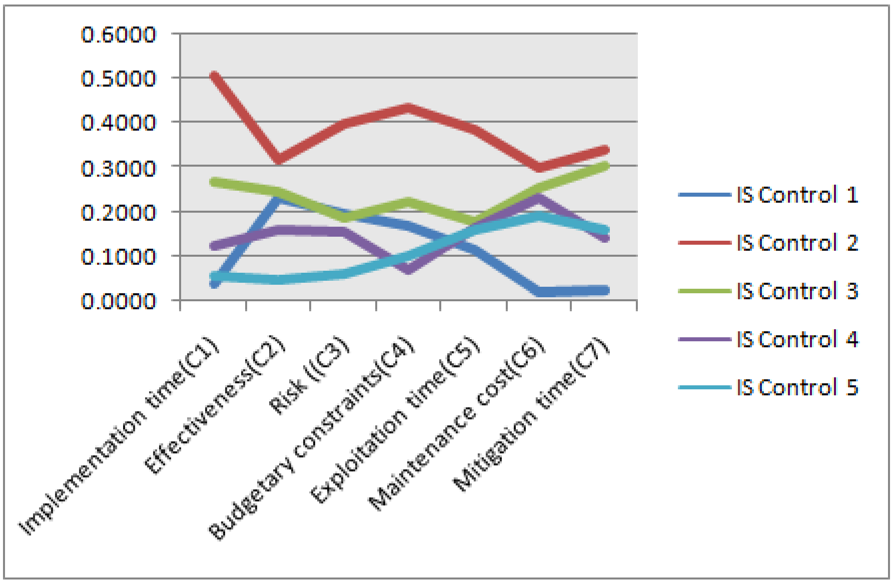
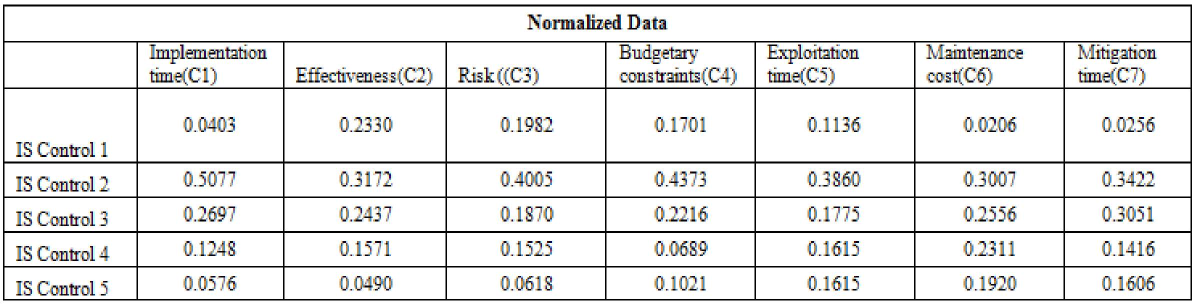


FIGURE 1. Information security controls

In the given figure 1, we have information on seven information security controls (IS Controls) and their corresponding scores for various parameters The following parameters were measured: C1: Duration of implementation C2: Efficiency C3: Risk C4: Financial limitations C5: Time for exploitation C6: Maintenance expenses, and C7: Time for mitigation .In this data set, each IS Control is assigned a score between 0 and 1 for each parameter. The scores represent the relative performance or characteristics of each control for the corresponding parameter. For example, Control 1 has an implementation time score of 0.042, indicating it has a relatively short implementation time compared to other controls. Similarly, Control 2 has a risk score of 0.499, suggesting it carries a higher risk compared to other controls.

TABLE 2. Normalized Data



Normalized Data							
	Implementation time(C1)	Effectiveness(C2)	Risk ((C3)	Budgetary constraints(C4)	Exploitation time(C5)	Maintenance cost(C6)	Mitigation time(C7)
IS Control 1	0.0403	0.2330	0.1982	0.1701	0.1136	0.0206	0.0256
IS Control 2	0.5077	0.3172	0.4005	0.4373	0.3860	0.3007	0.3422
IS Control 3	0.2697	0.2437	0.1870	0.2216	0.1775	0.2556	0.3051
IS Control 4	0.1248	0.1571	0.1525	0.0689	0.1615	0.2311	0.1416
IS Control 5	0.0576	0.0490	0.0618	0.1021	0.1615	0.1920	0.1606

