

IMPACT ON STUDY OF DATA SECURITY IN ENTERPRISE'S CLOUD COMPUTING

Submitted in partial fulfillment of the requirements for the award of
MASTER OF BUSINESS ADMINISTRATION

by

DHANUSHIYA.G
Register No. 42410223



SCHOOL OF MANAGEMENT STUDIES

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Accredited with Grade "A++" by NAAC I 12B Status by UGC I

Approved by AICTE

JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI - 600 119



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE

www.sathyabama.ac.in

SCHOOL OF MANAGEMENT STUDIES

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **DHANUSHIYA.G (42410223)** who carried out the project entitled "**Impact on study of data security in enterprise's cloud computing**" under my supervision from September 2023 to October 2023.

Dr MOLI GHOSH

Internal guide

External Guide

Dr. BHUVANESWARI G
Dean – School of Management Studies

Submitted for Viva voce Examination held on

Internal Examiner

External Examiner

DECLARATION

I, **DHANUSHIYA. G (42410223)** hereby declare that the Project Report entitled **“Impact on study of data security in enterprise’s cloud computing”** done by me under the guidance of **DR. MOLI GHOSH** is submitted in partial fulfillment of the requirements for the award of Master of Business Administration degree.

DATE:

PLACE:

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my sincere thanks to **Dr. G. Bhuvaneswari, Dean - School of Management Studies** and **Dr. A. Palani, Head - School of Management Studies** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **DR. MOLI GHOSH** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **School of Management Studies** who were helpful in many ways for the completion of the project.

DHANUSHIYA.G

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	LIST OF TABLES	7
	LIST OF CHARTS	8
	INTRODUCTION	
1	1.1 Introduction	9
	1.2 Objectives of the Study	10
	1.3 Need for the study	10
	1.4 Scope & Significance of the study	10
	REVIEW OF LITERATURE	
2	2.1 Review of Literature	11
	RESEARCH METHODOLOGY	
3	3.1 Methodology	14
	3.2. Research Design	14
	3.3. Sources of Data	14
	3.4. Questionnaire Development	14
	3.5. Sample Size	15
	3.6. Hypothesis	16
	DATA ANALYSIS AND INTERPRETATION	
4	4.1 Percentage Analysis	16
	4.2. ANOVA	30
	FINDINGS, SUGGESTIONS, AND CONCLUSION	
5	5.1. Findings of the Study	32
	5.2. Suggestions & Recommendations	33
	5.3. Limitations of the study	33
	5.4. Conclusion	34
	REFERENCES	35
	ANNEXURE – QUESTIONNAIRE	36

ABSTRACT

Cloud computing technology has acquired a massive vogue in the business technology area over the years. It has offered many services, features, and benefits to the enterprises to utilize cloud computing instead of on-premise computing resources. However, many challenges affect enterprises to adopt cloud computing. Yet, some enterprises still have issues related to implementing cloud services and using this new technology. The primary concerns are cost advantages and security risks that directly affect enterprises to migrate into cloud computing. The cloud deployment model is selected based on several factors such as cost, company strategy, current challenges, and future roadmap. Small and medium enterprises are very suited to the public cloud model. In contrast, large enterprises always favor the private cloud due to security and the hybrid cloud because of the flexibility and combination of operation savings and risk balance. Finally, this research has discovered the main challenges, concerns, services related to cloud computing and highlighted the issues and suggestions to mitigate the indicated risks related to the security and cost before migrating into cloud computing.

LIST OF TABLES

TABLE NO.	PARTICULARS	PAGE NO.
4.1.1	GENDER OF THE RESPONDENTS	16
4.1.2	SALARY OF THE RESPONDENTS	17
4.1.3	AGE OF RESPONDENTS	18
4.1.4	EDUCATION OF RESPONDENTS	19
4.1.5	PROFESSION OF RESPONDENTS	20
4.1.6	TABLE SHOWING RESPONSES OF THE QUESTIONNAIRE	21
4.1.7	TABLE SHOWING RESPONSES OF THE QUESTIONNAIRE	22
4.1.8	TABLE SHOWING RESPONSES OF THE QUESTIONNAIRE	23
4.1.9	TABLE SHOWING RESPONSES OF THE QUESTIONNAIRE	24
4.1.10	TABLE SHOWING RESPONSES OF THE QUESTIONNAIRE	25
4.1.11	TABLE SHOWING RESPONSES OF THE QUESTIONNAIRE	26
4.1.12	TABLE SHOWING RESPONSES OF THE QUESTIONNAIRE	27
4.1.13	TABLE SHOWING RESPONSES OF THE QUESTIONNAIRE	28
4.1.14	TABLE SHOWING RESPONSES OF THE QUESTIONNAIRE	29
4.1.15	TABLE SHOWING RESPONSES OF THE QUESTIONNAIRE	30

LIST OF CHARTS

CHARTS NO.	PARTICULARS	PAGE NO.
4.1.1	GENDER OF THE RESPONDENTS	16
4.1.2	SALARY OF THE RESPONDENTS	17
4.1.3	AGE OF THE RESPONDENTS	18
4.1.4	EDUCAION OF THE RESPONDENTS	19
4.1.5	PROFESSION OF THE RESPONDENTS	20
4.1.6	CHART REPRESENTING THE QUESTIONNAIRE RESPONSE	21
4.1.7	CHART REPRESENTING THE QUESTIONNAIRE RESPONSE	22
4.1.8	CHART REPRESENTING THE QUESTIONNAIRE RESPONSE	23
4.1.9	CHART REPRESENTING THE QUESTIONNAIRE RESPONSE	24
4.1.10	CHART REPRESENTING THE QUESTIONNAIRE RESPONSE	25
4.1.11	CHART REPRESENTING THE QUESTIONNAIRE RESPONSE	26
4.1.12	CHART REPRESENTING THE QUESTIONNAIRE RESPONSE	27
4.1.13	CHART REPRESENTING THE QUESTIONNAIRE RESPONSE	28
4.1.14	CHART REPRESENTING THE QUESTIONNAIRE RESPONSE	29
4.1.15	CHART REPRESENTING THE QUESTIONNAIRE RESPONSE	30

CHAPTER 1 – INTRODUCTION

1.1 INTRODUCTION

Cloud computing has been envisioned as the next generation paradigm in computation. In the cloud computing environment, both applications and resources are delivered on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data Centre that provide diverse services over the network or the Internet to satisfy user's requirements.

The explanation of “cloud computing” from the National Institute of Standards and Technology (NIST) is that cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. According to the explanation, cloud computing provides a convenient on-demand network access to a shared pool of configurable computing resources. Resources refer to computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure.

Cloud computing can be considered as a new computing archetype that can provide services on demand at a minimal cost. The three well-known and commonly used service models in the cloud paradigm are software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). In SaaS, software with the related data is deployed by a cloud service provider, and users can use it through the web browsers. In PaaS, a service provider facilitates services to the users with a set of software programs that can solve the specific tasks. In IaaS, the cloud service provider facilitates services to the users with virtual machines and storage to improve their business capabilities.

Cloud computing is closely related to but not the same as grid computing . Grid computing integrates diverse resources together and controls the resources with the unified operating systems to provide high performance computing services, while cloud computing combines the computing and storage resources controlled by different operating systems to provide services such as large-scaled data storage and high Performance computing to users. The overall picture of grid computing has been changed by cloud computing. Distribution of data is in a new way of cloud computing comparing with the grid computing.

Cloud computing will enable services to be consumed easily on demand. Cloud computing has the characteristics such as on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing, and transference of risk. These merits of cloud computing have attracted substantial interests from both the industrial world and the academic research world. Cloud computing technology is currently changing the way to do business in the world.

Cloud computing is very promising for the IT applications; however, there are still some problems to be solved for personal users and enterprises to store data and deploy applications in the cloud computing environment. One of the most significant barriers to adoption is data security, which is accompanied by issues including compliance, privacy, trust, and legal

matters. The role of institutions and institutional evolution is close to privacy and security in cloud computing.

Data security has consistently been a major issue in IT. Data security becomes particularly serious in the cloud computing environment, because data are scattered in different machines and storage devices including servers, PCs, and various mobile devices such as wireless sensor networks and smart phones. Data security in the cloud computing is more complicated than data security in the traditional information systems.

To make the cloud computing be adopted by users and enterprise, the security concerns of users should be rectified first to make cloud environment trustworthy. The trustworthy environment is the basic prerequisite to win confidence of users to adopt such a technology. Latif et al. discussed the assessment of cloud computing risks .

Before the data security issues are discussed, the functions of cloud computing are analyzed first. Cloud computing is also known as on-demand service. In the cloud computing environment, there is a cloud service provider that facilitates services and manages the services. The cloud provider facilitates all the services over the Internet, while end users use services for satisfying their business needs and then pay the service provider accordingly.

Cloud computing environment provides two basic types of functions: *computing* and *data storage*. In the cloud computing environment, consumers of cloud services do not need anything and they can get access to their data and finish their computing tasks just through the Internet connectivity. During the access to the data and computing, the clients do not even know where the data are stored and which machines execute the computing tasks.

Coming to data storage, data protection and security are the primary factors for gaining user's trust and making the cloud technology successfully used. A number of data protections and data security techniques have been proposed in the research field of cloud computing. However, data protection related techniques need to be further enhanced.

Services of cloud computing are provided across the entire computing spectrum. Nowadays, organizations and companies are moving and extending their business by adopting the cloud computing to lower their cost. This can contribute to free more man-powers to focus on creating strategic differentiation and business division of labour is clearer.

The concept of cloud has a number of implementations based on the services from service providers. For example, Google Apps Engine, Microsoft Azure, and Amazon Stack are popular implementations of cloud computing provided by cloud service providers, that is, Google, Microsoft, and Amazon companies. Besides, the ACME enterprise implemented VMware based v-Cloud for permitting multiple organizations to share computing resources.

According to the difference of access scope, cloud can be divided into three types: *public cloud*, *private cloud*, and *hybrid cloud*. Public cloud is as the property of service provider and can be used in public, private cloud refers to being the property of a company, and hybrid cloud is the blends of public and private cloud. Most of the existing cloud services are provided by large cloud service companies such as Google, Amazon, and IBM. A private cloud is a cloud in which only the authorized users can access the services from the provider. In the public cloud anybody can use the cloud services whereas the hybrid cloud contains the concept of both public and private clouds.

Cloud computing can save an organization's time and money, but trusting the system is more important because the real asset of any organization is the data which they share in the cloud to use the needed services by putting it either directly in the relational database or eventually in a relational database through an application.

