International Journal of Mathematical, Engineering and Management Sciences
Vol. 8, No. 1, 78-93, 2023
https://doi.org/10.33889/IJMEMS.2023.8.1.005

Risk Managed Cloud Adoption: An ANP Approach

Shikha Gupta
University Institute of Engineering (CSE),
Chandigarh University, Punjab, India.
E-mail: shikha.g.206@gmail.com

Subhendu Kumar Pani
Krupajal Engineering College,
Biju Patnaik University of Technology, Odisha, India.
E-mail: pani.subhendu@gmail.com

Kamalakanta Muduli
Papua New Guinea University of Technology, Papua New Guinea.
Corresponding author: kamalakantam@gmail.com

Arti Vaish
School of Engineering and Technology,
Sushant University, Gurugram, India.
E-mail: vaisharti@gmail.com

Anil Kumar
Supply Chain and Business Analytics,
London Metropolitan University, United Kingdom (UK).
E-mail: anilror@gmail.com

(Received on March 23, 2022; Accepted on September 17, 2022)

Abstract
To meet the ever-increasing demand for offering a sustainable environment, organizations are beginning to aim for cloud adoption and the migration of their IT infrastructure and operations to the cloud, utilizing various cloud-based technologies. However, cloud adoption has been impeded by the risk of being exposed as a result of a variety of concerns, including performance, security, and privacy concerns, as well as vulnerabilities and data portability. As a result, this study was carried out to investigate and analyse a variety of risks that come with cloud computing adoption by estimating the impact and frequency of these hazards. In this study, the Analytical Network Process (ANP) is used to prioritise these hazards. Prioritization of these risks based on their influence on cloud adoption may be useful for organizations in building a corrective action plan. According to their negative influence on cloud adoption, "business continuity and recovery planning" and "poor availability of services" are shown to be the most prominent hazards. This research also found that the two most common dangers encountered by cloud adopters in India are "poor availability of services" and "slow response rate."

Keywords- Cloud, Sustainability, Risk, Analytical network process, Multi-criteria decision making, Cloud adoption.

1. Introduction

Cloud computing has transformed the landscape of information technology as a result of its ability to change the entire computing paradigm away from traditional on-premise computing and toward a rent-per-use approach (Tulasi, 2009). Those organizations that are attempting to reduce their information technology expenditures or who wish to shift their investment from information technology to core business processes to create a more sustainable organizational environment have discovered that utilizing economically viable

cloud options can be beneficial to their operations (Buyya et al., 2008). Organizations can shift their resources away from information technology (IT) and into other activities that contribute to the advancement of their core business as a result of cloud computing, which allows them to employ IT services on a pay-per-use basis (Son et al., 2011; Gill and Buyya, 2018). Above and beyond these benefits, cloud computing-enabled practices have the potential to improve resource utilization, which in turn can cut operating and electrical expenses, making a substantial contribution to the long-term profitability of the organization, among other things (Gill and Buyya, 2018). When a renewable energy source is used in conjunction with cloud computing hardware, it is feasible to issue "green" certifications to cloud computing services and applications, as well as to cloud computing hardware (Briscoe and Marinos, 2009). It is possible to reduce environmental harm by only using hardware when it is necessary, which can help to avoid a catastrophic environmental catastrophe. Aside from that, as previously said, the usage of cloud computing technology has the potential to drastically reduce carbon emissions, ultimately leading to a reduction in the accumulation of greenhouse gases in the environment.

Although flexibility and cost-effectiveness have always been the key drivers for businesses, cloud computing has gained prominence because of a variety of features like cost-effectiveness, availability, agility, extensibility, scalability, and elasticity (Singh and Misra, 2021). Although cloud adoption promises and provides many benefits for businesses, several hazards might result in complications associated with cloud adoption, which a firm considering cloud migration should be aware of before proceeding (Buyya and Gill, 2018). While more and more organizations are being drawn to the cloud as a result of its sustainability, many organizations are concerned about issues such as data availability, privacy, security, and performance, as well as lack of compliance, among others, when it comes to cloud adoption (Chow et al., 2009; Stinchcombe, 2009). Therefore, research that investigates the multiple hazards connected with cloud adoption and offers a framework that can be used as a guideline for organizations on their journey toward risk-managed cloud adoption is becoming increasingly important. This research was conducted in two stages to investigate the hazards associated with excessive usage of cloud computing in general and the suggested use of the analytic network process (ANP) to assess these risks and rank them depending on their severity. The following are the research objectives for this study:

(i) To establish a link between business needs and cloud-related concerns.
(ii) To estimate the loss exposures associated with cloud adoption by investigating the risk impact of cloud adoption.
(iii) To provide information to businesses considering cloud adoption and to help them make decisions based on a variety of parameters.

The following is the structure of the paper: Section 1 is devoted to the exposition of cloud computing ideas and business requirements. Section 2 comprises a review of the literature on cloud adoption and organizational sustainability, which is divided into two parts. Section 3 discusses the risks connected with the introduction of cloud computing. A special emphasis is placed in Section 4 on the Analytical Network Process-based technique that was employed in the study for the solution of multi-criteria decision issues. Section 5 contains the risk matrix that was generated. The findings of the investigation are discussed in Section 6. Section 7 presents a conclusion as well as a vision for the future.

2. Review of the Literature

"Cloud computing," according to the National Institute of Standards and Technology, is a "concept that allows demand-based access through the network to a shared pool of computational services such as networks, servers, and applications that can be quickly demanded or issued with little administrative exertion or interaction with the service provider." Researchers have each developed their method of

analyzing and defining cloud computing. According to (Saaty and Vargas, 2013), cloud computing has a variety of meanings that vary depending on the characteristics of the cloud. The definition used in this study would be that of (Awaysheh et al., 2021), which regards cloud computing as a broad skeleton that serves as an enabler for providing computing resources as a service to the intended customers. These diverse computing resources may include resources such as hardware, software, and even infrastructure, all of which are available on demand and at a fair price, depending on the situation. Services such as the following can be obtained through the internet: Using Software as a Service (SaaS), an implementation can be delivered as a web-based service. This eliminates the need for users to install software on their computers, as well as the effort and money associated with maintaining software because it is provided on-demand. It is possible to create applications using Platform as a Service (PaaS), which is dependent on the size of the hardware resources available for the execution of services, and this is done transparently. Cloud computing, also known as Infrastructure as a Service, is a massive collection of computing resources capable of processing large amounts of data. Cloud computing is currently the most talked-about concept in both the business and academic worlds. Figure 1 shows the different cloud services and available deployment strategies, as well as their prices.