The table 2 represents the normalized data for the seven information security controls (IS Controls) and their corresponding scores for various parameters. The following parameters were measured: C1: Duration of implementation C2: Efficiency C3: Risk C4: Financial limitations C5: Time for exploitation C6: Maintenance expenses, and C7: Time for mitigation. In this normalized data set, each IS Control is assigned a score between 0 and 1 for each parameter. The scores have been normalized to a scale of 0 to 1, indicating the relative performance or characteristics of each control for the corresponding parameter. The normalization process scales the values to allow for meaningful comparisons between controls across different parameters. For example, Control 1 has a normalized implementation time score of 0.0403, suggesting it has a relatively short implementation time compared to other controls. Similarly, Control 2 has a normalized risk score of 0.4005, indicating it carries a higher risk compared to other controls.

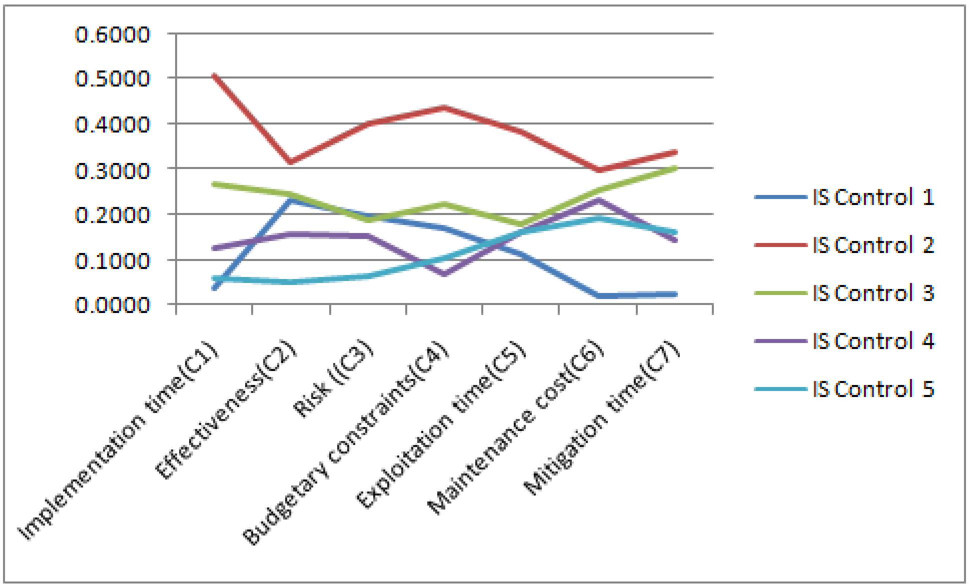
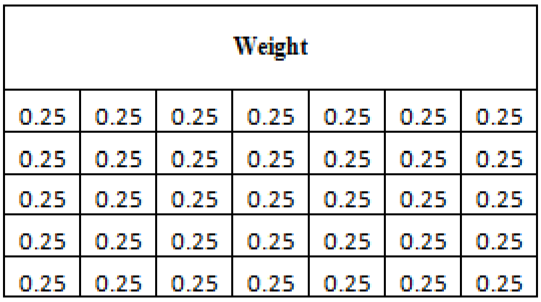


FIGURE 2. Normalized Data

The figure 2 represents the normalized data for the seven information security controls (IS Controls) and their corresponding scores for various parameters. The following parameters were measured: C1: Duration of implementation C2: Efficiency C3: Risk C4: Financial limitations C5: Time for exploitation C6: Maintenance expenses, and C7: Time for mitigation. In this normalized data set, each IS Control is assigned a score between 0 and 1 for each parameter. The scores have been normalized to a scale of 0 to 1, indicating the relative performance or characteristics of each control for the corresponding parameter. The normalization process scales the values to allow for meaningful comparisons between controls across different parameters. For example, Control 1 has a normalized implementation time score of 0.0403, suggesting it has a relatively short implementation time compared to other controls. Similarly, Control 2 has a normalized risk score of 0.4005, indicating it carries a higher risk compared to other controls.