Cloud computing brings a number of attributes that require special attention when it comes to trusting the system. The trust of the entire system depends on the data protection and prevention techniques used in it. Numerous different tools and techniques have been tested and introduced by the researchers for data protection and prevention to gain and remove the hurdle of trust but there are still gaps which need attention and are required to be lined up by making these techniques much better and effective.

The meaning of security is plentiful. Security is the combination of confidentiality, the prevention of the unauthorized disclosure of information, integrity, the prevention of the unauthorized amendment or deletion of information, and availability, the prevention of unauthorized withholding of information.

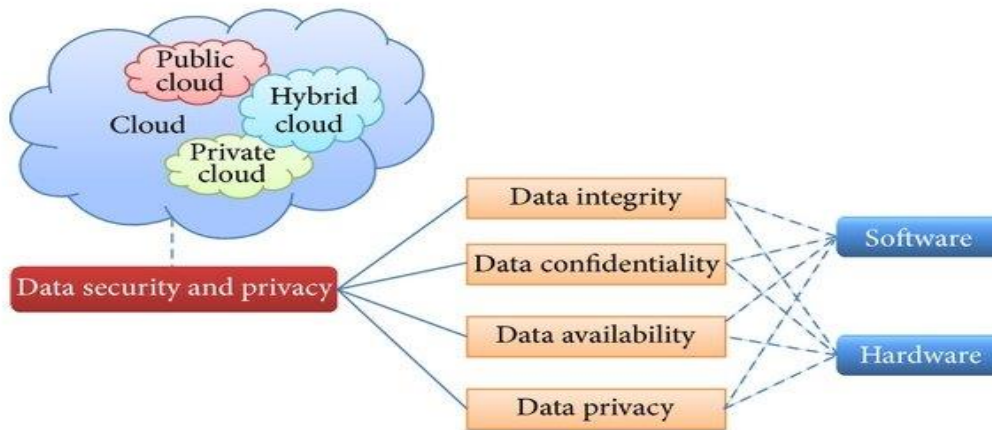
The major issues in the cloud computing include resource security, resource management, and resource monitoring. Currently, there are no standard rules and regulations to deploy applications in the cloud, and there is a lack of standardization control in the cloud. Numerous novel techniques had been designed and implemented in cloud; however, these techniques fall short of ensuring total security due to the dynamics of the cloud environment.

The inherent issues of data security, governance, and management with respect to control in the cloud computing are discussed in highlighted the key security, privacy, and trust issues in the existing environment of cloud computing and help users to recognize the tangible and intangible threats related to its use. According to the authors, there are three major potential threats in cloud computing, namely, *security*, *privacy*, and *trust*. Security plays a critical role in the current era of long dreamed vision of computing as a utility.

A data security framework for cloud computing networks is proposed . The authors mainly discussed the security issues related to cloud data storage. There are also some patents about the data storage security techniques .Younis and Kifayat give a survey on secure cloud computing for critical infrastructure . A security and privacy framework for RFID in cloud computing was proposed for RFID technology integrated to the cloud computing ,which will combine the cloud computing with the Internet of Things.

In short, the foremost issues in cloud data security include data privacy, data protection, data availability, data location, and secure transmission. The security challenges in the cloud include threats, data loss, service disruption, outside malicious attacks, and multitenancy issues . Chen and Zhao analyzed privacy and data security issues in the cloud computing by focusing on privacy protection, data segregation, and cloud security. Data security issues are primarily at SPI (SaaS, PaaS, and IaaS) level and the major challenge in cloud computing is data sharing.

In this paper, we will review different security techniques and challenges for data storage security and privacy protection in the cloud computing environment. As Figure shows, this paper presents a comparative research analysis of the existing research work regarding the techniques used in the cloud computing through data security aspects including data integrity, confidentiality, and availability. Data privacy issues and technologies in the cloud are also studied, because data privacy is traditionally accompanied with data security. Comparative studies on data security and privacy could help to enhance the user's trust by securing data in the cloud computing environment.



Data Integrity

Data integrity is one of the most critical elements in any information system. Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication. Managing entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, or stolen.

Data integrity is easily achieved in a standalone system with a single database. Data integrity in the standalone system is maintained via database constraints and transactions, which is usually finished by a database management system (DBMS). Transactions should follow ACID (atomicity, consistency, isolation, and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity.

Authorization is used to control the access of data. It is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system.

Data integrity in the cloud system means preserving information integrity. The data should not be lost or modified by unauthorized users. Data integrity is the basis to provide cloud computing service such as SaaS, PaaS, and IaaS. Besides data storage of large-scaled data, cloud computing environment usually provides data processing service. Data integrity can be obtained by techniques such as RAID-like strategies and digital signature.

Owing to the large quantity of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data. By avoiding the unauthorized access, organizations can achieve greater confidence in data integrity. The monitoring mechanisms offer the greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity. Cloud computing providers are trusted to maintain data integrity and accuracy. However, it is necessary to build the third party supervision mechanism besides users and cloud service providers.

Verifying the integrity of data in the cloud remotely is the prerequisite to deploy applications. Bowers et al. proposed a theoretical framework "Proofs of Retrievability" to realize the

remote data integrity checking by combining error correction code and spot-checking . The HAIL system uses POR mechanism to check the storage of data in different clouds, and it can ensure the redundancy of different copies and realize the availability and integrity checking . Schiffman et al. proposed trusted platform module (TPM) remote checking to check the data integrity remotely .

Data Confidentiality

Data confidentiality is important for users to store their private or confidential data in the cloud. Authentication and access control strategies are used to ensure data confidentiality. The data confidentiality, authentication, and access control issues in cloud computing could be addressed by increasing the cloud reliability and trustworthiness .

Because the users do not trust the cloud providers and cloud storage service providers are virtually impossible to eliminate potential insider threat, it is very dangerous for users to store their sensitive data in cloud storage directly. Simple encryption is faced with the key management problem and cannot support complex requirements such as query, parallel modification, and fine-grained authorization.

Data Availability

Data availability means the following: when accidents such as hard disk damage, IDC fire, and network failures occur, the extent that user's data can be used or recovered and how the users verify their data by techniques rather than depending on the credit guarantee by the cloud service provider alone.

The issue of storing data over the trans boarder servers is a serious concern of clients because the cloud vendors are governed by the local laws and, therefore, the cloud clients should be cognizant of those laws. Moreover, the cloud service provider should ensure the data security, particularly data confidentiality and integrity. The cloud provider should share all such concerns with the client and build trust relationship in this connection. The cloud vendor should provide guarantees of data safety and explain jurisdiction of local laws to the clients. The main focus of the paper is on those data issues and challenges which are associated with data storage location and its relocation, cost, availability, and security.

Locating data can help users to increase their trust on the cloud. Cloud storage provides the transparent storage service for users, which can decrease the complexity of cloud, but it also decreases the control ability on data storage of users. Benson et al. studied the proofs of geographic replication and succeeded in locating the data stored in Amazon cloud

Data Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal them selectively Privacy has the following elements.

(i)

When: a subject may be more concerned about the current or future information being revealed than information from the past.

How: a user may be comfortable if his/her friends can manually request his/her information, but the user may not like alerts to be sent automatically and frequently.

(iii)

Extent: a user may rather have his/her information reported as an ambiguous region rather than a precise point.

In commerce, consumer's context and privacy need to be protected and used appropriately. In organizations, privacy entails the application of laws, mechanisms, standards, and processes by which personally identifiable information is managed .

In the cloud, the privacy means when users visit the sensitive data, the cloud services can prevent potential adversary from inferring the user's behaviour by the user's visit model (not direct data leakage). Researchers have focused on Oblivious RAM (ORAM) technology. ORAM technology visits several copies of data to hide the real visiting aims of users. ORAM has been widely used in software protection and has been used in protecting the privacy in the cloud as a promising technology. Stefanov et al. proposed that a path ORAM algorithm is state-of-the-art implementation.

(i)

how to enable users to have control over their data when the data are stored and processed in cloud and avoid theft, nefarious use, and unauthorized resale,

(ii)

how to guarantee data replications in a jurisdiction and consistent state, where replicating user data to multiple suitable locations is an usual choice, and avoid data loss, leakage, and unauthorized modification or fabrication,

(iii)

which party is responsible for ensuring legal requirements for personal information,

(iv)

to what extent cloud subcontractors are involved in processing which can be properly identified, checked, and ascertained.

1.2 OBJECTIVE OF THE STUDY

“Impact on study of data security in enterprises cloud computing “

- To analyze the benefit of the biggest challenge that lead enterprises to migrate into the cloud computing.
- To study the cloud computing is a technology that used to minimize the cost of a company.
- To find the service provider for cloud computing application.

1.3 NEED OF THE STUDY

- This includes protecting against unauthorized access, ensuring data accuracy, and maintaining system functionality.
- The increasing reliance on cloud services, understanding and addressing security concerns are essential to safeguarding business operations and maintaining trust with customers and partners.
- Studying data security in enterprise cloud computing is crucial due to the potential impact on confidentiality, integrity, and availability of sensitive information.

1.4 SCOPE OF THE STUDY

- The study of data security in enterprise cloud computing has gained prominence due to the heightened awareness and concern for protecting sensitive information.
- Understanding the impact involves developing comprehensive incident response plans to efficiently address and mitigate security incidents in a timely manner.
- The scope involves exploring and implementing robust encryption techniques to safeguard data during transmission and storage within cloud infrastructures.

CHAPTER 2 – REVIEW OF LITERATURE

2.1 REVIEW OF LITERATURE

Paul T. Jaeger (2008), Cloud Computing and Information Policy: Computing in a Policy Cloud, Cloud computing is a computing platform that resides in a large data center and is able to dynamically provide servers with the ability to address a wide range of needs, from scientific research to e-commerce. The provision of computing resources as if it were a utility such as electricity, while potentially revolutionary as a computing service, presents many major problems of information policy, including issues of privacy, security, reliability, access, and regulation. This article explores the nature and potential of cloud computing, the policy issues raised, and research questions related to cloud computing and policy. Ultimately, the policy issues raised by cloud computing are examined as a part of larger issues of public policy attempting to respond to rapid technological evolution.

Mohammed A. Al-Sharaf (2017), Factors Influencing the Continuous Use of Cloud Computing Services in Organization Level: The primary purpose of carrying out this research work is to identify the crucial factors that influence the continuous use of cloud computing services in organizations. To achieve this identified objective, this research work carried out a comprehensive literature review on cloud computing services' adoption at the organizational level, particularly emphasizing the factors that define the prolonged adoption of cloud computing services. The factors identified, served as a guide required by organizations for completely safe and effective cloud computing service and their use in businesses. This research adopts the criteria of Wymer and Regan as a basis for this study. A total of 53 factors were obtained from prior studies on the cloud computing services' adoption. Results obtained during the course of study revealed that the most crucial factors affecting the continuous use of cloud computing services in organizations are as follows: Relative advantage; Complexity; Perceived security and privacy; Compatibility; Top manager's support; Cost reduction; Competitive pressure; IT readiness; Firm size; Vendor support; Regulations and Government policy; Trialability; Perceived reliability; Perceived availability; Uncertainty and Perceived Trust.