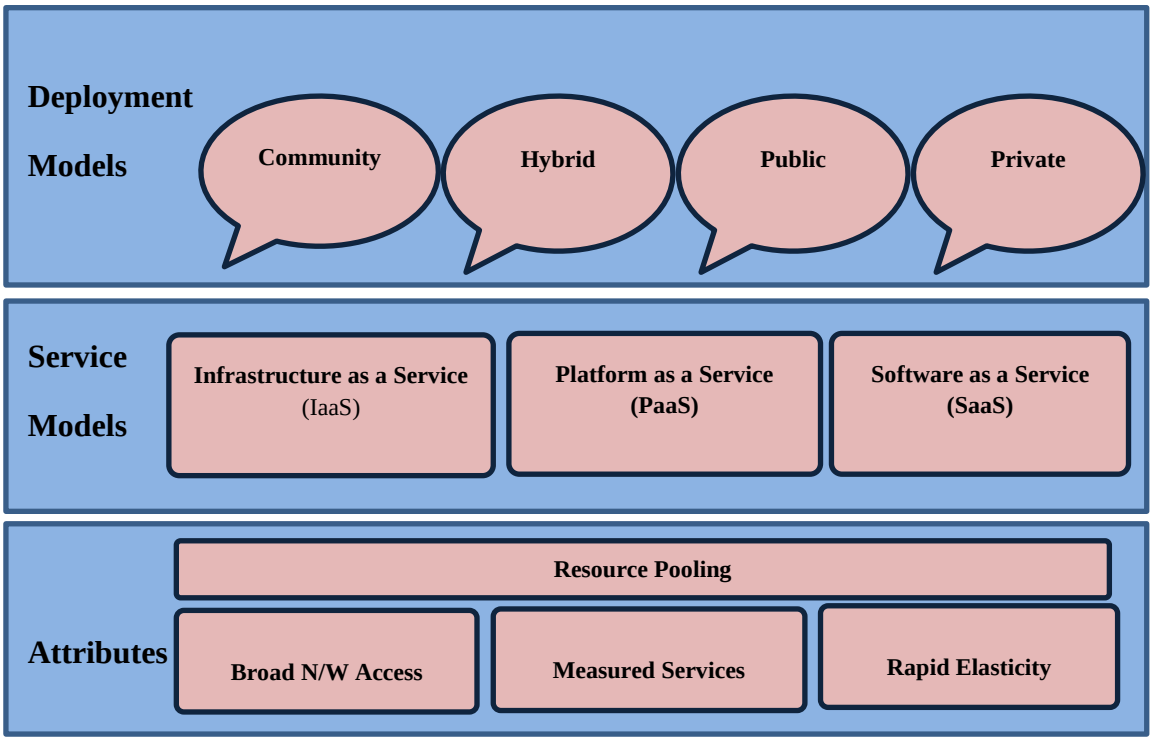

Figure 1. Cloud services and deployment strategies.

Cloud computing has sparked significant concern and study in the information technology industry due to its rapid proliferation, ubiquitous nature, and pervasive potential. Researchers investigated the efficacy and strategy implementation of cloud adoption, as well as challenges and concerns such as security, performance, and integration. They also looked into cloud interoperability solutions, which were all explored and disputed in the cloud computing adoption research (Kim et al., 2009). Many studies have also been conducted to analyze the accomplishments or drawbacks of cloud computing adoption, as well as the

success or failure of cloud computing adoption in general. The potential of cloud computing to dynamically extend resources in response to changes in the company's operations, in particular, is a big draw for business owners (Radu, 2017; Dewangan et al., 2020; Liu et al., 2021). One of the environmental benefits of cloud computing is the advancement of energy-saving techniques as well as a reduction in the amount of equipment required (Radu, 2017).

2.1 Constructing a Link Between Business Requirements and Cloud-Related Concerns

Even though many characteristics of cloud computing are attractive to businesses, several risks must be addressed to establish a relationship between business requirements and cloud goods. Some characteristics of cloud computing are still up in the air. It is vital for firms that do not rely on information technology as a major business function to become educated on the many difficulties and hazards involved with cloud computing adoption. Even the cloud service provider's service level agreements (SLA) contain ambiguous words such as "we deliver quality services," which do not provide any specifics on what they mean by this statement. A firm must understand how to quantify the phrase "availability" before it can ensure that the availability of services and data is one of the features of cloud adoption. Otherwise, once cloud adoption has occurred, the feature itself becomes a problem.

2.2 Risks Associated with the Adoption of Cloud Computing

Although cloud computing is becoming increasingly popular among businesses, there are several issues or threats associated with cloud adoption that, if not managed properly, could result in potential losses rather than the anticipated benefits. Performance risks, security and privacy risks, and risks associated with the service environment are all examples of hazards that can arise. There have been a lot of studies done to find and look at performance-related risks. These risks could be anything from concerns about data and processes being available to a lack of help to a slow response time from the cloud service provider.

We are focusing our efforts on companies that do not have an IT core business. It is only when a corporation adopting the cloud is aware of performance-related issues and can handle these risks during the cloud adoption process that cloud adoption may be advantageous and achieve the desired benefits. In the alternative, the company that adopts cloud computing may experience possible losses as a result of business interruption. To ensure that business operations continue uninterrupted, data and services must remain available whenever they are needed and without encountering any unexpected or undesired delays. Information security, privacy, and availability are all important factors when deploying cloud computing services. Cloud adoption is fraught with perils, according to the experts, and one of the most significant is data security and privacy concerns, which they say should be taken into consideration. Businesses can suffer large financial losses as a result of the intended or unintentional exposure, modification, or theft of critical information and operations. The risks posed by the service environment include having to follow rules and regulations both inside and outside of your country, having the ability to move your data, and other things about the service environment.

According to the cloud adoption framework, Table 1 outlines the multiple hazards involved with cloud adoption and how to mitigate them. When deciding whether or not to use the cloud, cost and risk are important considerations. The most crucial aspect is an inclination, which is triggered by awareness. However, these variables cannot be compared because, no matter how unequal the cost vs. risk is, no one will choose cloud if the risk is excessively high.