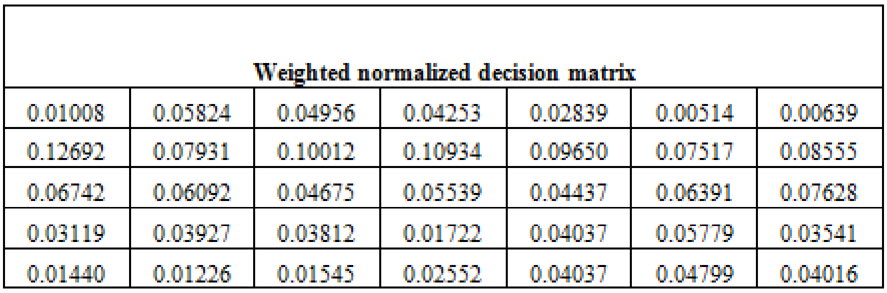
TABLE 3. Weight



Weight						
0.25	0.25	0.25	0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25	0.25	0.25	0.25
0.25	0.25	0.25	0.25	0.25	0.25	0.25

The table 3 provided appears to represent the weights assigned to each of the seven parameters (Implementation time, Effectiveness, Risk, Budgetary constraints, Exploitation time, Maintenance cost, and Mitigation time) for evaluating alternative values. The weight values determine the relative importance or significance of each parameter in the evaluation process. Each weight is set at 0.25, indicating that each parameter is equally important in the evaluation process. The alternative values for each parameter will be combined with these weights to calculate an overall evaluation score for each information security control.

TABLE 4. Weighted normalized decision matrix



Weighted normalized decision matrix						
0.01008	0.05824	0.04956	0.04253	0.02839	0.00514	0.00639
0.12692	0.07931	0.10012	0.10934	0.09650	0.07517	0.08555
0.06742	0.06092	0.04675	0.05539	0.04437	0.06391	0.07628
0.03119	0.03927	0.03812	0.01722	0.04037	0.05779	0.03541
0.01440	0.01226	0.01545	0.02552	0.04037	0.04799	0.04016

The table 4 provided appears to represent the weighted normalized decision matrix for evaluating alternative values for each information security control. The matrix combines the normalized scores for each parameter (Implementation time, Effectiveness, Risk, Budgetary constraints, Exploitation time, Maintenance cost, and Mitigation time) with the corresponding weights to calculate an overall evaluation score for each control. In this matrix, each cell represents the weighted and normalized score for a specific parameter for each IS Control. The values in the matrix are obtained by multiplying the normalized scores with the corresponding weights assigned to each parameter. The resulting scores represent the overall evaluation of each information security control based on the specified weights and normalized data. These evaluation scores can be used to compare and rank the controls based on their overall performance and suitability for the specific evaluation criteria.

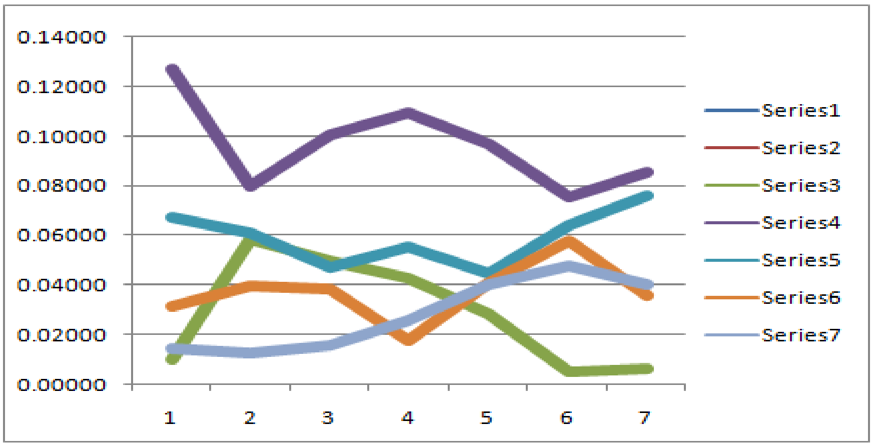
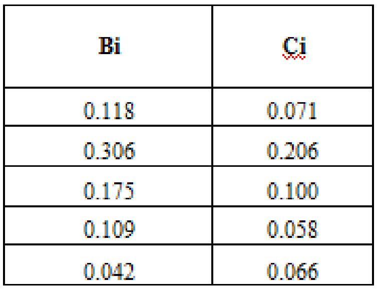


FIGURE 3. Weighted normalized decision matrix

The figure 3 appears to represent the weighted normalized decision matrix for evaluating alternative values for each information security control. The matrix combines the normalized scores for each parameter (Implementation time, Effectiveness, Risk, Budgetary constraints, Exploitation time, Maintenance cost, and Mitigation time) with the corresponding weights to calculate an overall evaluation score for each control. In this matrix, each cell represents the weighted and normalized score for a specific parameter for each IS Control. The values in the matrix are obtained by multiplying the normalized scores with the corresponding weights assigned to each parameter. The resulting scores represent the overall evaluation of each information security control based on the specified weights and normalized data. These evaluation scores can be used to compare and rank the controls based on their overall performance and suitability for the specific evaluation criteria.