Siti Maliza Salleh (2012), Cloud Enterprise Systems: A Review Of Literature And Its Adoption: In recent years, Cloud computing has revolutionized the IT industry by introducing a whole new concept and platform of enterprise systems (ES). The traditional ES seem to be too clunky, expensive and complex for most organizations to implement and use. To improve such situation Cloud ES concept was recently introduced to offer competitive advantage to organizations through flexibility, scalability and independence in IT infrastructure and capabilities. Today, this area has not been fully explored in the academia due to little available literature but it has attracted tremendous interest from the general practitioners. This study seeks to contribute to IS literature by conceptualising Cloud ES from a pragmatic understanding between practitioners and academic. It further elaborates the advantages and challenges of Cloud ES and discusses the potential of Cloud ES as an attractive option to SME in solving the problems of high investments in IT infrastructures and IT resource

Asatiani (2014), A review of cloud adoption determinants in organizations :Adoption of cloud computing in organizations is increasing at a rapid pace. It is expected that the majority of the organizations in industrialized nations will be using cloud services to some extent in the near future. In this review I categorize adoption factors utilized in the literature and identify determinants playing a key role in organizations' decision to adopt cloud. I analyze both quantitative and qualitative evidence and code relationships between factors and adoption of cloud by systematically reviewing the literature. Findings show underrepresentation of the factors related to organization and external environment in cloud adoption literature. This study contributes a set of determinants of cloud adoption, which serves as a foundation for the future research and advancement of the theories in information systems field.

Adam M. Mahmood (2012), Impact of Cloud Computing Adoption on Firm Stock Price – An Empirical Research: In this paper, we investigate how cloud computing adoption impacts publicly traded 26 cloud-adopting companies' stocks. In an effort to perform a valid assessment of a firm's cloud adoption initiatives, we also evaluate the stocks of 26 companies, which did not adopt cloud computing and operate in the same industry with similar market capitalization. Our study differs from the previous studies in the area because it uses Fama-French three factor model to derive the stock abnormal returns for both adopters and non-adopters. Furthermore, given the announced risks of cloud computing in the literature, we analyzed the stock risk between adopters and non-adopters. Our preliminary analysis implies that businesses adopting cloud computing experience positive cumulative abnormal returns during the time the event was announced. Our research also indicates that both cloud adopting and non-cloud adopting companies suffer from higher stock risk during the announcement but this risk is not statistically significant.

Jitendra Singh (2014), Cyber-Attacks in Cloud Computing: A Case Study:Cloud computing has emerged from the legacy system; consequently, threats applicable in legacy system are equally applicable to cloud computing. In addition, cloud specific new threats have also emerged due to the various reasons including, multi-tenancy, access from anywhere, control of cloud, etc. Considering the significance of cloud security, this work is an attempt to identify the major threat factors to cloud security that may be critical in cloud environment. It also highlights the various methods employed by the attackers to cause the damage. To accomplish our objective, we have reviewed the major publication related to cyber security. It is revealed that cyber-attacks are industry specific and vary significantly from one industry type to another. Finally, we have conducted the case study on cyber-attacks that are already occurred in cloud paradigm. Cyber-attacks were highlighted by categorizing them into phishing attacks and distributed denial of services. This work will be profoundly helpful to the industry and researchers in understanding the various cloud specific cyber-attack and enable them to evolve the strategy to counter them more effectively.

Yashar Abed and Meena Chavan (2018), The Challenges of Institutional Distance: Data Privacy Issues in Cloud Computing: Data protection and data privacy are significant challenges in cloud computing for multinational corporations. There are no standard laws to protect data across borders. The institutional and regulatory constraints and governance differ across countries. This article explores the challenges of institutional constraints faced by cloud computing service providers in regard to data privacy issues across borders.

Yunchuan Sun (2014), .Data Security and Privacy in Cloud Computing : Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in all the globe. Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business. Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture. This study is to review different security techniques and challenges from both software and hardware aspects for protecting data in the cloud and aims at enhancing the data security and privacy protection for the trustworthy cloud environment. In this paper, we make a comparative research analysis of the existing research work regarding the data security and privacy protection techniques used in the cloud computing.

Prashant Gupta (2013), The usage and adoption of cloud computing by small and medium businesses: Cloud computing has become the buzzword in the industry today. Though, it is not an entirely new concept but in today's digital age, it has become ubiquitous due to the proliferation of Internet, broadband, mobile devices, better bandwidth and mobility requirements for end-users (be it consumers, SMEs or enterprises). In this paper, the focus is on the perceived inclination of micro and small businesses (SMEs or SMBs) toward cloud computing and the benefits reaped by them. This paper presents five factors influencing the cloud usage by this business community, whose needs and business requirements are very different from large enterprises. Firstly, ease of use and convenience is the biggest favourable factor followed by security and privacy and then comes the cost reduction. The fourth factor reliability is ignored as SMEs do not consider cloud as reliable. Lastly but not the least, SMEs do not want to use cloud for sharing and collaboration and prefer their old conventional methods for sharing and collaborating with their stakeholders.

Ge Zhang (2021), Investigating the Impact of Cloud Computing Vendor on the Adoption of Cloud Computing: Cloud computing offers significant impacts on organization by changing how information systems are developed, deployed, operated, maintained, and paid for. Therefore, the adoption of cloud computing becomes the focus of relevant research; however, previous studies have mostly studied the factors affecting cloud computing adoption from the perspective of adopters, ignoring the influence of the vendors. This study defines cloud service capability and develops scale to measure it from the perspective of cloud computing vendors to empirically examine the impact of the supply-side of cloud computing. The initial scale of cloud service capability is constructed using qualitative research, and the formal scale is obtained after two rounds of pretest. The statistical results of matched data collected from 132 cloud computing vendors and their users show that cloud service capability significantly affects cloud computing adoption. This study shifts the research perspective on cloud adoption to make theoretical contributions and management insights from the perspective of cloud computing vendors.

Theo Lynn (2020):High performance computing (HPC) is widely recognized as a key enabling technology for advancing scientific progress, industrial competitiveness, national and regional security, and the quality of human life. Notwithstanding this contribution, the large upfront investment and technical expertise required has limited the adoption of HPC to large organizations, government bodies, and third level institutions. Recent advances in cloud computing and telecommunications have the potential to overcome the historical issues associated with HPC through increased flexibility and efficiency, and reduced capital and operational expenditure. This study seeks to advance the literature on technology adoption and assimilation in the under-examined HPC context through a mixed methods approach. Firstly, the determinants of cloud computing adoption for HPC are examined through a survey of 121 HPC decision makers worldwide. Secondly, a modified Delphi method was conducted with 13 experts to identify and prioritize critical issues in the adoption of cloud computing for HPC. Results from the quantitative phase suggest that only organizational and human factors significantly influence cloud computing adoption decisions for HPC. While security was not identified as a significant influencer in adoption decisions, qualitative research findings suggest that data privacy and security issues are an immediate and long-term concern.

Diogo A. B. Fernandes, (2014) Security issues in cloud environments: In the last few years, the appealing features of cloud computing have been fueling the integration of cloud environments in the industry, which has been consequently motivating the research on related technologies by both the industry and the academia. The possibility of paying-as-you-go mixed with an on-demand elastic operation is changing the enterprise computing model, shifting on-premises infrastructures to off-premises data centers, accessed over the Internet and managed by cloud hosting providers. Regardless of its advantages, the transition to this computing paradigm raises security concerns, which are the subject of several studies. Besides of the issues derived from Web technologies and the Internet, clouds introduce new issues that should be cleared out first in order to further allow the number of cloud deployments to increase. This paper surveys the works on cloud security issues, making a comprehensive review of the literature on the subject. It addresses several key topics, namely vulnerabilities, threats, and attacks, proposing a taxonomy for their classification. It also contains a thorough review of the main concepts concerning the security state of cloud environments and discusses several open research topics.

Mary Macharia (2022), A Decision-making Framework: Cloud computing systems have the potential to provide many advantages for businesses. However, the use of cloud-based systems exposes organizations to risks that they might not otherwise have experienced, specifically because their data is stored on remote servers accessed via password-protected applications and controlled by cloud service providers, thus allowing for the possibility of a myriad of risks. Prior research on cloud computing has either focused on the advantages of cloud computing or on its associated risks, doing so which only provides half the picture. This two-part study presents findings from a survey questionnaire and a review culminating in a proposed model that combines both the proposed positive outcomes and potential risks of cloud computing.

Kamal Upreti (2021), Analytical Study on Performance of Cloud Computing with Respect to Data Security: The new technology of computer-oriented services is cloud computing. Cloud computing is becoming increasingly common and continues to expand due to rapid growth in the “cloud computing” sector. It makes major safety issues in big organizations more cost-effective since they pool valuable resources. As a result of the growing demand for more clouds and data, many security problems such as confidentiality, integrity and authentication could emerge in an open setting. These innovations have transformed the shape of conventional IT. This technology provides numerous advantages to IT companies, despite being challenged to meet their maturity. This paper has been debated Data security and privacy concerns are critical for both cloud architecture hardware and applications. The algorithm preserves confidential data across the cloud through encryption and decryption. This algorithm may be used for improving data confidentiality in the results assessment.

Yashar Abed (2018), The Challenges of Institutional Distance: Data Privacy Issues in Cloud Computing: Data protection and data privacy are significant challenges in cloud computing for multinational corporations. There are no standard laws to protect data across borders. The institutional and regulatory constraints and governance differ across countries. This article explores the challenges of institutional constraints faced by cloud computing service providers in regard to data privacy issues across borders. Through a qualitative case study methodology, this research compares the institutional structure of a few host countries, with regard to data privacy in cloud computing and delineates a relative case study. This article will also review the cloud computing legal frameworks and the history of cloud computing to make the concept more comprehensible to a layman.

Raphael Horvath (2015), A Literature Review on Challenges and Effects of Software Defined Networking: Network technologies have always been a crucial part of success for technologies like cloud computing. But due to the slow development of a scalable IT infrastructure, this can lead to issues in competitiveness. Software defined networking (SDN) can thereby counteract such issues by giving new functions to the whole network topology. With SDN, administrators have the possibility to abstract the underlying network infrastructure for applications and network services. The paper reports on the main outcomes of a systematic literature review on challenges and effects of SDN. It shows that most papers address the implementation of software defined networking as a challenge, including factors like vendor lock-in and the general risk of changing traditional network architectures. Attention is also given to security issues arising with software defined networks and the permanent high demand from the end-user combined with the fear of changing traditional networks.