2.2.1 Performance Assurance Risks

Availability/business continuity, unavailability of services, and sluggish reaction time have all been cited by various researchers (Kostyuchenko, 2021). In cloud computing, performance risks include the loss of

important skills or the development of incorrect skills, inexperienced workers, and a lack of organizational learning. Performance hazards are a major problem for cloud adoption since cloud computing relies on the quality and availability of the Internet connection and the cloud service itself, resulting in worries about availability (stated as a percentage of annual uptime) and service issues, as well as business continuity concerns due to Internet unavailability, connection instability, or CSP outages. The term availability can be defined as a cloud property that allows users to access services and data whenever they want, i.e., delivering services at the moment of request without any unexpected or unwelcome delays. In contracts and SLAs, availability is also defined as the ratio or percentage of time that the system was available (i.e., "operation time"), excluding maintenance periods, with non-availability referred to as downtime. Furthermore, latency, or the time it takes for data packets to be transferred, is a concern, particularly for time-critical applications like those used in financial markets and international trading. Cloud Computing service delays and disruptions have occurred in the past. Even inadvertent downtime can occur owing to technological faults or natural calamities. When a cloud service provider is attacked, service non-availability or outages may result in major commercial consequences. When a service provider files for bankruptcy or is bought by new management, disaster recovery and business continuity planning become necessary. When users are unable to log on to the service, they lose access to their data, which is held on the Cloud Computing provider's remote servers.

2.2.2 Risks to Data Security and Privacy

Companies are moving to the cloud for many reasons, but ignorant and haphazard cloud decisions can lead to insecurity. The importance of quantifying IT security incidents as an element in risk management is emphasized. The most important concern for cloud computing, according to several studies, is data security and privacy risk. Among the challenges that lead to data security, integrity, and confidentiality are proper identity management, security incident management and reporting, auditing, security verifications, proper authorizations and authentications, data transfer protection, and data backup mechanism. Maintaining the privacy of users' data from unintentional disclosure, as well as the legalities surrounding data protection, confidentiality, copyright, and audits, are all major concerns. When it comes to cloud adoption, system vulnerability must be addressed with extreme caution. Companies might suffer significant financial and goodwill damages as a result of data loss or leaking.

2.2.3 Risks to Service Environment

One of the most significant aspects of cloud adoption is the service environment. With the influence of multiple country authorities and industries across borders, rules and regulations about data storage, confidentiality, and disclosure alter with boundaries. As a result, ensuring compliance with local, regional, and worldwide legislative and legal obligations could be a stumbling block for cloud adoption. One of the challenges with cloud computing is that providers' servers may be located in several countries, causing compliance and data privacy issues. Some countries have liberal norms and legislation, while others have stringent restrictions on information transfer beyond the user's territory. The majority of the time, businesses are ignorant of where their data is stored. Data portability is another major service issue that must be treated with caution. The following are the risks associated with cloud adoption, as listed in Table 1.

Various Risks of Cloud Adoption: The various risks of cloud adoption from the cloud adoption framework as taken from are listed below in Table 1.

Risk Management Plotting: The study aims at analyzing the severity and frequency of all the risks in the cloud adoption framework through the risk matrix method as shown in Figure 2.

Table 1. Various risk components of cloud adoption.

Performance Assurance	AS: Poor Availability of Services	Uptime is defined as Available Time – (Downtime – Allowable Downtime which can be considered as the total number of available measurable time in hours, minutes, or seconds for billing Downtime which is allowed is only for predefined or agreed jobs like maintenance already scheduled and informed
	RT: Slow Response Time	Percentage of successful requests
		Percentage of timely service provisioning requests
	SR: Inadequate Supporting Resources	support staff for training, maintenance
	BCRP: Business Continuity and Recovery Planning	Business continuity during a natural disaster or man-made events that have an impact on the availability of IT infrastructure or software systems.
Data Security & Privacy	AA: Authentication & Authorization	Verification of the claimed identity and various permissions assigned for access and use of resources.
	DTP: Data Transmission Protection	Protecting data during transfer within the cloud provider's proprietary cloud, outside that cloud
	SIMR: Security Incident Management & Reporting	Managing security incidents through developing processes for detection, reporting, assessment, responses, dealing with, and creating feedback on security incidents.
	LMSI: Logging & Monitoring of Security Incidents	Monitoring and logging data records of operations and use
	ASV: Audit & Security Verification	Assuring that the cloud service provider meets particular criteria of interest to the cloud service customer
	DURDL: Data Use, Retention & Disclosure Limitation	policy for any intended use and disclosure of cloud service customer primary and derived data
	ACC: Accountability	Documentation of appropriate steps to ensure data protection
	DPM: Data Backup Mechanism	Disclosure of Data Backup Methods, Frequency, Retention Time, Generations etc.
Service Environment	DP: Data Portability	Ability to easily transfer data from one system to another without being required to re-enter data.
	PPM: Payment & Penalty Models	Information on when and how payment is to be made and also the provisions for obtaining service credit payments for outages.
	LNCA: List of Non-Covered Activities	Documentation of services not offered or covered in the contract
	ISS: Industry Specific Standards	Documentation of standards specific to the particular industry the client company belongs to
	RC: Regulatory Compliance	Compliance with data protection law

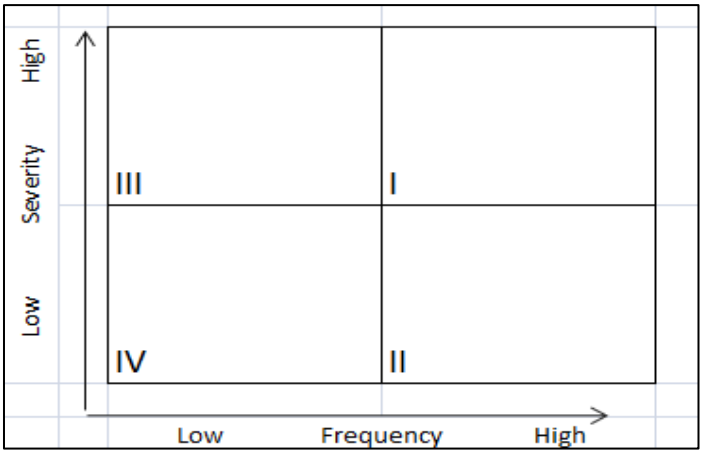

Figure 2. Risk matrix.

Region I: High frequency and High impact (severity) risks are placed here; this is the region of Risk Avoidance.
Region II: High frequency and Low impact risks are placed here; this is the region of Risk Mitigation.
Region III: Low frequency and High impact risks are placed here; this is the region of Risk Transference.
Region IV: Low frequency and Low impact risks are placed here; this is the region of Risk Acceptance.