TABLE 5. Bi and Ci



Bi	Ci
0.118	0.071
0.306	0.206
0.175	0.100
0.109	0.058
0.042	0.066

In this table 5 represents a two-column matrix with the values of Bi and Ci for five different elements or entities. Each row in the matrix represents an element or entity, and the columns Bi and Ci represent the corresponding values assigned to each element. The meaning and context of these values would depend on the specific application or analysis being conducted. These values may represent different attributes, characteristics, or performance metrics of the elements being evaluated.

TABLE 6. Bi, Ci and **Min(Ci)/Ci**

Bi	Ci	Min(Ci)/Ci
0.118	0.071	0.8120
0.306	0.206	0.2798
0.175	0.100	0.5773
0.109	0.058	1.0000
0.042	0.066	0.8741

In this table 6 each row in the matrix represents an element or entity, and the columns Bi, Ci, and Min(Ci)/Ci represent the corresponding values assigned to each element. The specific meaning and context of these values will depend on the application or analysis being conducted. Here's a brief explanation of each column: Bi: Represents the value of Bi for each element. Ci: Represents the value of Ci for each element. Min(Ci)/Ci: Represents the result of the calculation Min(Ci)/Ci for each element. The value in the Min(Ci)/Ci column is derived by dividing each Ci value by the minimum Ci value. Min(Ci) is the minimum value of the Ci column in this computation.

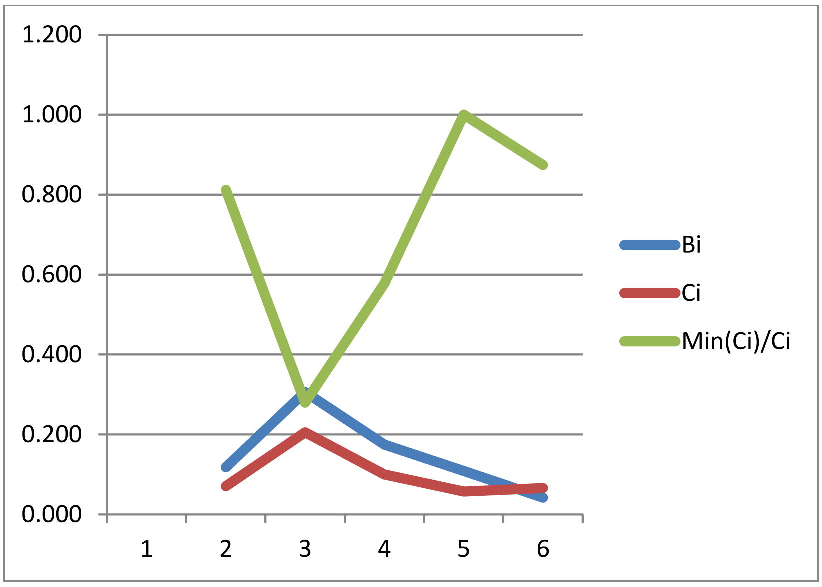


FIGURE 4. Bi, Ci and Min(Ci)/Ci

Table 7. Qi, Ui and Ui

Qi	Ui	Ui
0.2325	67.21752	0.67218
0.3458	100	1
0.2566	74.18436	0.74184
0.2497	72.20199	0.72202
0.1654	47.84019	0.4784

The table 7 represents a three-column matrix with the values of Qi, Ui, and Ui for five different elements or entities. Each row in the matrix represents an element or entity, and the columns Qi, Ui, and Ui represent the corresponding values assigned to each element. The specific meaning and context of these values will depend on the application or analysis being conducted. Here's a brief explanation of each column: Qi: Represents the value of Qi for each element. Ui: Represents the value of Ui for each element. Ui (percentage): It appears that the third column is a duplicate of the Ui column. The values are the same as those in the Ui column.