Shailendra Giri (2019), :Cloud computing is being an alternate choice of computer and mobile users for the data storage and access. Cloud computing and data security both are being major issues in Nepal. The author is trying to explorer about cloud computing and data security in cloud. The content analysis method is used to conduct the study. The study concludes that the cloud computing is essential for Nepal means of data accessible, regulation and storage. Nepal is under developed country as well it has not sufficient technological knowhow, sufficient financial resources, huge digital divide, and skilled human resources so the data security issue is genuine in this time. The storage, virtualization, and networks are the major security concerns in Cloud Computing. Virtualization allows multiple users to share a physical server is one of the key concerns for cloud users and providers. Cloud networks are in target for attacks particularly while communicating with remote virtual equipment basically their target in data. It is clear that Nepal is facing many challenges in cloud computing are securities, storage, data centre operation, costing model, charging model, service level agreement, locality, integrity, access, segregation, breaches and confidentiality. Nepal is one of the developing country, it should start to use own sever and satellite for communication as well as data centre or data bank.

Shailja Tripathi (2015), Task-Technology Fit (TTF) Model To Evaluate Adoption of Cloud Computing:Cloud computing technology (CCT) provides software applications, storage, computing power and other services from remote data center with internet support. Obeidat and Turgay (2012) applied Triple-T and TAM models to evaluate adoption of cloud technology. To evaluate the performance impact of cloud technology in the organization, this study attempts to apply TPC (technology to performance chain) model, which is a combination of TTF (task technology fit) and utilization models. A detailed survey in the form of questionnaire was carried out around four multinational IT firms. The feedback data collected from senior project people has been examined in detail. It is found that all the surveyed firms supported use of CCT to increase effectiveness of individuals in performing their job tasks. Production timeliness, system reliability, ease of use, authorization to access data, automation and training are found as positive factors that influence the individual performance through CCT usage. TPC is found as a useful model to evaluate adoption of CCT.

Manal M. Yunis (2010), A 'cloud-free' security model for cloud computing: Characterised by low investment cost, economies of scale, open standards and sustainability, cloud computing is being increasingly adopted by organisations. This paper presents the development of a comprehensive model that highlights the security impacts of cloud computing on organisations' information security strategies. The 'cloud-free' security model symbolises a computing model with a low level of uncertainty regarding security concerns. Using theoretical frameworks and deploying the analytic hierarchy process as a quantitative method technique, the model will be both validated and assessed. The model can be applied in assessing the security issues emanating from cloud computing, identifying the security countermeasures needed to address these issues and coordinating the efforts of the various participants to enhance information security in organisations adopting cloud computing. This contribution is believed to be useful to practitioners, academicians and researchers in the information security and cloud computing research streams.

Elena Jaramillo (2013), A Survey of Key Issues and the Premises of a Proposal: More sophisticated inter-organizational interactions have generated changes in the way in which organizations make business. Advanced forms of collaborations, such as Business Process as a Service (BPaaS), allow different partners to leverage business intelligence within organizations. However, although it presents power full economical and technical benefits, it also arises some pitfalls about data security, especially when it is mediated by the cloud. In this article, current aspects which have been tackled in the literature related to data risks and accountability are presented. In addition, some open issues are also presented from the analysis of the existing methodologies and techniques proposed in the literature. A final point is made by proposing an approach, which aims at preventive, detective and corrective accountability and data risk management, based on usage control policies and model driven engineering.

CHAPTER 3 – RESEARCH METHODOLOGY

3.1 METHODOLOGY

Research methodology is the specific procedures or techniques used to identify, select, process, and analyse information about a topic. In a research paper, the methodology section allows the reader to critically evaluate a study's overall validity and reliability. It is a design or plan as a guide for conducting research and to systematically solve the research problem. It includes research design, sampling procedures, data collection method and analysis process.

3.2 RESEARCH DESIGN

Research design is a blue print framework which specifies the details of the procedures necessary for obtaining the information needed to structure or solve research problems. The research design refers to the overall strategy that you choose to integrate the different components of the study in a coherent and logical way, thereby, ensuring you will effectively address the research problem

3.3 SAMPLE DESIGN

Sample means “where only a small unit of unknown population under study are considered for analysis”. For the research work, we have adopted methods. For this study adopted 97 samples were taken.

SAMPLE AREA

The sample area selected for the study is Chennai City.

3.4 SAMPLING TECHNIQUE

Convenience Level Sampling: A convenience sample is one of the main types of non-probability sampling methods. A convenience sample is made up of people who are easy to reach.

DATA COLLECTION

While dealing about the method of data collection to be used for the study, we should keep in mind two types of data. i.e., primary data and secondary.

PRIMARY DATA

Primary data are these which are collected for the first time and they are original in character. The researcher to study a particular problem and collects them himself. Here, questionnaire is the primary data.

SECONDARY DATA

The secondary data are those, which are already collected by someone for some purpose and are available for the present study. In this study secondary data has been collected for supportive evidence and analytical study. Here, I have collected some from journals and books.

SAMPLING METHOD

These are the two types of sampling methods namely:

- Probability sampling
- Non probability sampling.

PROBABILITY SAMPLING

Probability sampling means that you use a completely random sample from the group of people you're interested in this group is called the population. By using a completely random sample, the results of your study will be generalisable to the entire population. In other words, you can expect the same results across the entire group, without having to collect data from the entire group which is often not possible for large groups.

NON- PROBABILITY SAMPLING

Non-probability sampling, on the other hand, doesn't use a random sample. For example, it might involve using a convenience sample, which means you'd interview or survey people that you have access to perhaps your friends, family or work colleagues, rather than a truly random sample which might be difficult to achieve due to resource constraints. With non-probability sampling, the results are typically not generalisable.

DATA COLLECTION INSTRUMENT

In this project, the research has used questionnaire for collecting primary data. The 16 Questionnaire consist of a number of questions typed in a definite order on a form or set of forms relating to certain specific aspects regarding which the researcher collects the data. Statistical tools used:

Percentage analysis was used to comparison.

Formula for Percentage (%) analysis:

Number of respondents $\div$ $\times$ 100 Total number of respondents.

SAMPLE SIZE

Sample size selected for the research is 97.

3.5 ANALYTICAL TOOLS (SPSS)

Tool for testing the Hypothesis (SPSS)

- Anova

ANOVA

TEST

One-Way ANOVA ("analysis of variance") compares the means of two or more independent groups in order to determine whether there is statistical evidence that the associated population means are significantly different. One-Way ANOVA is a parametric test. This test is also known as: One-Factor ANOVA.

3.6 HYPOTHESIS:

In research, hypothesis typically is an idea or explanation that is tested through study and experimentation.

NULL HYPOTHESIS:

- H0: There is a significance between age and cost benefit satisfaction towards cloud computing.

ALTERNATIVE HYPOTHESIS:

- H1: There is no significance between age and cost benefit satisfaction towards cloud computing.

CHAPTER 4 - DATA ANALYSIS AND INTERPRETATION

4.1 PERCENTAGE ANALYSIS

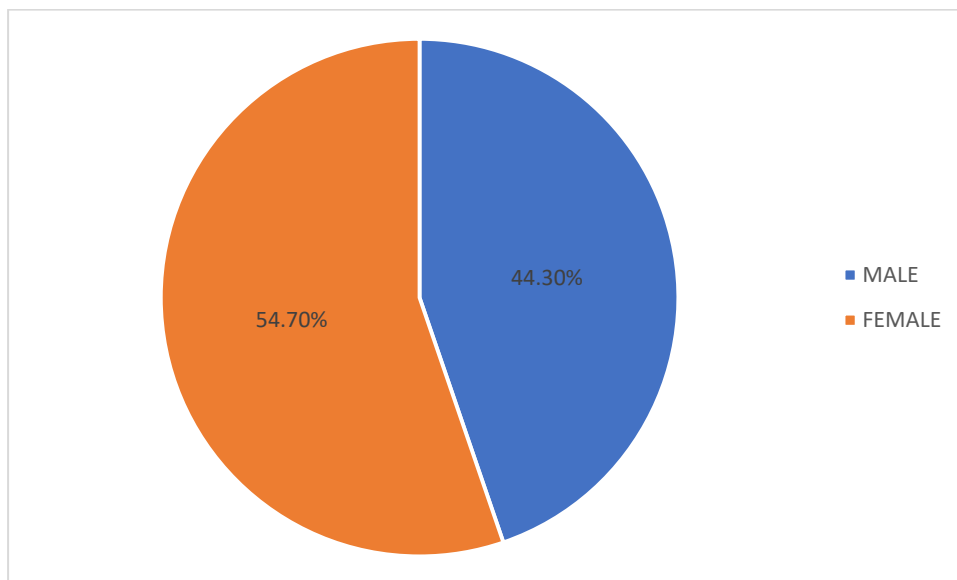
s

4.1.1 TABLE SHOWING GENDER OF THE RESPONDENTS

OPTION	NO OF RESPONDENTS	PERCENTAGE
MALE	43	44.30%
FEMALE	54	54.70%
TOTAL	97	100%

FINDINGS

From the above table it is found 44.3% of the respondents are male, 54.7% of the respondents are female.