3. Solution Methodology

The ANP technique, a multi-criteria decision-making (MCDM) technique, was used in this study to analyze and rate the hazards associated with cloud adoption in terms of their severity. In the real world, this MCDM strategy is widely used to deal with a wide range of real-world problems because it analyses intricate and interconnected interactions between option elements and has the capability of applying both quantitative and qualitative aspects at the same time (Muduli and Barve, 2013b; Biswal et al., 2019; Kheybari et al., 2020). Methods such as pair-wise comparison, Analytic Hierarchy Process (AHP), and Structural Equation Modelling (SEM) can be discovered in the literature and used to accomplish tasks that are comparable to those performed by ANP. In contrast to pair-wise comparison which is incapable of capturing interrelationships, ANP can do so (Raj et al., 2010; Muduli and Barve, 2013a). In structural equation modeling (SEM), as opposed to mining the data to generate a model, the theory drives the construction and specifications of the model. This is in contrast to traditional modeling, in which a model is developed by mining the data (Kline, 1998). Also, structural equation modeling needs a large sample size because the accuracy of estimates is related to the size of the sample (Muduli and Barve, 2013b). Unlike the Analytic Hierarchy Process, which only considers the relationships between levels of a hierarchical organization (Muduli, and Barve, 2015), the Analytic Network Process takes into account the relationships between levels of a hierarchical organization. Because of the interplay and dependence of higher-level components on lower-level attributes that characterize many of them, it is hard to organize choice dilemmas hierarchically (Biswal et al., 2017; Sorourkhah, 2022). Instead of having a hierarchical representation like AHP, ANP is represented as a network of links as a result of this development (Satty and Varges, 2006). ANP is well suited for solving MCDM issues where the criteria are nonlinearly related to one another. ANP is the first mathematical theory to be founded on a system of systematic feedback. As shown in Figure 3, the problems solved using ANP are distinct from AHP problems in that the problem is composed of criteria and sub-criteria that have inter and inner dependencies, and the entire problem does not need to be described as a levelled architecture to be solved. Clusters, components, nodes, or criteria, as well as elements or sub-criteria inside these clusters, make up a network structure.

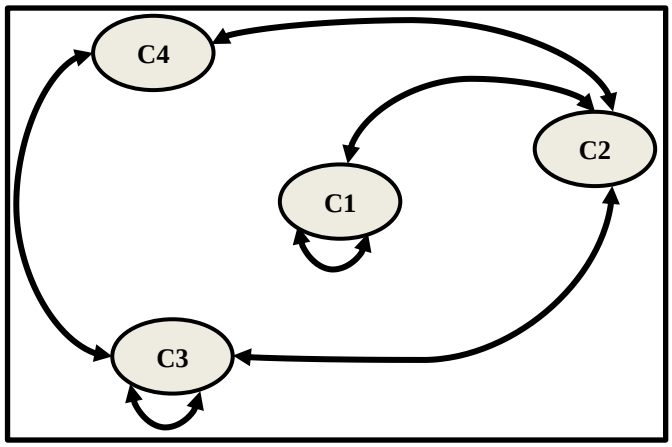

Figure 3. Cluster and dependency in a network for decision-making.

The ANP process is divided into many steps that are mentioned and explained below-

Step 1: Creating Network: Specifying Criteria, Sub Criteria

By constructing a network of its most critical components, ANP starts from the very beginning with a precise specification of the problem at hand. Eventually, nodes are formed when the higher-level parts of the network, known as clusters, are fragmented into sub-elements, which are in turn subdivided into sub-elements, and so on. As depicted in Figure 4, the authors have already begun to construct the network necessary for this phase.

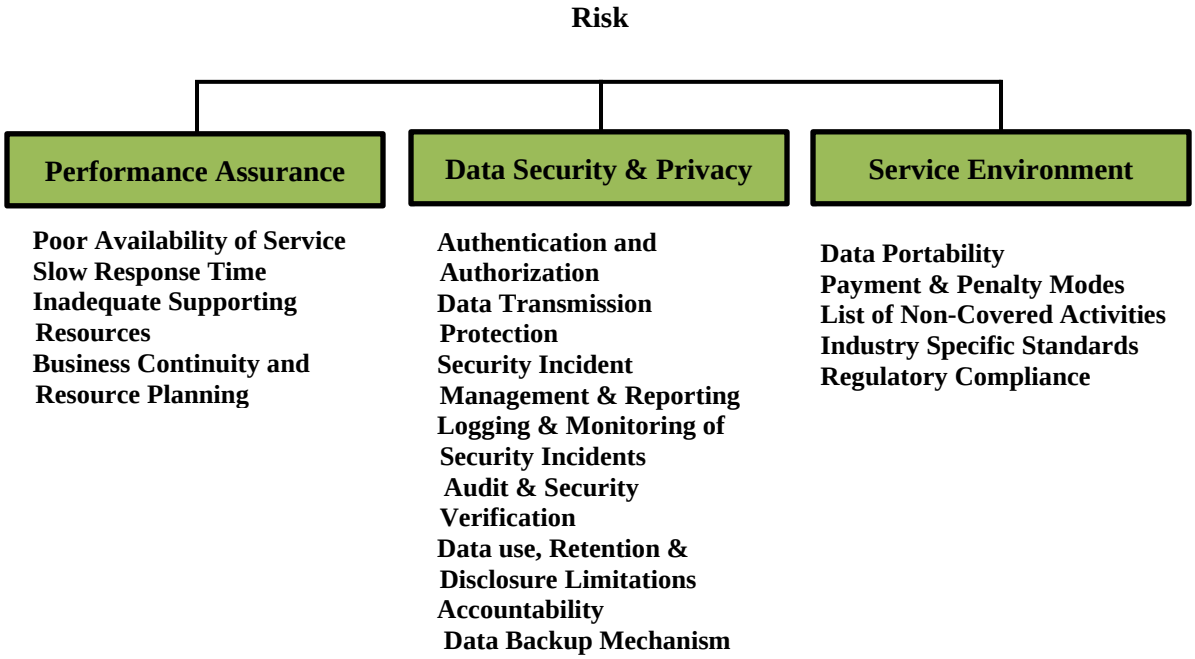

Figure 4. Risk management framework of cloud adoption.

Step 2: Pairwise Comparisons

Having constructed the network, the following step is to create a comparison matrix of pairwise comparisons to use in the network. This step evaluates the relationships between decision items inside the cluster as well as between decision elements in other clusters as well as between decision elements at other levels. Following the recommendations of (Muduli and Barve, 2013a), a scale of 1-9 is used for comparison, with 1 denoting equal importance and 9 denoting great importance (Table 2).