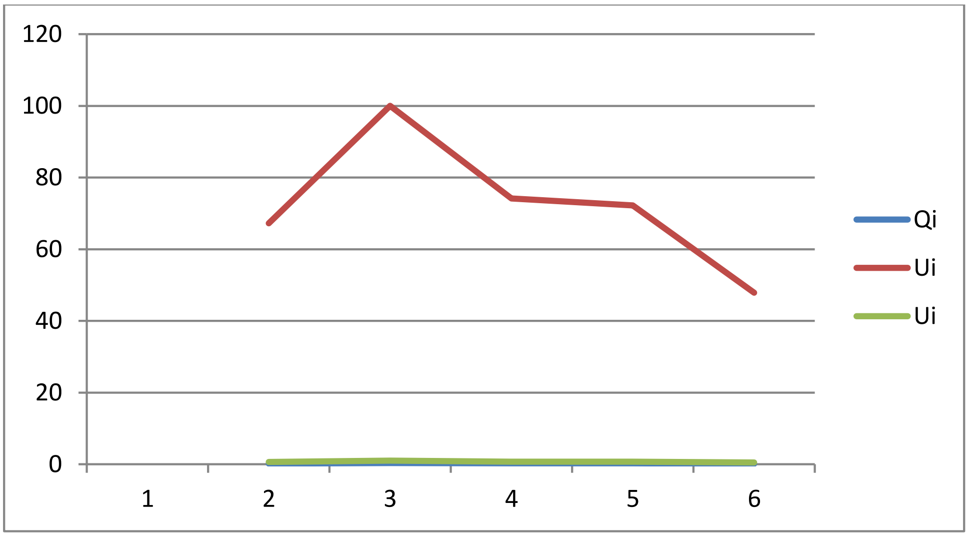


FIGURE 5. Qi, Ui and Ui

The figure represents a three-column matrix with the values of Qi, Ui, and Ui for five different elements or entities. Each row in the matrix represents an element or entity, and the columns Qi, Ui, and Ui represent the corresponding values assigned to each element. The specific meaning and context of these values will depend on the application or analysis being conducted. Here's a brief explanation of each column: Qi: Represents the value of Qi for each element. Ui: Represents the value of Ui for each element. Ui (percentage): It appears that the third column is a duplicate of the Ui column. The values are the same as those in the Ui column.

TABLE 8. Rank

	Rank
IS Control 1	4
IS Control 2	1
IS Control 3	2
IS Control 4	3
IS Control 5	5

The table 8 represents the ranking of five information security controls (IS Controls) based on their performance or evaluation score. The "Rank" column shows the ranking order for each IS Control, where 1 indicates the highest rank, 2 the second highest, and so on. Based on the ranking, Control 2 received the highest rank (1), indicating that it performed the best among all the controls. Control 3 received the second-highest rank (2), Control 4 received the third-highest rank (3), Control 1 received the fourth-highest rank (4), and Control 5 received the lowest rank (5). The ranking can be based on the evaluation scores obtained from the weighted normalized decision matrix or any other evaluation method used to assess the performance of the information security controls.