4.1.1 CHART SHOWING GENDER OF THE RESPONDENTS

INFERENCE

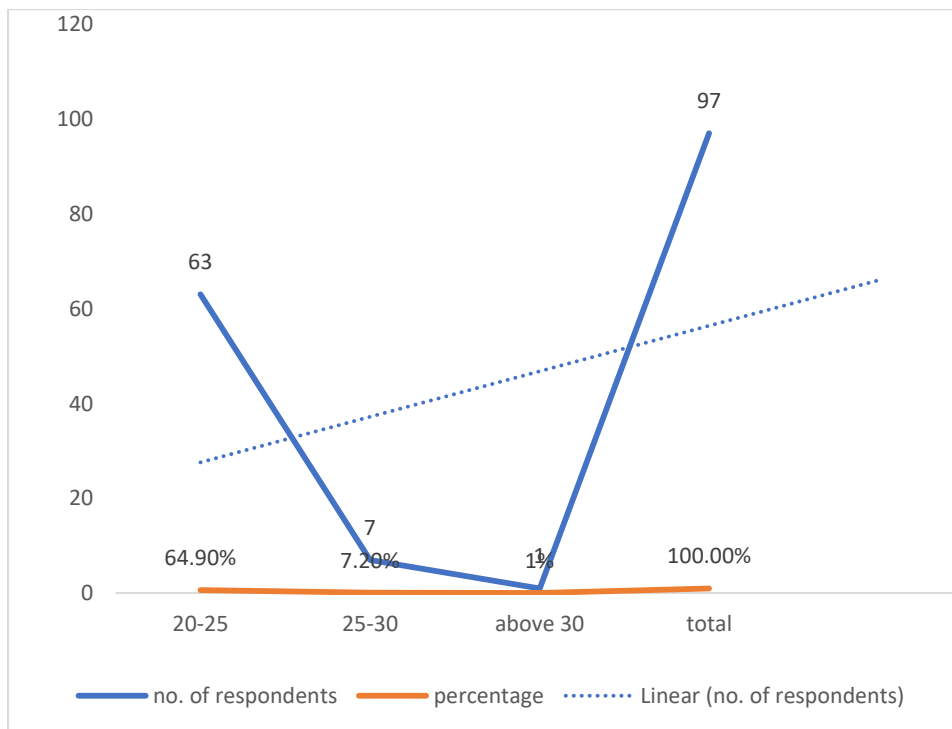
It is interpreted that 54.7% of the respondents are female

4.1.2 TABLE SHOWING AGE OF THE RESPONDENTS

Age	No. of respondents	percentage
18-20	26	26.80%
20-25	63	64.90%
25-30	7	7.20%
above 30	1	1%
total	97	100.00%

FINDINGS

From the above table it is found that 26.8% respondents are between 18-20 and 64.9% are between 20-25 and 7.2% are between 25-30 and 1% are above 30



4.1.2 CHART SHOWING AGE OF THE RESPONDENTS

INFERENCE

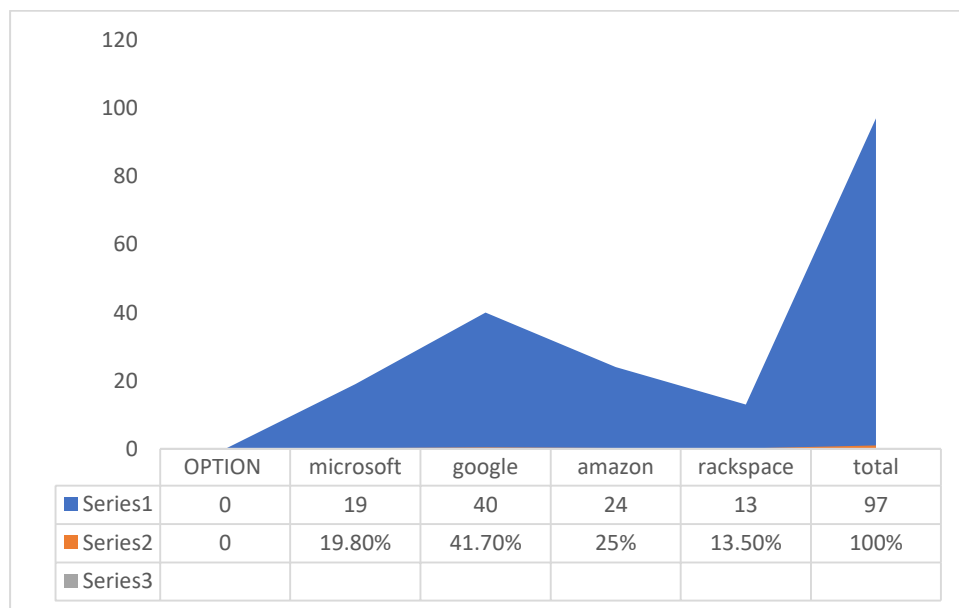
It is interpreted that 64.9% are between age group of 20-25 years

4.1.3 TABLE SHOWING THE SERVICE PROVIDER FOR CLOUD COMPUTING APPLICATIONS

OPTION	NO. OF RESPONDENTS	PERCENTAGE
Microsoft	19	19.80%
google	40	41.70%
amazon	24	25%
Rack space	13	13.50%
total	97	100%

FINDINGS

From the above table it is founded 41.7% of the respondents from google, 25% of the respondents from amazon, 19.8% of the respondents from Microsoft and 13.5% of the respondents from rack space.



4.1.3 CHART SHOWING THE SERVICE PROVIDER FOR CLOUD COMPUTING APPLICATIONS

INFERENCE

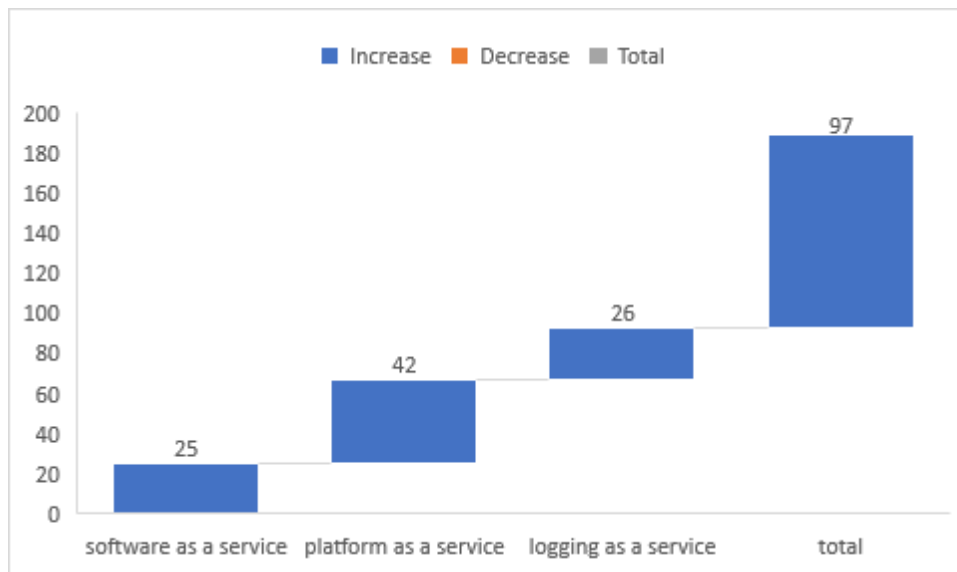
It is interpreted that 41.7% of the respondents are from google

4.1.4 TABLE SHOWING THE TYPE OF SERVICE DELIVERY SOLUTIONS ARE MORE SUITABLE FOR ALL SIZED ENTERPRISES

OPTION	NO. OF RESPONDENTS	PERCENTAGE
software as a service	25	26.90%
platform as a service	42	45.20%
logging as a service	26	28%
total	97	100%

FINDINGS

From the above table it is founded 45.2% of the respondents from platform as a service,26.9% of the respondents from software as a service and 28% of the respondents from logging as a service.



4.1.4 CHART SHOWING THE TYPE OF SERVICE DELIVERY SOLUTIONS ARE MORE SUITABLE FOR ALL SIZED ENTERPRISES

INFERENCE

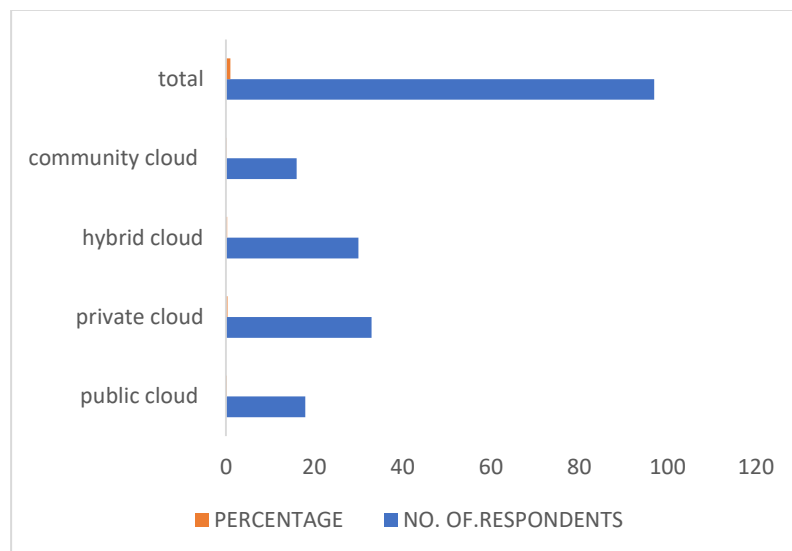
It is interpreted that 45.2% of the respondents from the platform as a service.

4.1.5 TABLE SHOWING THE TYPE OF CLOUD COMPUTING MODELS IS MORE SUITABLE FOR ALL SIZED ENTERPRISES

OPTION	NO. OF.RESPONDENTS	PERCENTAGE
public cloud	18	18.60%
private cloud	33	34%
hybrid cloud	30	30.90%
community cloud	16	16.50%
total	97	100%

FINDINGS

From the above table is it founded 34% of the respondents from private cloud, 30.9% of the respondents from hybrid cloud, 18.6% of the respondents from public cloud, 16.5% of the respondents from community cloud.



4.1.5 CHART SHOWING THE TYPE OF CLOUD COMPUTING MODELS IS MORE

INFERENCE

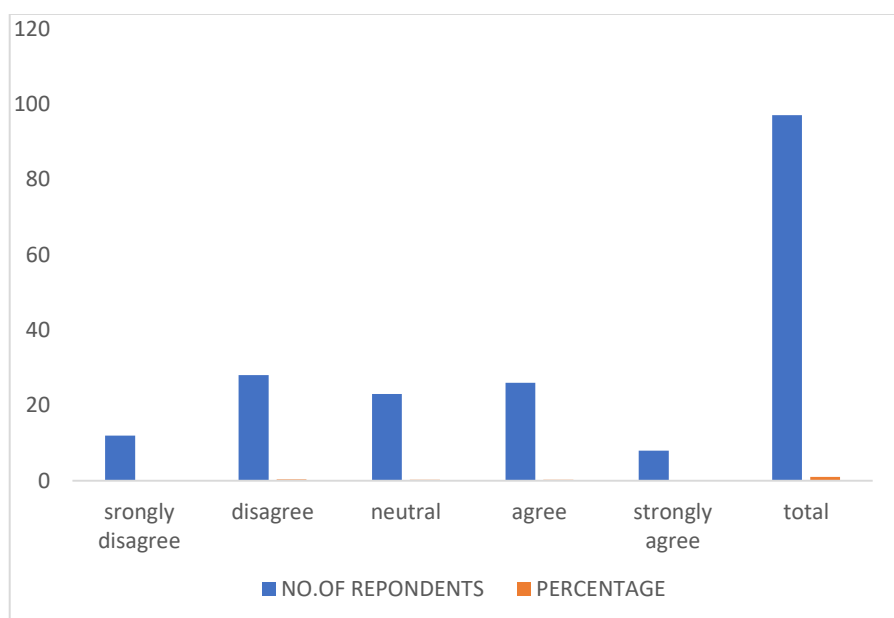
It is interpreted that 34% of the respondents from the private cloud

4.1.6 TABLE HOWING THE COST BENEFIT IS THE BIGGEST CHALLENGE THAT LEADS ENTERPRISES TO MIGRATE INTO CLOUD COMPUTING

OPTION	NO.OF REPENDENTS	PERCENTAGE
strongly disagree	12	12.40%
disagree	28	28.90%
neutral	23	23.70%
agree	26	26.80%
strongly agree	8	8.20%
total	97	100%

FINDINGS

From the above table is it founded 28.9% of the respondents feels disagree, 26.8% of the respondents feels agree, 23.7% of the respondents feels neutral, 12.4% of the respondents feels strongly disagree and 8.2% of the respondents feels strongly agree.