Table 2. Scale for pair-wise comparisons.

Scales for importance	Importance Intensity Numbers	Reciprocal Numbers
Equally important (EQI)	1	1/2
Moderately important (MI)	3	1/3
Strong or essential important (SI)	5	1/5
Very Strong or Demonstrated important (DI)	7	1/7
Extreme important (EXI)	9	1/9
Intermediate values (IV)	2,4,6,8	1/2,1/4,1/61/8

In the matrix a_{ij} (as in Table 2) represents the value after comparing an element in i^{th} row with an element in j^{th} column and diagonal value a_{ji} will represent the reciprocal of a_{ij} i.e. ;

$a_{ji} = 1 / a_{ij}$. (1)

All the diagonal values represent the relation of an element with itself, which is 1. The entire ANP process has been carried out by super Decisions software.

The relationship between Performance assurance, data security and privacy and service environment with Risk is depicted in Figure 5.

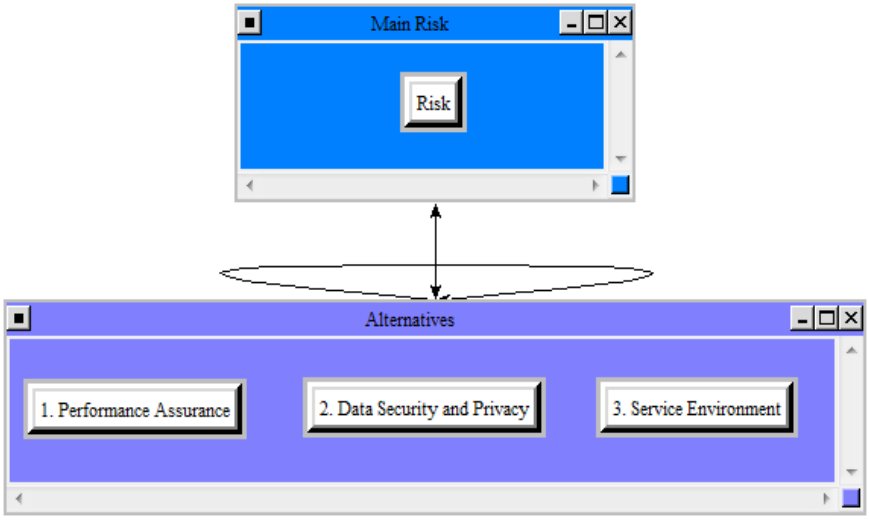

Figure 5. Super decisions snapshot depicting framework at 2 levels.

The relationship between Performance assurance, data security and privacy and service environment is depicted in Figure 6.

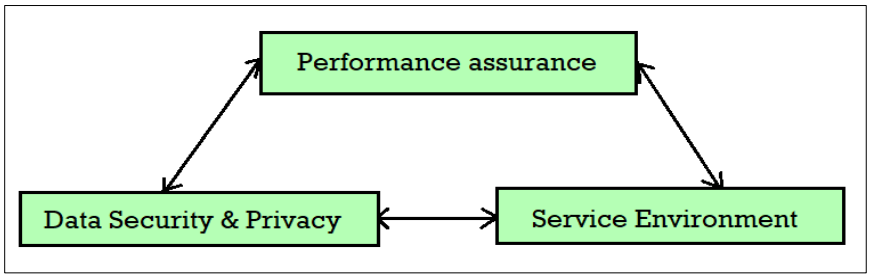

Figure 6. Pair-wise comparison of all three criteria.

Step 3: Pairwise Interdependence Matrices

Once all the pairwise comparisons are complete, the relative importance weight for each component is determined. Given that, A is the pairwise comparison matrix; the weights can be determined by an expression.

$$A.w = \lambda_{max} \quad (2)$$

where, A is the matrix of pairwise comparison, w is the eigenvector or priority vector, and λ_{max} is the largest eigenvalue of A.

Table 3. displays the relative impact and frequency of these risks.

Name	Impact	Frequency
Data Security and Privacy	0.716652655	0.502002439
Performance Assurance	0.205090625	0.420010237
Service Environment	0.07825672	0.077987324

To compare the properties of each risk dimension cluster inside a particular risks control hierarchy network, given an initial determinant of the risk control hierarchy network, pairwise comparisons must be performed (Table 3). Using pairwise comparisons, all of these relationships are evaluated, and the resulting priority vectors combine to form a super-matrix, which is a matrix of influence among the various elements. When a super-matrix is genuinely a partitioned matrix, it reflects a relationship between two nodes (components or clusters) in a system, with each matrix segment representing one of those relationships. Figures 7, 8 and 9 demonstrate the links between various risks and their effects on performance assurance, service environment, security and privacy, and other factors.

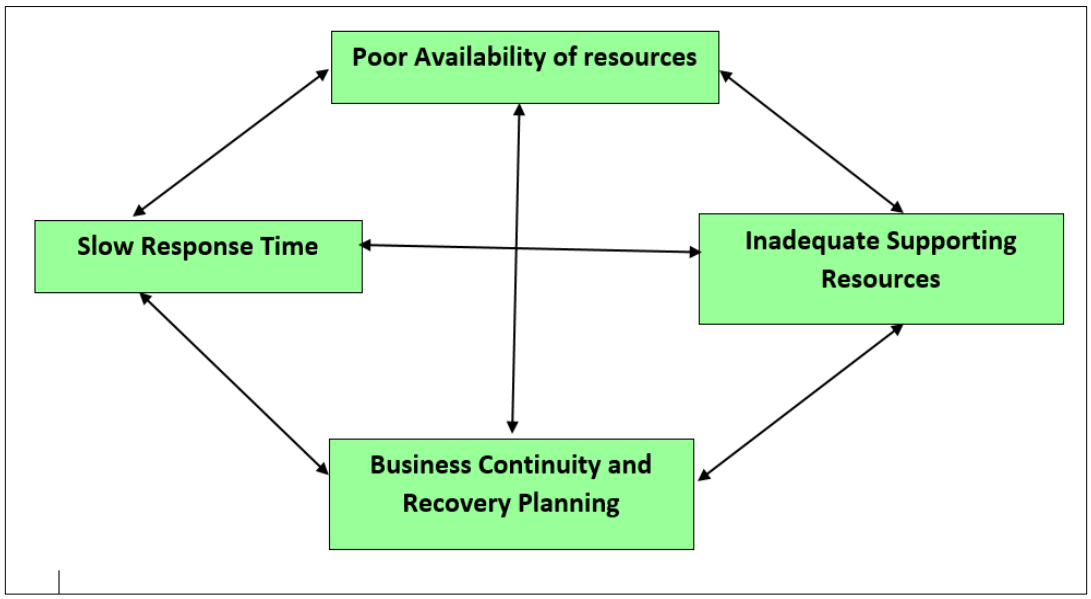

Figure 7. Pair-wise comparison of different risk factors with respect to service environment.