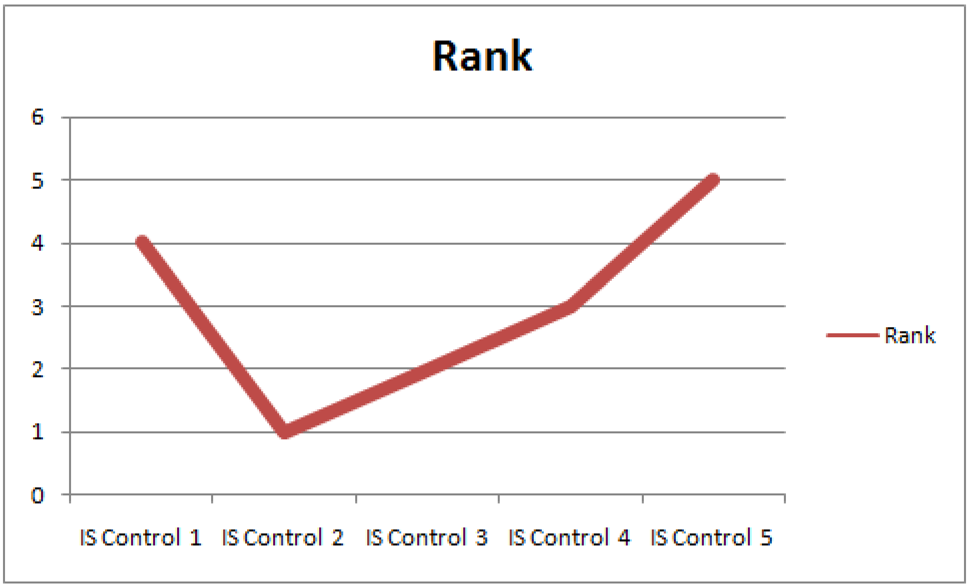


FIGURE 6. Rank

The figure 6 represents the ranking of five information security controls (IS Controls) based on their performance or evaluation score. The "Rank" column shows the ranking order for each IS Control, where 1 indicates the highest rank, 2 the second highest, and so on. Based on the ranking, Control 2 received the highest rank (1), indicating that it performed the best among all the controls. Control 3 received the second-highest rank (2), Control 4 received the third-highest rank (3), Control 1 received the fourth-highest rank (4), and Control 5 received the lowest rank (5). The ranking can be based on the evaluation scores obtained from the weighted normalized decision matrix or any other evaluation method used to assess the performance of the information security controls.

4. CONCLUSION

Organisations can benefit from accurate ISC selection and evaluation while conducting risk assessment exercises for cloud networks linked with networks. Pairwise comparisons of the expert opinions and the evaluation criteria were made using the COPRAS. The results of the aforementioned comparisons were then included in a matrix with the advice of experts and were reciprocal. Numerous aspects related to the organisation itself, such as the deployed information security system and the environment, affected the prioritisation of the information security controls and the choice of the optimal one. Organisations look for pertinent solutions to install suitable, affordable, and effective information security controls which may boost the reliability of the system when information security best practises have too many information security controls. Based on the elements discovered during the literature review, the proposed model was created. Many information security professionals optimised this model for the choice of information security controls. The model includes seven criteria for ranking and evaluating information security policies. Decision-makers' opinions were given COPRAS numbers, which were then assigned to them. For assessments, a thorough analysis was done to explain the synthetic priority weights for each criterion. Multi-criteria decision making techniques were employed to collect the data for this investigation. The results of this application demonstrate how successfully the suggested model performed. This paper included the ranking's results as well.

REFERANCE

[1]. Sharma, Mahak, Ruchita Gupta, and Padmanav Acharya. "Prioritizing the critical factors of cloud computing adoption using multi-criteria decision-making techniques." *Global Business Review* 21, no. 1 (2020): 142-161.

[2]. Youssef, Ahmed E. "An integrated MCDM approach for cloud service selection based on TOPSIS and BWM." *IEEE Access* 8 (2020): 71851-71865.

[3]. Neeraj, Major Singh Goraya, and Damanpreet Singh. "A comparative analysis of prominently used MCDM methods in cloud environment." *The Journal of Supercomputing* 77 (2021): 3422-3449.

[4]. Priyadarshinee, Pragati, Manoj Kumar Jha, Rakesh D. Raut, Manoj Govind Kharat, and Sachin S. Kamble. "To identify the critical success factors for cloud computing adoption by MCDM technique." *International Journal of Business Information Systems* 24, no. 4 (2017): 469-510.

[5]. Kumar, Rakesh Ranjan, Siba Mishra, and Chiranjeev Kumar. "Prioritizing the solution of cloud service selection using integrated MCDM methods under Fuzzy environment." *The Journal of Supercomputing* 73 (2017): 4652-4682.

[6]. Sharma, Mahak, and Rajat Sehrawat. "A hybrid multi-criteria decision-making method for cloud adoption: Evidence from the healthcare sector." *Technology in Society* 61 (2020): 101258.

[7]. Kumar, Rakesh Ranjan, Binita Kumari, and Chiranjeev Kumar. "CCS-OSSR: a framework based on hybrid MCDM for optimal service selection and ranking of cloud computing services." *Cluster Computing* 24, no. 2 (2021): 867-883.

[8]. Trabay, Doaa, Azezza Asem, Ibrahim El-Henawy, and Wajeb Gharibi. "A hybrid technique for evaluating the trust of cloud services." *International Journal of Information Technology* 13 (2021): 687-695.

[9]. Mostafa, Ahmed M. "An MCDM approach for cloud computing service selection based on best-only method." *IEEE Access* 9 (2021): 155072-155086.

[10]. Gyani, Jayadev, Ahsan Ahmed, and Mohd Anul Haq. "MCDM and various prioritization methods in AHP for CSS: A comprehensive review." *IEEE Access* 10 (2022): 33492-33511.