4.1.6 CHART SHOWING THE COST BENEFIT IS THE BIGGEST CHALLENGE THAT LEADS ENTERPRISES TO MIGRATE INTO CLOUD COMPUTING

INFERENCE

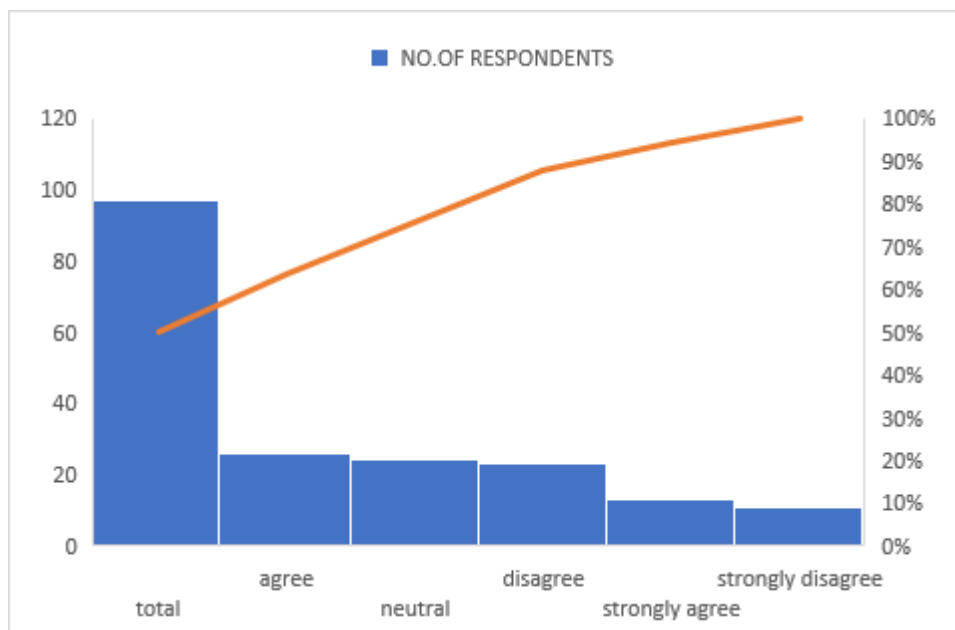
It is interpreted that 28.9% of the respondents feels disagree.

4.1.7 TABLE SHOWING THE SECURITY IS THE MOST CONCERN FOR ENTERPRISES BEFORE GIONG TO THE CLOUD COMPUTING

OPTION	NO.OF. RESPONDENTS	PERCENTAGE
strongly disagree	11	11.30%
disagree	23	23.70%
neutral	24	24.70%
agree	26	26.80%
strongly agree	13	13.40%
total	97	100%

FINDINGS

From the above table it is founded 26.8% of the respondents feels agree, 24.7% of the respondents feels neural, 23.7% of the respondents feels disagree, 13.4% of the respondents feels strongly agree, 11.3% of the respondents feels strongly disagree.



4.1.7 CHART SHOWING THE SECURITY IS THE MOST CONCERN FOR ENTERPRISES BEFORE GIONG TO THE CLOUD COMPUTING

INFERENCE

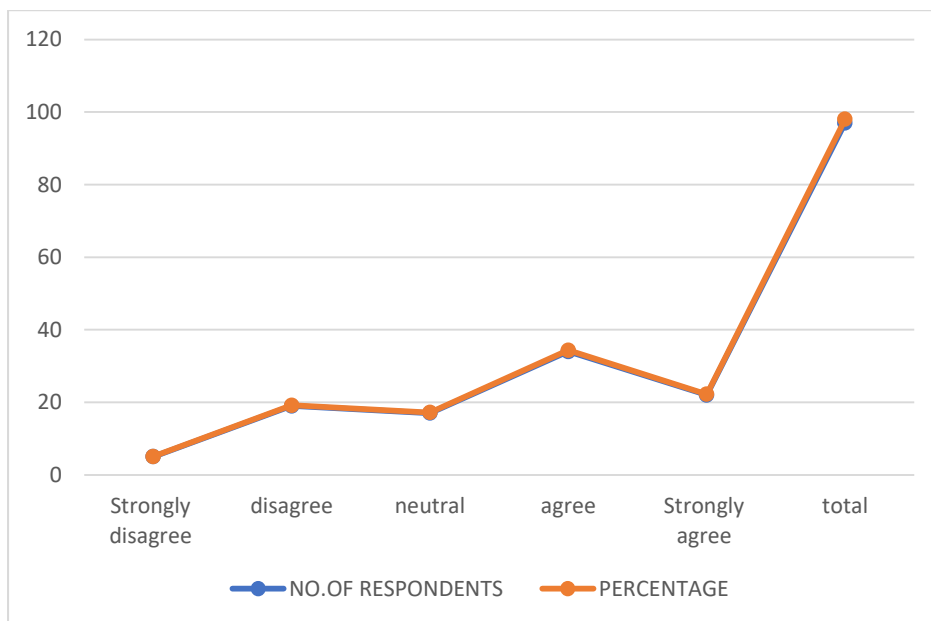
It is interpreted that 26.8% of the respondents feels agree.

4.1.8 TABLE SHOWING WHILE USING THE CLOUDE TECHNOLOGY COMPATIBLE WITH MOST ASPECTS OF THE COMPANY WORK

OPTION	NO.OF. RESPONDENTS	PERCENTAGE
Strongly disagree	5	5.20%
disagree	19	19.60%
neutral	17	17.50%
agree	34	35.10%
Strongly agree	22	22.70%
total	97	100%

FINDINGS

From the above table it is founded 35.1% of the respondents feels agree, 22.7% of the respondents feels strongly agree, 19.6% of the respondents feels disagree, 17.5% of the respondents feels neutral and 5.2% of the respondents feels strongly disagree.



4.1.8 CHART SHOWING WHILE USING THE CLOUDE TECHNOLOGY I COMPATIBLE WITH MOST ASPECTS OF THE COMPANY WORK

INFERNCE

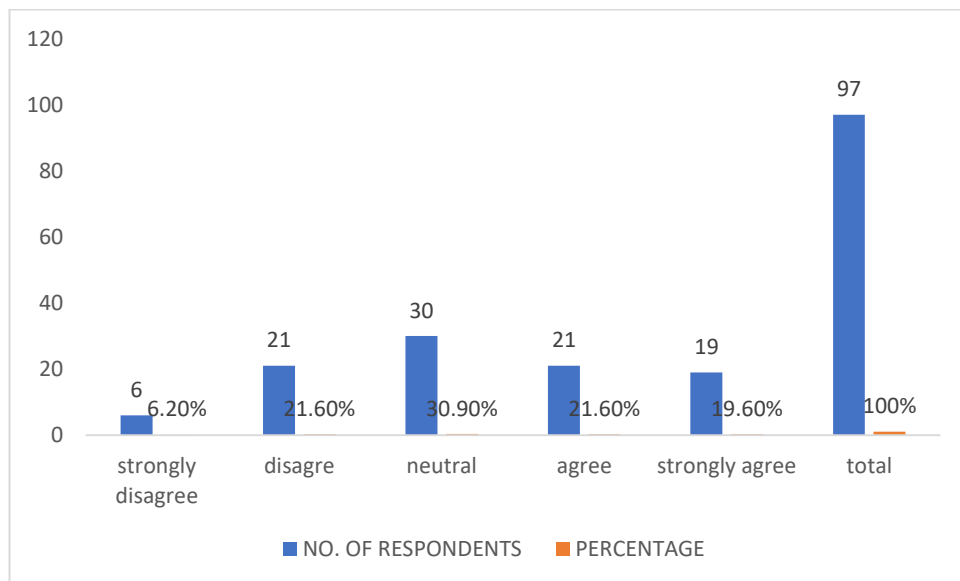
It is interpreted that 35.1% of the respondents feels.

4.1.9 TABLE SHOWING WHETHER THE CLOUD COMPUTING IS A CLOUD TECHNOLOGY THAT USED TO MINIMIZE THE COST OF A COMPANY

OPTION	NO. OF RESPONDENTS	PERCENTAGE
strongly disagree	6	6.20%
disagree	21	21.60%
neutral	30	30.90%
agree	21	21.60%
strongly agree	19	19.60%
total	97	100%

FINDINGS

From the above table it is founded that 30.9% of the respondents feels neutral, 21.60% of the respondents feels disagree , 21.6% of the respondents feels agree, 19.6% of the respondents feels strongly agree and 6.2% of the respondents feels strongly disagree.