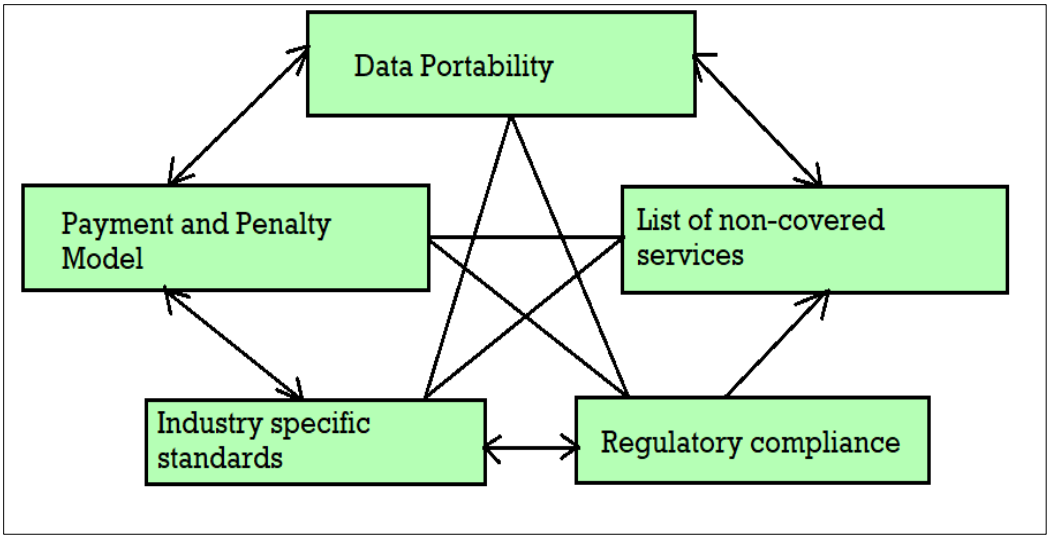

Figure 8. Pair-wise comparison of different risk factors with respect to performance assurance.

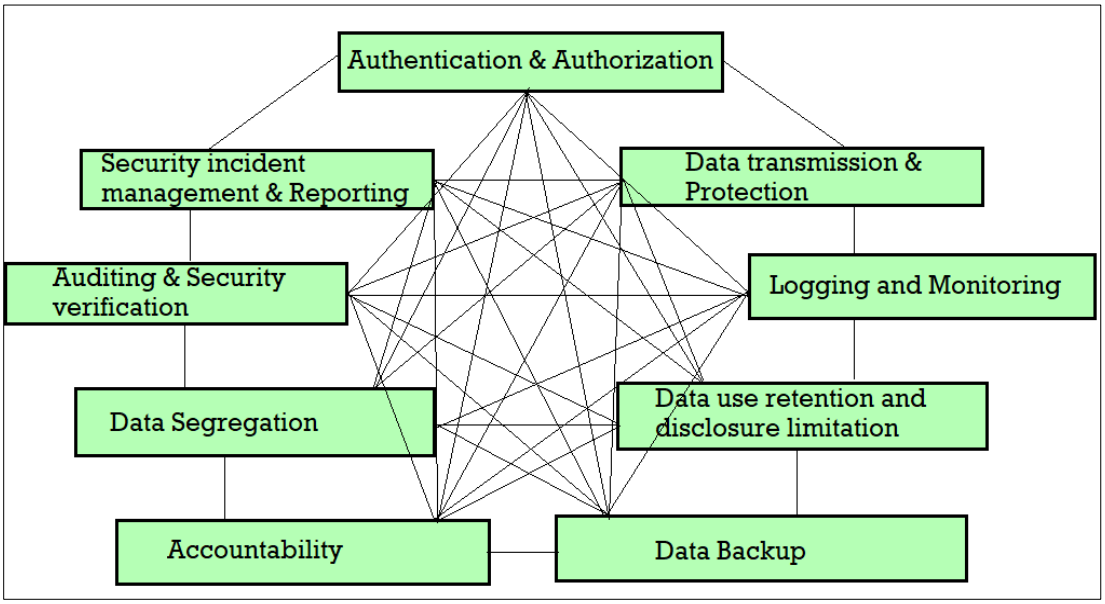

Figure 9. Pair-wise comparison of different risk factors with respect to Data Security & Privacy.

Matrix W_{32} as shown in Table 4, represents the e-Vector Column 1 for Performance Assurance, Column 2 for Data Security & Privacy, and Column 3 for Service Environment representing the relative importance of sub-criteria with respect to impact as in Table 4.

Table 4. Relative impact of various risks.

			Column 1	Column 2	Column 3
		Various Risk Factors	**Performance Assurance**	**Data Security and privacy**	**Service Environment**
Relative impact of various risk factors	AS	Poor Availability of Service	0.37213	0	0
	BCDRP	Business Continuity & Disaster Recovery Planning	0.40606	0	0
	RT	Slow Response Time	0.08865	0	0
	SR	Inadequate supporting Resources	0.13316	0	0
	ACC	Accountability	0	0.158	0
	ASV	Auditing & Security Verification	0	0.04567	0
	AA	Authentications & Authorization	0	0.20269	0
	DB	Data Backup	0	0.19503	0
	DS	Data Segregation	0	0.08979	0
	DTP	Data Transmission Protection	0	0.08185	0
	DURDL	Data Use Retention & Discloser Limitation	0	0.11365	0
	LMSI	Logging & Monitoring	0	0.06275	0
	SIMR	Security Incident Management & Reporting	0	0.05056	0
	DP	Data Probability	0	0	0.35849
	ISS	Industry Specific Standards	0	0	0.11856
	LNCS	List of Non covered Services	0	0	0.21689
	PPM	Payment & Penalty Modals	0	0	0.24431
	RC	Regulatory Compliance	0	0	0.06175

The frequency matrix is organized in the same manner and finally, we get respective priorities of frequency and impact of all 18 risks as shown in Table 5.

Table 5. Relative impact and frequencies ranking of 18 risks.