[11]. Al-Jabri, Ibrahim M., Eid Mustafa I, and M. Sadiq Sohail. "A group decision-making method for selecting cloud computing service model." *International Journal of Advanced Computer Science and Applications (IJACSA)* 9, no. 1 (2018): 449-456.

[12]. Tanoumand, Neda, Dicle Yagmur Ozdemir, Kemal Kilic, and Faran Ahmed. "Selecting cloud computing service provider with fuzzy AHP." In *2017 IEEE international conference on fuzzy systems (FUZZ-IEEE)*, pp. 1-5. IEEE, 2017.

[13]. Sohaib, Osama, and Mohsen Naderpour. "Decision making on adoption of cloud computing in e-commerce using fuzzy TOPSIS." In *2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, pp. 1-6. IEEE, 2017.

[14]. Kumar, Rakesh Ranjan, and Chiranjeev Kumar. "A multi criteria decision making method for cloud service selection and ranking." *International Journal of Ambient Computing and Intelligence (IJACI)* 9, no. 3 (2018): 1-14.

[15]. Maroc, Sarah, and Jian Biao Zhang. "Cloud services security-driven evaluation for multiple tenants." *Cluster Computing* 24 (2021): 1103-1121.

[16]. Huang, Chi-Yo, Pei-Chu Hsu, and Gwo-Hshiung Tzeng. "Evaluating cloud computing based telecommunications service quality enhancement by using a new hybrid MCDM model." In *Intelligent Decision Technologies: Proceedings of the 4th International Conference on Intelligent Decision Technologies (IDT´ 2012)-Volume 1*, pp. 519-536. Springer Berlin Heidelberg, 2012.

[17]. Chakraborty, Biswanath, and Santanu Das. "Introducing a new supply chain management concept by hybridizing topsis, IoT and cloud computing." *Journal of The Institution of Engineers (India): Series C* 102, no. 1 (2021): 109-119.

[18]. Nawaz, Falak, Mehdi Rajabi Asadabadi, Naeem Khalid Janjua, Omar Khadeer Hussain, Elizabeth Chang, and Morteza Saberi. "An MCDM method for cloud service selection using a Markov chain and the best-worst method." *Knowledge-Based Systems* 159 (2018): 120-131.

[19]. Eisa, Mona, Muhammad Younas, Kashinath Basu, and Irfan Awan. "Modelling and simulation of QoS-aware service selection in cloud computing." *Simulation Modelling Practice and Theory* 103 (2020): 102108.

[20]. Büyüközkan, Gülçin, Fethullah Göçer, and Orhan Feyzioğlu. "Cloud computing technology selection based on interval-valued intuitionistic fuzzy MCDM methods." *Soft Computing* 22, no. 15 (2018): 5091-5114.

[21]. Raut, Rakesh D., Bhaskar B. Gardas, Manoj Kumar Jha, and Pragati Priyadarshinee. "Examining the critical success factors of cloud computing adoption in the MSMEs by using ISM model." *The Journal of High Technology Management Research* 28, no. 2 (2017): 125-141.

[22]. Sun, Le, Jiangang Ma, Yanchun Zhang, Hai Dong, and Farookh Khadeer Hussain. "Cloud-FuSeR: Fuzzy ontology and MCDM based cloud service selection." *Future Generation Computer Systems* 57 (2016): 42-55.

[23]. Tariq, Muhammad Imran, Shakeel Ahmed, Nisar Ahmed Memon, Shahzadi Tayyaba, Muhammad Waseem Ashraf, Mohsin Nazir, Akhtar Hussain, Valentina Emilia Balas, and Marius M. Balas. "Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks." *Sensors* 20, no. 5 (2020): 1310.

[24]. Thasni, T., C. Kalaiarasan, and K. A. Venkatesh. "Cloud service provider selection using fuzzy TOPSIS." In *2020 IEEE international conference for innovation in technology (INOCON)*, pp. 1-5. IEEE, 2020.

[25]. Jatoth, Chandrashekar, G. R. Gangadharan, Ugo Fiore, and Rajkumar Buyya. "SELCLOUD: a hybrid multi-criteria decision-making model for selection of cloud services." *Soft Computing* 23 (2019): 4701-4715.

[26]. Meesariganda, Bhaskara Raju, and Alessio Ishizaka. "Mapping verbal AHP scale to numerical scale for cloud computing strategy selection." *Applied Soft Computing* 53 (2017): 111-118.