4.1.9 CHART SHOWING WHETHER THE CLOUD COMPUTING IS A CLOUD TECHNOLOGY THAT USED TO MINIMIZE THE COST OF A COMPANY

INFERENCE

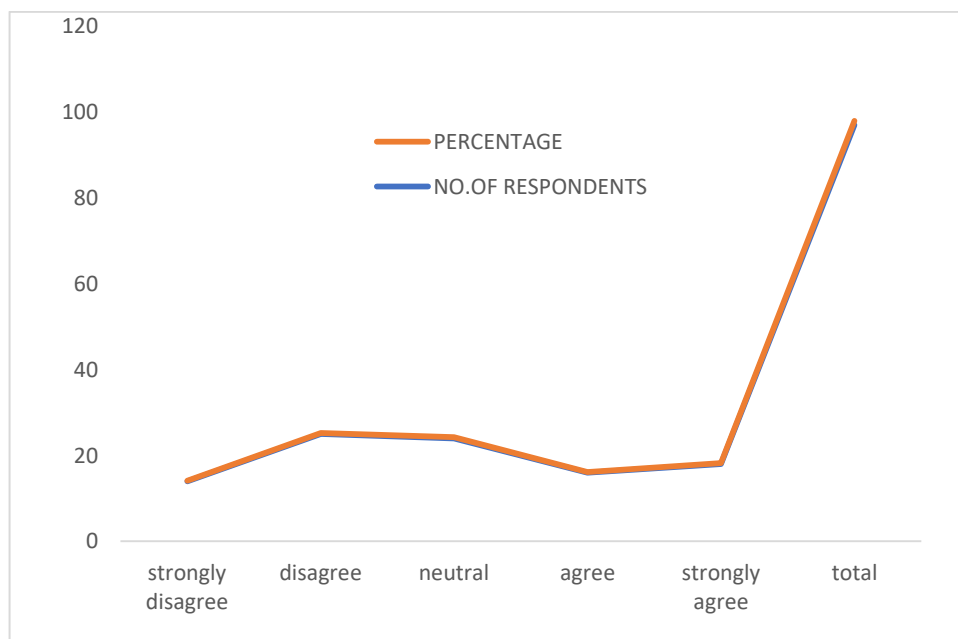
It is interpreted that 30.9% of the respondents feels neutral.

4.1.10 TABLE SHOWING THAT USING AN APPLICATION HOSTED IN THE CLOUD IS MUCH EASIER THAN WHEN HOSTED IN ON-PREMISE ENVIRONMENT

OPTION	NO.OF. RESPONDENTS	PERCENTAGE
strongly disagree	14	14.40%
disagree	25	25.80%
neutral	24	24.70%
agree	16	16.50%
strongly agree	18	18.60%
total	97	100%

FINDINGS

From the above table it is founded that 25.8% of the respondents feels disagree, 24.7% of the respondents feels neutral, 18.6% of the respondents feels strongly agree, 16.5% of the respondents feels agree, 14.4% of the respondents feels strongly disagree.



4.1.10 CHART SHOWING THAT USING AN APPLICATION HOSTED IN THE CLOUD IS MUCH EASIER THAN WHEN HOSTED IN ON-PREMISE ENVIRONMENT

INFERENCE

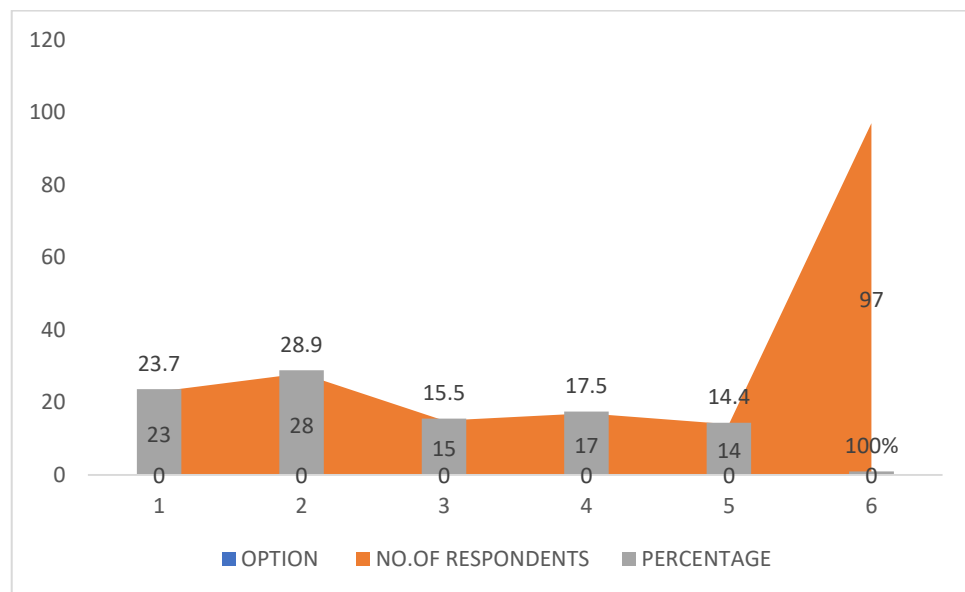
It is interpreted that 25.8% of the respondents feels disagree.

4.1.11 TABLE SHOWING THAT BELOW ARE THE MOST CLOUD COMPETING CHALLENGES THAT AFFECT ENTERPRISES

OPTION	NO.OF. RESPONDENTS	PERCENTAGE
Strongly disagree	23	23.7%
Disagree	28	28.9%
Neutral	15	15.5%
Agree	17	17.5%
Strongly agree	14	14.4%
Total	97	100%

FINDINGS

From the above table it is founded that 28.9% of the respondents feels disagree, 23.7% of the respondents feels strongly disagree, 17.5% of the respondents feels agree, 15.5% of the respondents feels neutral, 14.4% of the respondents feels strongly agree.



4.1.11 CHART SHOWING THAT BELOW ARE THE MOST CLOUD COMPETING CHALLENGES THAT AFFECT ENTERPRISES

INFERENCE

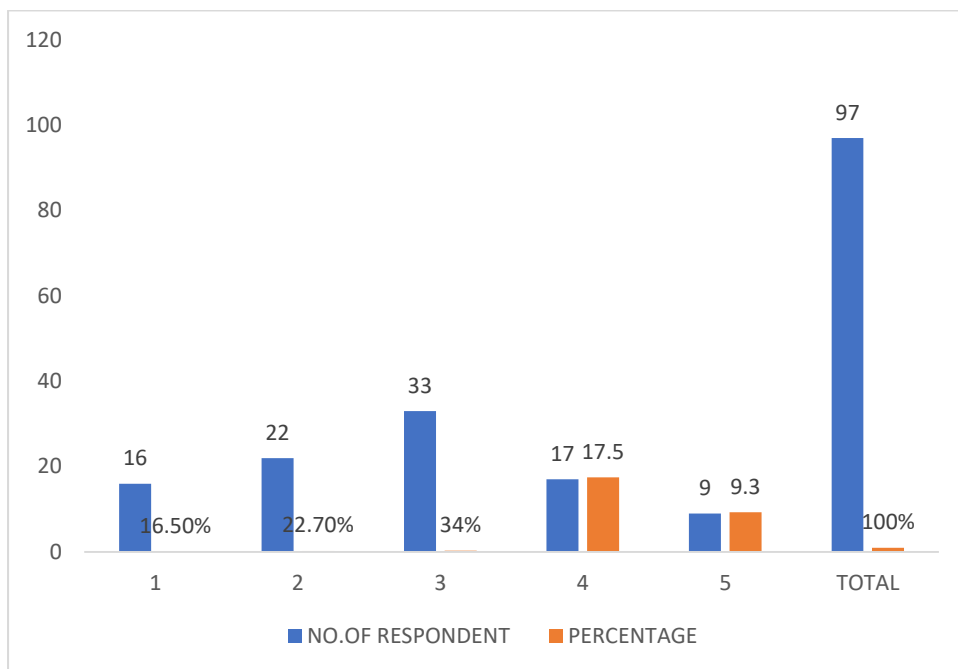
It is interpreted that 28.9% of the respondents feels disagree.

4.1.12 TABLE SHOWING THAT ESSENTIAL POSITIVE REASONS THAT ENTERPRISES ADOPT TO CLOUD COMPUTING

OPTION	NO.OF. RESPONDENT	PERCENTAGE
1	16	16.50%
2	22	22.70%
3	33	34%
4	17	17.5%
5	9	9.3%
TOTAL	97	100%

FINDINGS

From the above table it is founded that 34% of the respondents chose rank 3, 22.7% of the respondents chose rank 2, 17.5% of the respondents chose rank 4, 16.5% of the respondents chose rank 1, 9.3% of the respondents chose rank 5.



4.1.12 CHART SHOWING THAT ESSENTIAL POSITIVE REASONS THAT ENTERPRISES ADOPT TO CLOUD COMPUTING

INFERENCE

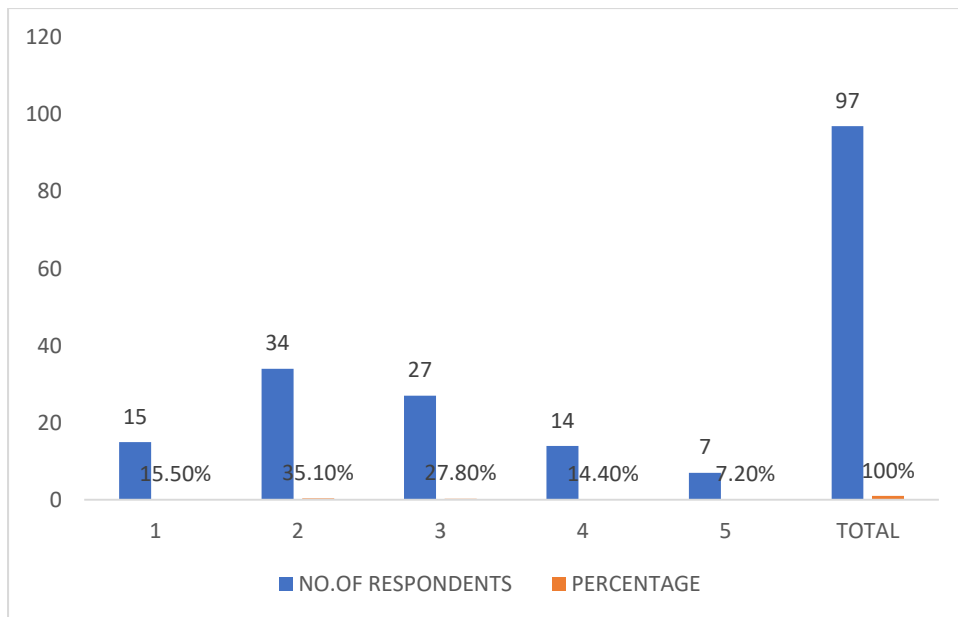
It is interpreted that 34% of the respondents chose rank 3.

4.1.13 TABLE SHOWING THE MAIN CONCERN BY ENTERPRISRES BEFORE MIGRATING TO CLOUD COMPUTING

OPTION	NO.OF. RESPONDENTS	PERCENTAGE
1	15	15.50%
2	34	35.10%
3	27	27.80%
4	14	14.40%
5	7	7.20%
TOTAL	97	100%

FINDINGS

From the above table it is founded that 35.1% of the respondents chose rank 2, 27.8% of the respondents chose rank 3, 15.5% of the respondents chose rank 1, 14.4% of the respondents chose rank 4, 7.2% of the respondents chose rank 5.