Risk	Impact	Risk	Frequency
BCDRP	0.43574	**AS**	0.44564
AS	0.30959	**RT**	0.37223
AA	0.26899	**SR**	0.32451
ACC	0.2479	**DBM**	0.26379
DBM	0.2243	**RC**	0.24379
DP	0.19748	**BCDRP**	0.22431
RT	0.19569	**AA**	0.19749
DTP	0.19403	**DP**	0.19667
DS	0.19149	**DTP**	0.19559
SR	0.17233	**DS**	0.19414
DURDL	0.16896	**ACC**	0.19314
SIMR	0.09797	**DURDL**	0.19244
ASV	0.08157	**ASV**	0.18456
LMSI	0.06317	**SIMR**	0.17896
PPM	0.05459	**PPM**	0.09905
RC	0.0448	**LMSI**	0.08157
ISS	0.02786	**ISS**	0.02865
LNCS	0.02353	**LNCS**	0.02456

Other studies utilized other MCDM (Multi-Criteria Decision Making) methods, but we selected ANP since it is suitable for the current study demands. We used the ANP approach in this study because of its capacity to describe possible connections and interdependencies. A pairwise comparison matrix must be used in the ANP approach. The ANP must be used to determine the optimal approach.

4. Result Analysis

4.1 Resultant Risk Matrix Plotting

In this section of the article, simulation results and findings are discussed based on the research methodology in Table 6.

Table 6. Final Result findings as per our research methodology are as follows.

Poor Availability of Service (AS)	First highest frequency
Slow Response Time (RT)	Second highest frequency
Inadequate Supporting Resources (SR)	Third highest frequency
Data Backup Monitoring (DBM)	Fourth highest frequency
Regulatory Compliance (RC), Business Continuity & Disaster Recovery Planning (BCDRP)	Frequencies are much higher than the geometric mean
Logging & Monitoring of Security Incidents (LMSI), Industry Specific Standards (ISS) and List of Non-Covered Services (LNCS)	Below geometric mean

Whereas the top impact risk is Business Continuity & Disaster Recovery Planning (BCDRP), the second highest impact risk is Poor Availability of Service (AS), third and fourth ranking is Authentication & Authorization (AA) and Accountability (ACC). Data Backup & Monitoring (DBM) and Data Portability (DP) are much higher than the geometric mean whereas Regulatory Compliance (RC), Industry Specific Standard (ISS) and List of Non-Covered Services (LNCS) are much below the geometric mean.

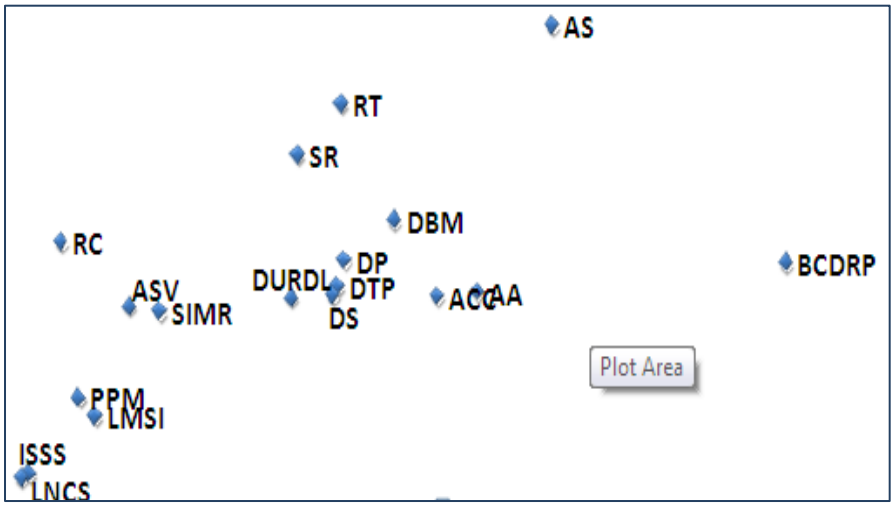

Figure 10. Plotting of various risks on impact v/s frequency plot.

5. Discussions

Following the findings of the risk management matrix depicted in Figures 7 to 9 of the criteria, Business Continuity & Disaster Recovery Planning, Poor Availability of Service, Authentication and Authorization, Accountability, Data Backup and Monitoring, Data Portability, Slow Response Time, Data Transmission Protection, Data Segregation, Inadequate Supporting Resources, Data Use Retention & Disclosure Limitation, are located in the region I, which is characterized by high impact and frequency. On the other hand, while Security Incident Management & Reporting, Auditing & Security Verification, and Regulatory Compliance are located in a region of low impact and high frequency, Logging & Monitoring of Security Incidents, Payments & Penalty Models, the List of Non-Covered Services, and Industry Specific Standards

are located in a region of low impact and low frequency, which is the region of least priority. It is becoming increasingly important for businesses to use cloud computing, and organizations are constantly seeking adoption roadmaps. Understanding the factors that drive acceptance can aid in the development of such roadmaps. One of the study's most important contributions is that it provides decision-makers with actionable knowledge when determining whether or not to use cloud computing. This is one of the study's most significant contributions.

6. Concluding Remarks

The cloud has always had an impact on business, and it will continue to do so. Cloud computing and adoption can result in enormous benefits, and, as a result, can make a major contribution to the long-term viability of an organization's operations. It helps businesses that want to use cloud computing for long-term growth by detecting, confirming, and assessing different risks that can arise during the decision-making process. It does this by looking at many different factors. The study attempts to provide cautious and risk-aware recommendations for cloud adoption. Starting from a review of the literature on cloud adoption, business requirements, and organizational sustainability, the study moves on to a discussion of cloud computing in practice. The risks connected with cloud adoption are discussed in detail in this report, which is extensive. Specifically, an Analytical Network Process-based technique is used to solve multi-criteria decision problems that are applied to the risks associated with cloud adoption. A risk matrix with the impact variables that can be used to make a risk-aware decision about cloud adoption was produced in this study. In the process of moving to the cloud, this would be good for things like risk management and design.