4.1.13 CHART SHOWING THE MAIN CONCERN BY ENTERPRISRES BEFORE MIGRATING TO CLOUD COMPUTING

INFERENCE

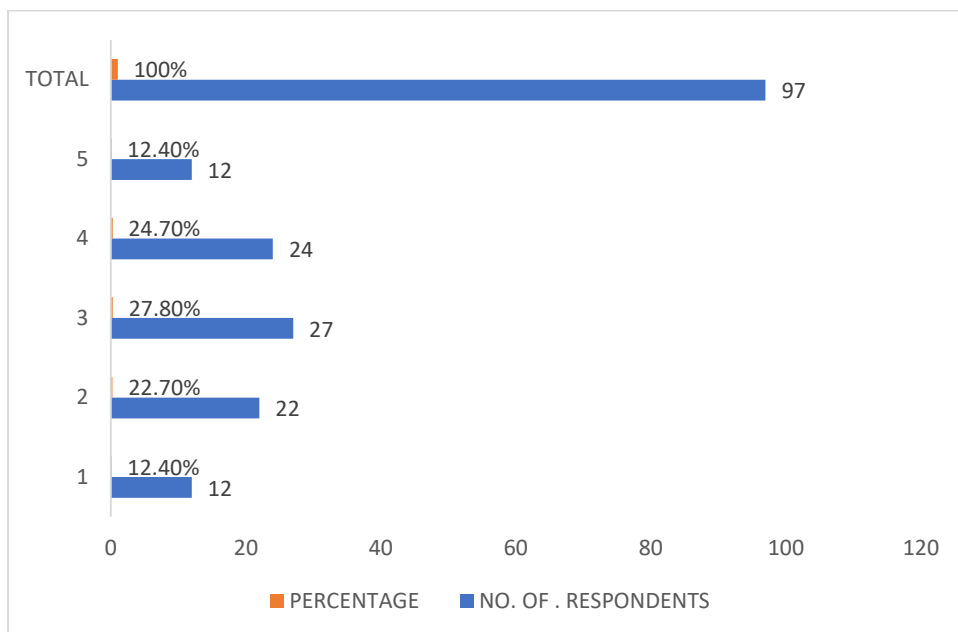
It is interpreted that 35.1% of the respondents chose rank 2.

4.1.14 TABLE SHOWING THE MAIN SECURITY RISKS WHEN ADOPT INTO THE CLOUD COMPUTING AREA

OPTION	NO. OF . RESPONDENTS	PERCENTAGE
1	12	12.40%
2	22	22.70%
3	27	27.80%
4	24	24.70%
5	12	12.40%
TOTAL	97	100%

FINDINGS

From the above table it is founded that 27.8% of the respondents chose rank 3, 24.7% of the respondents chose rank 4, 22.7% of the respondents chose rank 2, 12.4% of the respondents chose rank 1, 12.4% of the respondents chose rank 5.



4.1.14 CHART SHOWING THE MAIN SECURITY RISKS WHEN ADOPT INTO THE CLOUD COMPUTING AREA

INFERENCE

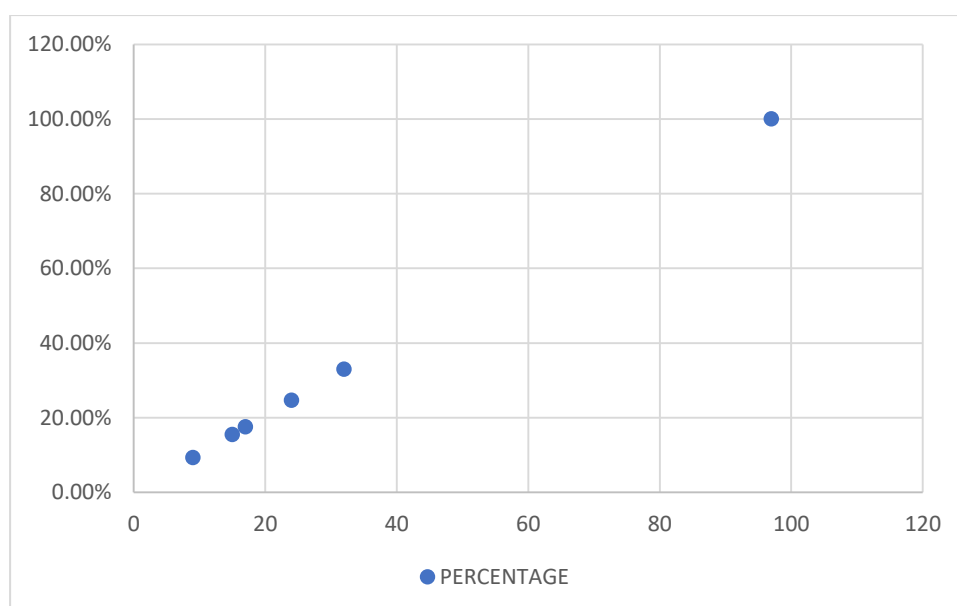
It is interpreted that 27.8% of the respondents chose rank 3.

4.1.15 TABLE SHOWING THE YOUR ORGANIZATION VIEW AS THE MOST IMPORTANT BENEFITS OF CLOUD COMPUTING

OPTION	NO.OF.RESPONDENTS	PERCENTAGE
strongly disagree	15	15.50%
disagree	24	24.70%
neutral	32	33%
agree	17	17.50%
strongly agree	9	9.30%
total	97	100%

FINDINGS

From the above table it is founded that 33% of the respondents feels neutral, 24.7% of the respondents feels disagree, 17.5% of the respondents feels agree, 15.5% of the respondents feels strongly disagree, 9.3% of the respondents feels strongly agree.



4.1.15 CHART SHOWING THE YOUR ORGANIZATION VIEW AS THE MOST IMPORTANT BENEFITS OF CLOUD COMPUTING

INFERENCE

It is interpreted that 33% of the respondents feels neutral.

4.2 STATISTICAL ANALYSIS

HYPOTHESIS:

- Null Hypothesis (H0): There is significance difference between age and cost benefit
- Alternative Hypothesis (H1): There is no significance difference between age and cost benefit.

TABLE SHOWING SIGNIFICANCE DIFFERENCE BETWEEN AGE AND COST BENEFIT

ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1.118	4	.279	.781	.540
Within Groups	32.903	92	.358		
Total	34.021	96			

INTERPRETATION

The p value is 0.540 which is greater than the significance value (0.05) hence null hypothesis (H0) is accepted. And H1 is rejected.

INFERENCE

There is no significant difference in the perception of cost benefit among different age groups.

CHAPTER – 5

FINDINGS, SUGGESTIONS AND CONCLUSION

5.1 FINDINGS

- Majority (54.7%) of the respondents are female
- Majority (64.9%) are between age group of 20-25 years
- Majority (41.7%) of the respondents are from google
- Majority (45.2%) of the respondents from the platform as a service.
- Majority (34%) of the respondents from the private cloud
- Majority (28.9%) of the respondents feels disagree.
- Majority (26.8%) of the respondents feels agree
- Majority (35.1%) of the respondents feels.
- Majority (30.9%) of the respondents feels neutral.
- Majority (25.8%) of the respondents feels disagree.
- Majority (28.9%) of the respondents feels disagree.
- Majority (34%) of the respondents chose rank 3.
- Majority (35.1%) of the respondents chose rank 2.
- Majority (27.8%) of the respondents chose rank 3.
- Majority (33%) of the respondents feels neutral.

5.2 SUGGESTIONS AND RECOMMENDATIONS

- Enterprises are likely to invest in advanced encryption technologies to safeguard sensitive data transmitted and stored in the cloud.
- Implementing stringent access controls ensures that only authorized personnel can access specific data, reducing the risk of unauthorized breaches.
- Enterprises may introduce training programs to educate employees about the importance of data security and best practices for handling sensitive information in the cloud.

5.3 LIMITATIONS OF THE STUDY

- Some of the respondents were having little difficulty in expressing their view
- Accuracy of the study is purely based on the information as given by the respondents.
- The respondents may have some personal bias in answering the questions. Due to constraint of time, only specific sample sizes from the entire unknown population

5.4 CONCLUSION

Cloud computing is a promising and emerging technology for the next generation of IT applications. The barrier and hurdles toward the rapid growth of cloud computing are data security and privacy issues. Reducing data storage and processing cost is a mandatory requirement of any organization, while analysis of data and information is always the most important tasks in all the organizations for decision making. So no organizations will transfer their data or information to the cloud until the trust is built between the cloud service providers and consumers. A number of techniques have been proposed by researchers for data protection and to attain highest level of data security in the cloud. However, there are still many gaps to be filled by making these techniques more effective. More work is required in the area of cloud computing to make it acceptable by the cloud service consumers. This paper surveyed different techniques about data security and privacy, focusing on the data storage and use in the cloud, for data protection in the cloud computing environments to build trust between cloud service providers and consumers.

REFERENCES

- [1] Bohu,L., Lin, Z. and Xudong, C., (2020). Introduction to cloud manufacturing. ZTE Communications, 8(4), pp.6-9.
- [2] Brannen, J. ed., (2017). Mixing methods: Qualitative and quantitative research. Routledge.
- [3] K. Lambert, (2020, April 13). IMPERVA.<https://www.imperva.com/blog/the-2020-cyberthreatdefense-report-simplify-security-with-unified-tools-and-monitoring/>.
- [4] Jain, A. and Mahajan, N., (2017). Introduction to cloud computing. In The Cloud DBA-Oracle (pp. 3-10). Apress, Berkeley, CA.
- [5] Zhe, D., Qinghong, W., Naizheng, S. and Yuhua, Z., (2017). Study on data security policy based on cloud storage. In 2017 IEEE 3rd international conference on big data security on cloud (bigdatasecurity), IEEE international conference on high performance and smart computing (hpsc), and IEEE international conference on intelligent data and security (ids) (pp. 145-149). IEEE.
- [6] Huy, A.Q. and Hung, P.D., (2019). Security and Cost Optimization Auditing for Amazon Web Services. In Proceedings of the 2nd International Conference on Software Engineering and Information Management (pp. 44-48).
- [7] Khayer, A., Talukder, M.S., Bao, Y. and Hossain, M.N., (2020). Cloud computing adoption and its impact on SMEs' performance for cloud supported operations: A dual-stage analytical approach. Technology in Society, 60, p.101225.
- [8] Jouini, M. and Rabai, L.B.A., (2019). A security framework for secure cloud computing environments. In Cloud security: Concepts, methodologies, tools, and applications (pp. 249-263). IGI Global.
- [9] Chang, Y. W., & Hsu, P. Y. (2019). An empirical investigation of organizations' switching intention to cloud enterprise resource planning: a cost-benefit perspective. Information Development, 35(2), 290-302.
- [10] Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115.