As the results of the risk management matrix illustrated in Figures 7 to 9 of the criteria, Business Continuity & Disaster Recovery Planning, Availability of Service, Authentication and Authorization, Accountability, Data Backup and Monitoring, Data Portability, Response Time, Data Transmission Protection, Data Segregation, Supporting Resources, Data Use Retention & Disclosure Limitation lie in the region I, region of high impact and high frequency. Whereas Security Incident Management & Reporting, Auditing& Security Verification and Regulatory Compliance lie in the region of low impact and high frequency, Logging & Monitoring of Security Incidents, Payments & Penalty Models, List of Non-Covered Services, and Industry Specific Standards lie in the region of low frequency and low impact which is a region of least priority. Cloud computing is becoming increasingly crucial for businesses to employ and organizations are always looking for adoption roadmaps, and understanding the elements that influence acceptance assists in the construction of such roadmaps. One of the study's most significant contributions is that it offers decision-makers actionable knowledge when deciding whether to utilize Cloud Computing. In future, the concept of cloud security will be involved that includes upgraded technologies, modified policies, better controls, and services to protect the users' cloud data, cloud-based applications, and infrastructure against both external and internal cyber threats.

Conflict of Interest

The authors certify that all of the authors have seen and agreed to the final version of the paper and that there are no competing interests. We also assure that the article is the original work of the authors listed in the manuscript, that it has never been published before, and that it is not being considered for publication anywhere else.

Acknowledgement

We would like to express our gratitude to the reviewers for devoting the requisite amount of time and effort to the review process of our article. We appreciate all of the insightful comments and suggestions, which helped us improve the manuscript as a whole.

References

Awaysheh, F.M., Aladwan, M.N., Alazab, M., Alawadi, S., Cabaleiro, J.C., & Pena, T.F. (2021). Security by design for big data frameworks over cloud computing. *IEEE Transactions on Engineering Management*, *69*(1), 3676-3693.

Biswal, J.N., Muduli, K., & Satapathy, S. (2017). Critical analysis of drivers and barriers of sustainable supply chain management in Indian thermal sector. *International Journal of Procurement Management*, *10*(4), 411-430.

Biswal, J.N., Muduli, K., Satapathy, S., & Yadav, D.K. (2019). A TISM based study of SSCM enablers: An Indian coal-fired thermal power plant perspective. *International Journal of System Assurance Engineering and Management*, *10*(1), 126-141.

Briscoe, G., & Marinos, A. (2009, June). Digital ecosystems in the clouds: Towards community cloud computing. In *2009 3rd IEEE International Conference on Digital Ecosystems and Technologies* (pp. 103-108). IEEE. Istanbul, Turkey.

Buyya, R., & Gill, S.S. (2018). Sustainable cloud computing: Foundations and future directions. arXiv:1805.01765, *21*(6).

Buyya, R., Yeo, C.S., & Venugopal, S. (2008, September). Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In *2008 10th IEEE International Conference on High Performance Computing and Communications* (pp. 5-13). IEEE. Dalian, China.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009, November). Controlling data in the cloud: Outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security* (pp. 85-90). https://doi.org/10.1145/1655008.1655020.

Dewangan, B.K., Agarwal, A., Choudhury, T., & Pasricha, A. (2020). Cloud resource optimization system based on time and cost. *International Journal of Mathematical, Engineering and Management Sciences*, *5*(4), 758-768.

Gill, S.S., & Buyya, R. (2018). A taxonomy and future directions for sustainable cloud computing: 360 degree view. *ACM Computing Surveys (CSUR)*, *51*(5), 1-33.

Kheybari, S., Rezaie, F.M., & Farazmand, H. (2020). Analytic network process: An overview of applications. *Applied Mathematics and Computation*, *367*, 124780. https://doi.org/10.1016/j.amc.2019.124780.

Kim, W., Kim, S.D., Lee, E., & Lee, S. (2009, December). Adoption issues for cloud computing. In *Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia* (pp. 2-5). Kuala Lumpur, Malaysia. https://doi.org/10.1145/1821748.1821751.

Kline, R.B. (1998). *Principles and practice of structural equation modeling*. Guilford Press, New York.

Kostyuchenko, E.Y., Balatskaya, L.N., Kharchenko, S.S., & Lapina, M.A. (2021, March). Comparison of recognition using Google and Kaldi to solve the problem of assessing intelligibility. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1069, No. 1, p. 012032). IOP Publishing.

Liu, Z., Dai, P., Xing, H., Yu, Z., & Zhang, W. (2021). A distributed algorithm for task offloading in vehicular networks with hybrid fog/cloud computing. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *52*(7), 4388-4401.

Muduli, K., & Barve, A. (2013a). Developing a framework for study of GSCM criteria in Indian mining industries. *APCBEE Procedia*, *5*, 22-26.

Muduli, K., & Barve, A. (2013b). Modelling the behavioural factors of green supply chain management implementation in mining industries in Indian scenario. *Asian Journal of Management Science and Applications*, *1*(1), 26-49.

Muduli, K., & Barve, A. (2015). Analysis of critical activities for GSCM implementation in mining supply chains in India using fuzzy analytical hierarchy process. *International Journal of Business Excellence*, *8*(6), 767-797.

Radu, L.D. (2017). Green cloud computing: A literature survey. *Symmetry*, *9*(12), 295. https://doi.org/10.3390/SYM9120295.

Raj, T., Shankar, R., & Suhaib, M. (2010). GTA-based framework for evaluating the feasibility of transition to FMS. *Journal of Manufacturing Technology Management*, *21*(2), 160-187.

Saaty, T.L., & Vargas, L.G. (2006). *Decision making with the analytic network process*. Springer Science+ Business Media, LLC. Berlin, Germany.

Saaty, T.L., & Vargas, L.G. (2013). *Decision making with the analytic network process*. Springer, USA. https://doi.org/10.1007/978-1-4614-7279-7.

Singh, S., & Misra, S.C. (2021). Exploring the challenges for adopting the cloud PLM in manufacturing organizations. *IEEE Transactions on Engineering Management*, *68*(3), 752-766. https://doi.org/10.1109/TEM.2019.2908454.

Son, I., Lee, D., Lee, J.N., & Chang, Y.B. (2011). Understanding the impact of IT service innovation on firm performance: The case of cloud computing. *PACIS 2011 - 15th Pacific Asia Conference on Information Systems: Quality Research in Pacific*, 180. https://aisel.aisnet.org/pacis2011/180.

Sorourkhah, A. (2022). Coping uncertainty in the supplier selection problem using a scenario-based approach and distance measure on type-2 intuitionistic fuzzy sets. *Fuzzy Optimization and Modeling Journal*, *3*(1), 64-71.

Stinchcombe, N. (2009). Cloud computing in the spotlight. *Infosecurity*, *6*(6), 30-33.

Tulasi, B. (2009). Market-oriented cloud computing-delivering IT services as computing utilities. *Mapana Journal of Sciences*, *8*(1), 26-34.